LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

PRELIMINARY VERSION

UNEDITED

The preliminary version of this legislative summary is made available to parliamentarians, parliamentary staff and the public to ensure timely access to the information, research and analysis needed to study the bill in question. The official version of the legislative summary, which may differ from this unedited version, will replace this document on the Parliament of Canada website.

Legislative Summary

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

45-1-C34-E

28 August 2026

Jed Chong, Stephanie Feldman, Alexandre Lafrenière and Liane Tanguay

Library and Research Services

PRELIMINARY VERSION
UNEDITED

AUTHORSHIP

28 August 2026 Jed Chong, Stephanie Feldman, Alexandre Lafrenière and Liane Tanguay

ABOUT THIS PUBLICATION

Library of Parliament legislative summaries summarize bills currently before Parliament and provide background information about them in an objective and impartial manner. They are prepared by Library and Research Services, which carries out research for and provides information and analysis to parliamentarians, Senate and House of Commons committees and parliamentary associations. Legislative summaries are revised as needed to reflect amendments made to bills as they move through the legislative process.

For clarity of exposition, the legislative proposals set out in the bill described in this legislative summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the Senate and House of Commons and have no force or effect unless and until they are passed by both houses of Parliament, receive Royal Assent and come into force.

Any substantive changes to this Library of Parliament legislative summary that have been made since the preceding issue are indicated in **bold print**.

© Library of Parliament, Ottawa, Canada, 2026

Legislative Summary of Bill C-34
(Preliminary version)

45-1-C34-E

Ce document est également publié en français.

PRELIMINARY VERSION
UNEDITED

CONTENTS

1 BACKGROUND 1

1.1 Online Harms in Canada 2

1.2 Current Legal Context 4

1.3 The Path to Bill C-34 5
1.3.1 Developing a Framework 5
1.3.2 Parliamentary Studies 6

2 DESCRIPTION AND ANALYSIS 8

2.1 Part 1: Digital Safety Act 8
2.1.1 Interpretation and Application (Sections 2 to 12 of the Digital Safety Act) 8
2.1.2 Digital Safety Commission of Canada (Sections 15 to 19 of the Digital Safety Act) 10
2.1.3 Duties of Operators (Sections 20 to 59 of the Digital Safety Act) 11
2.1.3.1 Duty to Protect Children (Sections 20 to 24 and 26 to 30 of the Digital Safety Act) 11
2.1.3.2 Duty to Act Responsibly (Sections 31 to 41 and 48 to 57 of the Digital Safety Act) 12
2.1.3.3 Duty to Be Transparent (Sections 25, 42, 58 and 59 of the Digital Safety Act) 14
2.1.3.4 Duty to Make Certain Content Inaccessible (Sections 43 to 47 of the Digital Safety Act) 16
2.1.4 Access to Inventories and Electronic Data (Sections 60 to 64 of the Digital Safety Act) 17
2.1.5 Remedies (Sections 65 to 72 of the Digital Safety Act) 17
2.1.6 Administration and Enforcement (Sections 73 to 112 of the Digital Safety Act) 18
2.1.7 Protections, Reports and Information Sharing (Sections 113 to 124 of the Digital Safety Act) 19
2.1.8 Regulations (Sections 126 and 127 of the Digital Safety Act) 20
2.1.9 Reviews by Minister (Sections 128 and 129 of the Digital Safety Act) 20
2.1.10 Coming into Force (Section 130 of the Digital Safety Act) 20
2.1.11 Coordinating Amendment (Clause 3 of Bill C-34) 21

2.2 Part 2: Digital Safety Commission of Canada Act 21

PRELIMINARY VERSION
UNEDITED

LEGISLATIVE SUMMARY OF 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

1 BACKGROUND

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 (short title: Safe Social Media Act),[1] was introduced in the House of Commons on 10 June 2026 by the Minister of Canadian Identity and Culture and Minister responsible for Official Languages. The bill is divided into two parts.

In Part 1, Bill C-34 enacts the Digital Safety Act, which is intended to promote safety, reduce online harms and ensure transparency and accountability on the part of regulated social media, chatbots and certain other online services, particularly with respect to children. Among other things, it requires operators of such services to:

- act responsibly by implementing measures to mitigate the risk of exposure to harmful content, by providing blocking and flagging tools and by labelling synthetic and automatically generated content;
- implement measures to mitigate the risk of a chatbot communicating harmful content or engaging in harmful behaviours, as well as ensure intervention in crisis situations;
- protect children by integrating safe design features and by implementing age restrictions for accessing pornographic content, as well as by limiting children under 16 from having accounts on certain social media services;
- make inaccessible on social media content that sexually victimizes a child or revictimizes a survivor, as well as non-consensual intimate content; and
- submit a digital safety plan to the Digital Safety Commission of Canada (the Commission) in order to determine compliance with the Act.

Part 1 also authorizes the Governor in Council to impose on operators of other online services the duty to protect children and to be transparent. Finally, it allows persons in Canada to file complaints about certain types of harmful content and to make other submissions to the Commission.

PRELIMINARY VERSION
UNEDITED

The bill identifies and provides definitions for seven types of harmful content:

- intimate content communicated without consent;
- content that sexually victimizes a child or revictimizes a survivor;
- content that induces a child to harm themselves;
- content used to bully a child;
- content that foments hatred;
- content that incites violence; and
- terrorism or violent extremism content.

Part 2 of the bill enacts the Digital Safety Commission of Canada Act, which establishes the Commission as well as its powers, duties and functions, and makes consequential amendments to other Acts.

It is important to note that Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts, introduced in Parliament on 15 June 2026 by the Minister of Artificial Intelligence and Digital Innovation, interacts with and affects Bill C-34, notably by expanding the mandate and changing the name of the Commission and by introducing certain privacy and data-protection rules that would govern the implementation of safety mechanisms under Bill C-34.[2]

1.1 ONLINE HARMS IN CANADA

Social media platforms have facilitated communication and connectivity on a global scale. At the same time, it is widely recognized that they have enabled the proliferation and widespread dissemination of content that can be harmful to personal well-being, to public safety and even to the integrity of democratic institutions.

In Canada, in 2025, 95% of adults had at least one social media account.[3] While the prevalence of specific harms can be difficult to ascertain, the 2022 Canadian Internet Use Survey revealed that 71% of Canadians aged 15 to 24 had been exposed over the previous 12 months to online content inciting hate or violence.[4] Additionally:

- In 2024, police reported 16,905 incidents where there was at least one online child sexual exploitation offence, including 12,978 incidents of online child sexual abuse and exploitation material.[5]
- In 2025, police reported 3,157 incidents of non-consensual distribution of intimate images,[6] of which 488 involved a victim aged 17 years or younger.[7]

PRELIMINARY VERSION
UNEDITED

- In 2024, police reported 368 incidents of sexual extortion involving victims 17 years of age or younger.[8]
- In 2022, youth aged 15–24 were more likely to report feeling victimized by online bullying, harassment or discrimination (6% versus 4% of the overall population).[9]
- In 2022, youth were more likely to report seeing harmful content, including content inciting hate or violence (74%), or intimate images shared without consent (34%).[10]

According to Women and Gender Equality Canada, women are more likely than men to experience online violence. They are also likely to experience more harm from online violence.[11] Statistics Canada also found that, in the year before the 2025 Survey of Safety in Public and Private Spaces, 11% of Canadians experienced unwanted online behaviours, including 12% of women and 9% of men. The disparity was greater among those aged 15 to 24: almost one-fifth of young women and girls reported such experiences, compared with 12% of young men and boys.[12] Statistics Canada noted that other characteristics, such as Indigenous identity, disability, or sexual orientation can "intersect with gender to impact not only the likelihood of experiencing violence, but also other factors such as levels of reporting to police or the availability of appropriate support services."[13] Women and Gender Equality Canada also identifies the "manosphere" as a collection of online communities that promote aggressive gender norms and can target and expose vulnerable young men and boys to radicalizing content.[14]

At the same time, research has indicated that social media can benefit young people, including those representing racial, ethnic, sexual and gender minorities, by providing community, connection and social support. The American Psychological Association has cited young sexual and gender minorities in particular as benefiting from access to peer support and the health information shared among peer networks.[15]

More recently, concerns have emerged around the risks of generative artificial intelligence (AI), including the creation of realistic synthetic content (deepfakes) and interactions with AI chatbots. The Social Media Lab at Toronto Metropolitan University found in April 2025 that 66% of Canadians had experimented with generative AI tools.[16] A June 2026 brief by the United Nations Children's Fund (UNICEF) notes that children are increasingly using such systems for advice, support and sometimes relationships, raising "concerns about inappropriate reliance, misleading advice, and insufficient safety responses in high-risk situations."[17]

PRELIMINARY VERSION
UNEDITED

1.2 CURRENT LEGAL CONTEXT

While several jurisdictions, including the United Kingdom,[18] the European Union,[19] and Australia,[20] have in recent years advanced or enacted legislative frameworks to impose responsibilities upon online services to mitigate online harms, with some beginning to address the risks posed by chatbots,[21] there is currently no such comprehensive framework in Canada. Platform liability for illegal content is currently limited to situations in which the platform knows about the content in advance and proceeds to publish it or is made aware of it and neglects to take it down.[22] However, *Criminal Code* (the Code)[23] provisions respecting uttering threats, hate propaganda, terrorist propaganda, obscene material, non-consensual distribution of intimate images, and some forms of sextortion, cyberbullying and cyberstalking are applicable to online content.[24]

Hate propaganda, including the advocacy and promotion of genocide as well as incitement to violence or discrimination, is a criminal offence under section 318 of the Code; section 319 criminalizes the public communication of statements that incite "hatred against any identifiable group where such incitement is likely to lead to a breach of the peace" or that "wilfully [promote] hatred against any identifiable group." In 2026, Parliament enacted the *Combatting Hate Act*,[25] which, among other things, created an offence of willfully promoting hatred through the public display of certain hate or terrorist symbols and introduced additional hate crime–related offences, such as a standalone hate crime offence (new section 320.1001 of the Code) when any offence under the Code or another Act of Parliament is motivated by hatred based on race, national or ethnic origin, language, colour, religion, sex, age, mental or physical disability, sexual orientation or gender identity or expression. Although these provisions make no specific reference to online speech,[26] hate propaganda located on Canadian computer systems can be ordered for deletion by the courts when stored on a server that is within the court's jurisdiction.[27]

The Code also includes provisions that allow a court to order the seizure of terrorist propaganda, defined in section 83.222(8) as "any writing, sign, visible representation or audio recording that counsels the commission of a terrorism offence." As with hate propaganda, terrorist propaganda may be ordered for deletion.

Content that victimizes a child or revictimizes a survivor is illegal under Code provisions relating to child sexual abuse and exploitation material. The non-consensual distribution of intimate images became a criminal offence with the *Protecting Canadians from Online Crime Act*[28] in 2014. In 2026, the *Protecting Victims Act*[29] expanded the offence to apply to non-consensual sexual deepfakes and to threats to distribute intimate images, including sexual deepfakes. The Code now also requires the court to order the custodian of a computer system within its jurisdiction to take down such material within 48 hours of the order being made (new section 164.1(5.1) of the Code).

PRELIMINARY VERSION
UNEDITED

Content that bullies a child or encourages a child to self-harm are not specifically addressed by the Code, but some forms of bullying, including harassment, intimidation, uttering threats and mischief in relation to data, are captured by provisions that have been applied to cases of cyberbullying. Counselling suicide is also an offence under section 241 of the Code. The law is less clear for other content that advocates self-harm such as disordered eating.

These existing measures generally operate through criminal investigations, prosecutions and court orders and do not establish a regulatory framework for online platforms to prevent or mitigate such content.

No provisions exist in current law for content that is "legal but harmful." There is also no dedicated body with the authority to regulate online platforms in respect of harmful content, illegal or otherwise.

1.3 THE PATH TO BILL C-34

1.3.1 Developing a Framework

The Government of Canada first articulated its commitment to regulating online platforms in respect of harmful content in the 2019 and 2021 mandate letters[30] for the Minister of Canadian Heritage and the Minister of Justice, as well as the 2020 Speech from the Throne.[31] In 2021–2022, the government undertook the following activities with a view to developing an online harms framework:

- consultations on a technical paper[32] proposing content moderation obligations, the establishment of an independent regulator and amendments to *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service* (Mandatory Reporting Act)[33] in 2021;
- establishment of an Expert Advisory Group in 2022 to advise the Minister of Canadian Heritage on the design of a "duty to act responsibly" framework based on risk assessment and management, as well as specific duties to protect children, an independent regulator and ombudsperson, and a content review and appeals process, among other things;[34]
- 19 regional and thematic roundtable discussions led by the Minister of Canadian Heritage in 2022;[35] and
- three Canadian Citizens' Assemblies on Democratic Expression between 2020 and 2022, the last of which reviewed the work of the Expert Advisory Group and made 43 recommendations for developing a regulatory framework.[36]

PRELIMINARY VERSION
UNEDITED

On 26 February 2024, the Minister of Justice introduced in the House of Commons Bill C-63, An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts (short title: Online Harms Act).[37] The bill proposed to establish a Digital Safety Commission of Canada, the position of the Digital Safety Ombudsperson of Canada and a Digital Safety Office of Canada, providing a mandate for the Commission and the Ombudsperson to ensure the protection of the public from harmful content published on social media and to impose a duty of care on operators with regard to such content.

In addition to its online harm provisions, Bill C-63 proposed amendments to the *Criminal Code* and the *Canadian Human Rights Act* concerning hate propaganda and hate speech. It also sought to amend the Mandatory Reporting Act to clarify the services in scope, provide that notifications be sent to a designated law enforcement body, require that transmission data be reported, and extend the period of preservation of data as well as the limitation period for prosecution. The House of Commons Standing Committee on Justice and Human Rights (JUST) began a pre-study of Bill C-63 in December 2024,[38] before it died on the *Order Paper* on 6 January 2025.

In the 45th Parliament, the *Criminal Code* provisions of Bill C-63 were partially reintroduced in the *Combatting Hate Act* (Bill C-9), which received Royal Assent on 18 June 2026 and came into force on 18 July 2026. Certain child protection measures proposed in Bill C-63, including amendments to the Mandatory Reporting Act, were incorporated into the *Protecting Victims Act* (Bill C-16), which received Royal Assent on 18 June 2026, with most of its provisions in force as of 18 July 2026.

On 12 March 2026, the Minister of Canadian Identity and Culture and Minister responsible for Official Languages reconvened the Expert Advisory Group on online safety, seeking its advice on new issues arising from technological changes, including the advent of AI chatbots and companions as well as other online trends.[39]

1.3.2 Parliamentary Studies

During the same period, a number of parliamentary committees undertook studies and made recommendations for regulating online platforms in the following reports:

- House of Commons Standing Committee on Justice and Human Rights (JUST), *Taking Action to End Online Hate* (2019);[40]
- House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Ensuring the Protection of Privacy and Reputation on Platforms such as Pornhub* (2021);[41]

- House of Commons Standing Committee on Public Safety and National Security, *The Rise of Ideologically Motivated Violent Extremism in Canada* (2022);[42]
- Standing Senate Committee on Human Rights (RIDR), *Combatting Hate: Islamophobia and its Impact on Muslims in Canada* (2023);[43]
- JUST, *Islamophobia on the Rise: Taking Action, Confronting Hate and Protecting Civil Liberties Together* (2024);[44]
- JUST, *Heightened Antisemitism in Canada and How to Confront It* (2024);[45]
- ETHI, *Oversight of Social Media Platforms: Ensuring Privacy and Safety Online* (2024);[46]
- House of Commons Standing Committee on Canadian Heritage (CHPC), *Harms Caused by Illegal Sexually Explicit Material Online* (2024);[47]
- House of Commons Standing Committee on the Status of Women, *Confronting Antifeminist Ideologies in Canada* (2026);[48]
- CHPC, *The Effects of Influencers and Social Media Content on Children and Adolescents* (2026);[49]
- RIDR, *Standing United Against Antisemitism: Protecting Communities and Strengthening Canadian Democracy* (2026);[50] and
- Standing Senate Committee on Social Affairs, Science and Technology, *Fuelled by Technology, Powered by Humanity: An interim report on a human-centred approach to AI in Canada* (2026).[51]

Parliament has also considered age-assurance measures aimed at limiting minors' access to online pornographic content. In the 44th Parliament, Bill S-210, An Act to restrict young persons' online access to sexually explicit material,[52] a Senate public bill, proposed requiring commercial providers of sexually explicit material to implement age-verification measures and created an enforcement regime for non-compliance. That bill was studied in both chambers but died on the *Order Paper* in June 2024. In the 45th Parliament, a similar framework was introduced as Bill S-209, An Act to restrict young persons' online access to pornographic material,[53] which retains the same objective but enables age-verification or age-estimation approaches. Bill S-209 was studied by the Standing Senate Committee on Legal and Constitutional Affairs, passed third reading in the Senate, and received first reading in the House of Commons on 30 April 2026.

PRELIMINARY VERSION
UNEDITED

2 DESCRIPTION AND ANALYSIS

Bill C-34 has four clauses and is divided into two main parts, respectively enacting the Digital Safety Act and the Digital Safety Commission of Canada Act.

This legislative summary touches on the most important aspects of Bill C-34 without listing every provision.

2.1 PART 1: DIGITAL SAFETY ACT

Bill C-34 establishes the Digital Safety Act in clause 2, which sets out obligations for social media service and chatbot service operators to reduce exposure to seven categories of harmful content, to block certain types of content in Canada, and to disclose the steps they are taking to protect users from harmful content.

The Digital Safety Act contains 130 sections, divided into seven parts. Its general purposes are to

- promote online safety;
- protect children's physical and mental health;
- mitigate the risk of exposure to harmful content while respecting freedom of expression;
- enable persons in Canada to participate in public discourse and exercise their freedom of expression, without interference from harmful content;
- reduce the risk of harm from the use of chatbot services;
- block content that sexually victimizes a child or revictimizes a survivor, as well as non-consensual intimate content;
- ensure that platforms and services are transparent and accountable with respect to their duties under the Act; and
- contribute to the development of online safety standards.

2.1.1 Interpretation and Application (Sections 2 to 12 of the Digital Safety Act)

Section 2 of the Digital Safety Act sets out definitions relevant to the Act. "Harmful content" is defined as:

- intimate or sexual content, including deepfakes generated by AI, where the person had a reasonable expectation of privacy at the time the content was made, and the content is posted or shared without the person's consent;

PRELIMINARY VERSION
UNEDITED

- content that sexually victimizes a child (child pornography) or identifies a survivor/victim of child pornography and links them to the content in which they were a victim of child pornography, with certain exceptions;
- content that advocates or counsels a child to harm themselves, including through disordered eating or suicide;
- content used to bully a child, where content intended to threaten, intimidate or humiliate a child could seriously harm their physical or mental health;
- content that fuels hatred by expressing detestation or vilification of an individual or group based on a prohibited ground of discrimination;
- content that encourages or threatens physical violence, and that could cause a person to seriously harm or endanger another person, or seriously interfere with or disrupt an essential service, facility or system; and
- content that incites violent extremism or terrorism by encouraging or threatening terrorism or violent extremism; recruiting or training a person to facilitate, commit or materially support acts of terrorism or violent extremism; or promoting such acts in a way that could be expected to encourage others to facilitate or commit them.

For the purposes of the Digital Safety Act, a "social media service" is defined as a website or application accessible in Canada, whose primary purpose is to facilitate interprovincial or international online communication between users who access and share content using the website or application. This could include social media platforms, live-streaming services, and adult content services. Section 10 specifies that a service where users cannot communicate content to the public is not a social media service.

A "chatbot service" means an AI system that communicates over the Internet and is available on a website or application accessible in Canada, that provides humanlike responses to user inputs using a natural language interface, that can be used to "simulate a sustained human-life relationship with a user," and that generates content or responses "not fully predetermined" by the developer or operator of the system.

An "online service" means a website or application other than a social media or chatbot service that is accessible over the Internet in Canada and allows users to interact with it.

A "regulated service" means a regulated social media service, a regulated chatbot service or a regulated online service with a certain number of users, as determined by regulation (see sections 6, 7 and 8 respectively). Different regulations may apply based on the number of users, with smaller services not required to meet the same obligations under the Act (sections 6(2), 7(2) and 8(2)). Regulations may also target

a particular social media service, regardless of size, if the Governor in Council determines that there is a significant risk that harmful content is accessible on the service (sections 6(3), 7(3) and 8(3)).

Section 5 authorizes the Governor in Council to make regulations establishing further categories of online service, on the recommendation of the Commission, if the Governor in Council is satisfied that online services within the category pose a significant risk of harm to children in Canada.

Section 11 specifies that the private messaging features of any regulated social media services or regulated online services are exempt from the duties imposed by the Act.

Under section 2 of the Act, a "person" includes a corporation and a trust, a partnership, a fund, a joint venture and any another unincorporated group. An "operator" is a person that operates a regulated service. Operators are not required to proactively search for harmful content but may be required to use technological means to prevent users from uploading content that sexually victimizes a child or revictimizes a survivor (section 12).

2.1.2 Digital Safety Commission of Canada (Sections 15 to 19 of the Digital Safety Act)

Section 15 of the Digital Safety Act mandates the Commission to promote online safety in Canada and reduce harms caused by certain online content by:

- administering and enforcing the Digital Safety Act;
- ensuring that regulated service operators are transparent and held accountable under the Act;
- investigating complaints related to content that sexually victimizes a child or revictimizes a survivor, or intimate content shared without consent;
- promoting research and education related to the development of online safety standards;
- facilitating the participation of Indigenous peoples, official language minority communities and other interested persons in the Commission's activities;
- collaborating with operators, individuals with professional, technical or specialized knowledge, the Commission's international counterparts and other experts and professionals;
- supporting users of regulated services;
- advocating for the public interest in relation to systemic online safety issues;

PRELIMINARY VERSION
UNEDITED

- gathering information on issues related to online safety and harmful content, for instance from users of regulated services and victims of harmful content; and
- directing users to resources to address their concerns regarding online safety, including resources provided for by the Digital Safety Act.

The Commission has the power to make regulations and issue guidelines and codes of conduct for regulated services (section 16). The Commission must also issue guidelines on the circumstances and manner in which operators should share information with the Royal Canadian Mounted Police (RCMP) (section 17).

Section 18 requires the Commission to take into account freedom of expression, equality rights, privacy rights,[54] the needs and perspectives of the Indigenous peoples of Canada and any other factor the Commission considers relevant, when making regulations and issuing guidelines, codes of conduct and other documents.[55] The Commission must also hold hearings or make reports on any issue within its mandate when requested by the Governor in Council (section 19).

2.1.3 Duties of Operators (Sections 20 to 59 of the Digital Safety Act)

The Digital Safety Act also sets out duties for operators of regulated services (sections 20 to 25), regulated social media services (sections 26 to 47), regulated chatbot services (sections 48 to 58), and regulated online services (section 59). These include:

- the duty to protect children;
- the duty to act responsibly;
- the duty to be transparent; and
- the duty to make certain content inaccessible.

2.1.3.1 Duty to Protect Children (Sections 20 to 24 and 26 to 30 of the Digital Safety Act)

The duty to protect children requires operators of regulated services to ensure their site integrates design features related to the protection of children (section 21), as provided by regulation. In addition, operators who have reasonable grounds to suspect that a regulated service provides access to pornographic content must implement age-verification or age-estimation measures designed to mitigate the risk that children will be exposed to it (section 22(1)). The Commission must be satisfied that any such measures are effective, limit the collection of personal information to that required for age assurance, and make adequate provisions for its protection and destruction (section 22(2)). Section 22(3) clarifies that operators are not required

PRELIMINARY VERSION
UNEDITED

under section 22(1) to implement measures that "unreasonably or disproportionately" limit users' expression.

Operators must also implement any measures provided by regulation to mitigate the risk of children's exposure to pornographic content (section 23).

Regulated social media services specified by Governor in Council (section 27(5)) are required to implement age-verification or age-estimation measures (section 27(1)), as well as other measures determined by regulation (section 28), to prevent persons under 16 from registering or holding an account with the service. The same standards and qualifications apply to these measures (sections 27(2) and 27(3)) as to those required under section 22. Section 29 allows a social media service to be exempted from these obligations where the Commission determines that the service provides adequate safeguards for the protection of children.

2.1.3.2 Duty to Act Responsibly (Sections 31 to 41 and 48 to 57 of the Digital Safety Act)

The duty to act responsibly requires operators of regulated social media services (sections 31 to 41) and regulated chatbot services (sections 48 to 57) to reduce the risk that users will be exposed to harmful content or harmful behaviours on their services. These include measures that are initiated by the operator (sections 32 and 49) as well as measures required by regulation (sections 33 and 50).

In the case of social media services, the Commission determines whether these measures are adequate by considering their effectiveness, the number of users of the service, the operator's technical and financial capacity, whether the measures are discriminatory based on a prohibited ground, and other factors (section 32(2)).

Regulated chatbot services are also required to implement measures, both initiated by the operator (section 51) and provided for by regulation (section 52), for crisis intervention where users express suicidal ideation or intentions to harm themselves or others. Section 51 specifies that such measures must entail the interruption of the interaction between user and chatbot and the direction of the user towards appropriate and available crisis intervention services permitting the user to interact with a human being.

Regulated chatbot services must also implement measures, both self-initiated (section 53) and provided by regulation (section 54), to mitigate the risk that the chatbot will engage in harmful behaviours, including:

- posing as a human being or otherwise being deceptive about its nature (i.e., in a way that could lead a user to mistake it for a human being);
- posing and giving advice as a medical, legal or other licensed professional;

PRELIMINARY VERSION
UNEDITED

- using techniques to manipulate a user into forming or maintaining an emotional attachment to the service;
- encouraging self-harm, suicide or acts that could cause death or serious bodily harm; or
- other behaviours specified by regulation.

Operators of regulated social media services must publish user guidelines that describe the risk mitigation measures implemented and a standard of conduct for users with respect to harmful content (section 34). For regulated chatbot services, these guidelines must also explain how the operator will mitigate the risk that the services will communicate harmful content or engage in the harmful behaviours described in section 53, and address situations in which users express suicidal ideation or intentions to harm themselves or others (section 55).

Operators of regulated social media services must provide users with tools to block other users (section 35). They must also implement tools and processes enabling users to flag to the operator any harmful content accessible on the service. The operator must then notify the user who flagged the content and the user who posted the content as to whether any measures were taken in response (section 36).

For regulated chatbot services, under section 56, operators must enable users to flag the communication of harmful content by the service, any failure on the part of the operator to address situations where a user expresses suicidal ideation or intentions to harm themselves or others, and other types of harmful behaviour as defined in section 53.

Section 37 requires operators of regulated social media services to implement adequate measures to label certain kinds of synthetic content, as determined by regulation. These include measures initiated by the operator (section 37) as well as determined by regulation (section 38). The Commission determines whether these measures are adequate by considering their effectiveness in labelling synthetic content and avoiding incorrect labelling, the technical feasibility of identifying synthetic content on the service, the size of the service, the technical and financial capacity of the operator, and other factors as provided by regulation (section 37(2)).

Operators of regulated social media services must also label harmful but legal content where they have reasonable grounds to believe it has been subject to multiple instances of automated communication by third-party computer programs and is more prominent on the service as a result (section 39).

Operators of regulated social media services and regulated chatbot services must ensure that a resource person is available to receive user concerns about harmful

PRELIMINARY VERSION
UNEDITED

content and behaviours, direct users to internal and external resources and provide guidance with respect to internal resources (sections 40 and 57).

Section 41 requires social media operators to preserve terrorism or violent extremism content or content inciting violence for one year following the day on which the content was made inaccessible, as well as its destruction thereafter, unless the content was never made accessible on the service.

2.1.3.3 Duty to Be Transparent (Sections 25, 42, 58 and 59 of the Digital Safety Act)

Under the duty to be transparent, operators of regulated social media services, regulated chatbot services and regulated online services must periodically[56] publish and submit a digital safety plan to the Commission for each regulated service they operate (sections 42, 58 and 59 respectively). Operators of regulated services must keep any records needed to show whether the operator is complying with the Act (section 25).

Section 59 sets out that all digital safety plans must include:

- information respecting the manner in which the operator complies with the duty to protect children (section 21), including a description of design features, the operator's assessment of their effectiveness and the indicators used to assess their effectiveness;
- information on compliance with section 22(1), or the mitigation of the risk that children will be exposed to pornographic content, as well as regulations pertaining thereto;
- information on any additional child-protection measures;
- information respecting the criteria and processes used to determine whether to notify law enforcement of certain content, as well as information on any such notifications made;
- information on the resources allocated to compliance with the duty to protect children (sections 21 to 23), including those allocated to automated decision making;
- information on measures implemented to comply with duties under the Mandatory Reporting Act;
- an inventory of data used to prepare the plan; and
- any other information provided for by regulation.

PRELIMINARY VERSION
UNEDITED

In addition to the requirements above, section 42 sets out that regulated social media services must provide:

- a risk assessment relating to user exposure to harmful content on the service;
- a description of measures implemented to mitigate those risks, the effectiveness of these measures and the factors considered when assessing effectiveness;
- information respecting the manner in which the operator complies with the duty to prevent children under 16 from holding an account with the service, as well as regulations pertaining thereto;
- information respecting measures such as guidelines, blocking and flagging mechanisms, and labelling of synthetic and automated content, as well as the availability of a resource person;
- information on the resources allocated to compliance with the duty to prevent children under 16 from holding an account with the service, as well as the duty to act responsibly;
- information on the volume and type of harmful content accessible on the service and on the manner and timing of moderation;
- information on the number of times users flagged various types of harmful content on the site, how the operator assessed the flags, and the manner and timing of the operator's response to user flags;
- information related to the type and volume of content, other than harmful content, that the operator moderated based on a belief that the content posed a risk of significant physical or psychological harm, including how and when the operator moderated the content;
- information on concerns received by the resource person referred to in section 40(1) and the resources to which users were directed; and
- information on research conducted by or for the operator on harmful content as well as other content and design features posing risks of significant psychological or physical harm.

In addition to the requirements imposed on regulated online services (section 59), section 58 indicates that regulated chatbot services must provide:

- a risk assessment related to the communication of harmful content by the service, or harmful behaviour on the part of the service;
- a description of measures implemented to mitigate these risks, the effectiveness of the measures and the factors considered when assessing effectiveness;
- information on the resources allocated to compliance with the duty to act responsibly, as defined in sections 49 to 57;

PRELIMINARY VERSION
UNEDITED

- information on the number of times users flagged harmful content or behaviour, as well as the manner and timing of measures taken to assess and respond to the flags;
- information on concerns received by the resource person and the resources to which users were directed; and
- information on research conducted by or for the operator on harmful content communicated by the service, harmful behaviour engaged in by the service, and other content, behaviour and design features posing a risk of psychological or physical harm.

Regulated services must ensure that digital safety plans do not contain personal information, information that must not be disclosed under the Mandatory Reporting Act, or information prejudicial to criminal investigations. The public version of the digital safety plan need not contain an inventory of the data used to prepare the plan, trade secrets, or other confidential commercial, scientific or technical information (sections 42(2) to 42(6), 58(2) to 58(6), and 59(2) to 59(6)).

2.1.3.4 Duty to Make Certain Content Inaccessible (Sections 43 to 47 of the Digital Safety Act)

An operator of a regulated social media service must block content on their site where there are reasonable grounds to suspect that the content sexually victimizes a child or revictimizes a survivor, or is intimate content shared without consent. Access to the content must be blocked in Canada within 24 hours of the operator or a user flagging the content as prohibited (sections 43 and 44). An operator is not required to block content flagged by a user where the operator determines the flag is trivial, frivolous, vexatious, made in bad faith or has already been investigated and found to be acceptable (section 44).

If the operator blocks the content, the operator must notify both the user who posted or shared the content and the user who flagged the content, if applicable (section 44(4)). Either user may appeal the operator's decision and make submissions to the operator as to whether the content falls in the category of forbidden content under the Act. The operator must then review the initial decision to block the content (section 45). Upon being notified of the reviewed decision, either user may resubmit arguments and ask the operator to reconsider the decision to block the disputed content a second and final time (section 46). The timelines for this process will be set out in regulation.

PRELIMINARY VERSION
UNEDITED

2.1.4 Access to Inventories and Electronic Data (Sections 60 to 64 of the Digital Safety Act)

Section 60 of the Digital Safety Act sets out a procedure by which persons[57] conducting research or education activities can be accredited by the Commission to receive access to the electronic data inventories included in digital safety plans submitted under the Act. It also provides regulation-making authority for the establishment of further criteria in the accreditation of such persons. That accreditation can also be suspended or revoked if the Commission determines that a person fails to comply with certain provisions of the Act.

Section 61 of the Act empowers the Commission to make orders requiring the operator of a regulated service to provide access to electronic data upon request of an accredited person for a research project related to the purposes of the Act.[58] It also requires that operators not disclose any information prejudicial to criminal investigations in complying with such an order. Section 62 of the Act further provides that such an order can be amended or revoked if compliance would cause the operator to suffer undue hardship.

Accredited persons who request that the Commission make an order under section 61 may make a complaint to the Commission under section 63 of the Act if the subject of that order failed to comply with the order.

Under section 64 of the Act, the Commission may publish a list of persons accredited to conduct research and education activities under section 60 and a description of research projects subject to an order under section 61.

2.1.5 Remedies (Sections 65 to 72 of the Digital Safety Act)

Sections 65 to 67 of the Act govern the making of public submissions to the Commission respecting harmful content or behaviour, or measures taken by an operator to comply with the Act. Under section 65, these submissions may be on harmful content, harmful behaviour engaged in by a regulated chatbot, or how operators comply with their duties under the Act. These submissions may be communicated to an operator or made public (sections 65(2) and 65(3)). Sections 66 and 67 manage the confidentiality requirements surrounding these submissions.

Sections 68 to 72 of the Act put in place procedures for making and handling complaints to the Commission respecting content that "sexually victimizes a child or revictimizes a survivor or intimate content communicated without consent." Section 68 provides that this recourse is only available after the procedures under sections 44 and 46 have been exhausted, and that the Commission can either dismiss the complaint or make an order requiring the content be made inaccessible.

PRELIMINARY VERSION
UNEDITED

2.1.6 Administration and Enforcement (Sections 73 to 112 of the Digital Safety Act)

Sections 73 to 112 of the Digital Safety Act set out the powers of the Commission to ensure compliance with the Act. Subject to any additional rules it may make for itself under the Digital Safety Commission of Canada Act, the Commission can summon witnesses and require them to provide testimony in the same way as a superior court. It may also administer oaths and make decisions on questions of procedure and evidence. The Commission is not required to follow any legal or technical rules of evidence, allowing it to receive evidence that would not be admissible in a court of law. Its only requirements are to deal with matters as quickly and as informally as possible, while ensuring fairness and following the principles of natural justice (sections 73 and 74).

The Commission may hold hearings in any manner it sees fit. Hearings are to be public unless the Commission considers that a private setting would be more appropriate, after weighing the public interest and privacy or confidentiality considerations (sections 75 and 76).

The Commission may designate inspectors responsible for ensuring compliance with the Act (section 77). Inspectors may enter, physically or electronically and either with the occupant's consent or under the authority of a warrant issued by a justice of the peace, any place to confirm compliance or prevent non-compliance. Inspectors may not use force unless specifically authorized by a warrant and accompanied by a peace officer (section 79(3)).

The Commission may issue an order itself directly, or through the authority of the Federal Court. to prevent an operator from contravening the Act (sections 81 and 82).

In the event of contraventions to its provisions or regulations, the Digital Safety Act sets out two distinct ways to proceed: an administrative monetary penalties (AMP) regime, and an offences track.

The offences track (sections 107 to 110) is narrower than the AMP regime, applying to operators who contravene an order by the Commission, fail to follow an undertaking or requirements imposed by the Commission, or otherwise obstruct or make false or misleading statements to the Commission.

Any of these acts or omissions may also be proceeded with as a violation under the AMP regime, but a proceeding under one prevents a proceeding under the other (section 103). Maximum penalties (fines) are outlined in section 107 for operators and section 108 for non-operators and vary depending on whether the offence is proceeding by way of indictment of summary conviction, and whether the offender is an individual. Maximum fines are to be the greater of a set amount or a set percentage

PRELIMINARY VERSION
UNEDITED

of gross global revenue, which will be calculated in accordance with regulations to be established under section 112. The highest maximum fine provided under these sections is 5% of gross global revenue or $20 million, in the case of an operator, who is not an individual, convicted on indictment.

Non-operators commit an offence if they fail to assist an inspector in fulfilling their duties, or if they do not provide a document or information that is requested by an inspector (section 108). Failure to pay a fine ordered under the Act may not be punished by imprisonment (section 111).

The AMP regime (sections 83 to 106) applies, in the case of operators, to any act or omission that may be proceeded with under the criminal offences track, in addition to more broadly applying to any provision of the Act or its regulations, and specifically to an operator who fails to provide information or access requested by an inspector.

This regime also applies to a person who operates a service that is not regulated (meaning that the person does not meet the definition of "operator") if they fail in their duty to provide information, contravene a requirement imposed by an inspector, or otherwise obstruct, or make false or misleading statements to the Commission (section 83(2)). A service would not be a "regulated service" if it does not meet the user threshold established under section 6 and is not designated by regulation.

Maximum penalties are set in section 88. Section 89 outlines the factors to be considered in determining the penalty, although additional factors may be added through regulations made under section 112(c). Each day on which a violation is committed is considered a separate violation (section 84).

Section 85 explains that penalties imposed under this regime are not meant to punish, but rather to encourage compliance. Sections 93 to 96 outline the procedure for entering into an undertaking with the Commission to address any act or omission.

2.1.7 Protections, Reports and Information Sharing (Sections 113 to 124 of the Digital Safety Act)

Sections 113 to 116 of the Digital Safety Act include legal protections for various types of persons and information. For example, section 113 provides that, in specified cases, persons acting on behalf of the Commission are not competent to act as a witness in certain types of legal proceedings. Section 114 of the Act empowers persons to designate some types of information submitted to the Commission as confidential, including trade secrets and confidential technical or commercial information. Any such confidential information can only be disclosed by the Commission if disclosure is in the public interest (section 114(5)). Section 115 of

PRELIMINARY VERSION
UNEDITED

the Act creates a summary conviction offence for the disclosure of confidential information, punishable by a fine of up to $5,000 for a first offence.

Sections 117 to 119 of the Act set out the details of the Commission's reports to the Minister,[59] including requirements for the content of annual reports and the provision of additional reports by request of the Minister.

The Commission may work with federal departments and agencies to support the implementation of the Act under the conditions set out in section 120. Under sections 121 to 123 of the Act, the Commission must consult with the Canadian Radio-television and Telecommunications Commission, the Privacy Commissioner[60] and the RCMP on various responsibilities under the Act. Section 124 also empowers the Commission to provide certain information to the Minister or any person designated by the Minister to support the making of regulations under the Act and to ensure that both the Act and its regulations "are effective and up to date."

2.1.8 Regulations
(Sections 126 and 127 of the Digital Safety Act)

The Commission is granted regulation-making authority on a broad range of enumerated subjects related to the Act under section 126. The Governor in Council is also empowered to make regulations on certain enumerated subjects listed under section 127.

2.1.9 Reviews by Minister
(Sections 128 and 129 of the Digital Safety Act)

Section 128 of the Act provides for periodic reviews of the Act as a whole by the Minister by the third anniversary of the coming into force of this section of the Act and every five years after that. These reports must be tabled before the Senate and House of Commons.

Section 129 of the Act provides for a review of sections 27 to 29 specifically on the third anniversary of the coming into force of this section of the Act. Sections 27 to 29 relate to the obligation imposed on operators to implement measures to ensure that users of a regulated social media service are of a minimum age to be able to have an account.

2.1.10 Coming into Force
(Section 130 of the Digital Safety Act)

Section 130 of the Act provides that the Act shall come into force on a day or days to be fixed by order of the Governor in Council.

PRELIMINARY VERSION
UNEDITED

2.1.11 Coordinating Amendment (Clause 3 of Bill C-34)

Clause 3 of Part 1 of Bill C-34 coordinates the text of several provisions of the Act in the event that Bill C-16, An Act to amend certain Acts in relation to criminal and correctional matters (child protection, gender-based violence, delays and other measures) receives Royal Assent before Bill C-34. On 18 June 2026, Bill C-16 received Royal Assent.

2.2 PART 2: DIGITAL SAFETY COMMISSION OF CANADA ACT

Clause 4 of Part 2 of Bill C-34 enacts An Act to Establish the Digital Safety Commission of Canada (alternative title: the Digital Safety Commission of Canada Act).[61] The Commission is composed of three to five full-time members[62] to be appointed by the Governor in Council (section 10), including the Chairperson (section 17), who hold office for renewable terms of up to five years (section 11). As a transitional provision, the Chairperson of the Commission, once designated, can exercise all the powers conferred to the Commission until there are at least two other members in office (section 23).

When there are exceptional circumstances, such as allegations related to misconduct or employee safety, the Governor in Council can suspend a member of the Commission, with pay, until the Governor in Council has decided whether to remove the member from office (section 14).

The Commission's mandate is to exercise the powers and perform the duties and functions conferred to it under the Digital Safety Act or under any other Act of Parliament (section 6). As detailed above, these powers include promoting online safety in Canada, reducing harms caused by certain online content, making regulations and issuing guidelines and codes of conduct for regulated services.[63]

Within three months of the end of each fiscal year, the Commission must submit a report to the designated Minister on its activities in that fiscal year. The Minister then has 15 sitting days to lay the report before each House of Parliament (section 21).

The Digital Safety Commission of Canada Act comes into force on a day or days to be fixed by an order of the Governor in Council (section 24).

Clauses 5 to 10 of the bill also add the Digital Safety Commission of Canada to certain lists of government institutions in the *Access to Information Act*, the *Financial Administration Act*, the *Privacy Act*, and the *Public Service Superannuation Act*.

PRELIMINARY VERSION
UNEDITED

NOTES

1. Bill C-34, An Act to enact the Digital Safety Act and the Digital Safety Commission of Canada Act and to make consequential amendments to other Acts, 45th Parliament, 1st Session.
2. See Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts, 45th Parliament, 1st Session; and Alexandra Savoie and Maxime-Olivier Thibodeau, *Legislative Summary of Bill C-36: An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts*, Preliminary version (unedited), Library of Parliament, 6 July 2026.
3. Anatoliy Gruzd and Philip Mai, *The State of Social Media in Canada 2025: A Census-balanced Survey About Social Media Adoption in Canada*, Social Media Lab, Toronto Metropolitan University.
4. Statistics Canada, "Online hate and aggression among young people in Canada," *The Daily*, 27 February 2024.
5. Laura Savage, "Online child sexual exploitation: A statistical profile of police-reported incidents in Canada, 2024," *Juristat*, Statistics Canada, 10 March 2026. Note that Cybertip.ca, Canada's national tipline for reporting the online sexual abuse and exploitation of children, received 28,453 reports from the public in 2024–2025. See Public Safety Canada, *About Online Child Sexual Exploitation*.
6. Statistics Canada, "Police-reported crime statistics in Canada, 2024 (Table 5)," *The Daily*, 22 July 2025.
7. Laura Savage, "Online child sexual exploitation: A statistical profile of police-reported incidents in Canada, 2024," *Juristat*, Statistics Canada, 10 March 2026.
8. Ibid.
9. Statistics Canada, *Online activities of Canadian youth, cybervictimization and exposure to harmful content*, 23 April 2025.
10. Ibid.
11. Women and Gender Equality Canada, *Infographic: Online violence*.
12. Adam Cotter and Marta Burczycka, "Gender differences in experiences of violence and unwanted sexual behaviour in Canada, 2025," *Juristat,* Statistics Canada, 31 March 2026.
13. Ibid.
14. Women and Gender Equality Canada, *What is the manosphere: Key terms, meanings, and why it matters*.
15. American Psychological Association, *Health advisory on social media use in adolescence*, May 2023. See also United States, Office of the Surgeon General, "Social Media Has Both Positive and Negative Impacts on Children and Adolescents," *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, 2023.
16. Dr. Anatoliy Gruzd, Philip Mai and Anthony Clements Haines, *[New Report] The State of Generative AI Use in Canada 2025: Exploring Public Attitudes and Adoption Trends*, Social Media Lab, Toronto Metropolitan University, 8 April 2025.
17. UNICEF, *When AI becomes a friend: Child rights risks, harms, and regulatory responses to AI chatbots and companions*, Policy brief, June 2026, p. 3.
18. United Kingdom, *Online Safety Act 2023*, 2023, c. 50.
19. European Union, EUR-Lex, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, in *Official Journal*, No. L 277.
20. Australia, *Enhancing Online Safety Act 2015* (No. 24, 2015); Australia, *Online Safety Act 2021* (No. 76, 2021); and Australia, *Online Safety Amendment (Social Media Minimum Age) Act 2024* (No. 127, 2024).
21. See for instance European Union, EUR-Lex, *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, in *Official Journal*, L series; and Schedule 5 and Schedule 6 of Australia's *Online Safety Act 2021*.

22. Platform liability, or "Internet intermediary liability," is a pivotal concept in debates about online harms, raising the question of whether platforms can be considered "publishers" given their reliance on algorithms to promote content to users. Some have argued that platforms do have knowledge of harmful content prior to publication based on the sophistication of these algorithms and can be considered publishers. See for instance the analysis provided in Friends of Canadian Broadcasting, *Platform for harm: Internet intermediary liability in Canadian law*, September 2020. See also *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45, paras. 89, 98, 99, 101 and 127 (in the context of the *Copyright Act*). Recently, some school boards launched lawsuits against social media operators (Caroline Alphonso, "Four Ontario school boards sue Instagram, Snapchat, TikTok owners over platforms' alleged harm to students," *The Globe and Mail*, 28 March 2024 [SUBSCRIPTION REQUIRED]).

23. *Criminal Code* (the Code), R.S.C. 1985, c. C-46.

24. In fact, the *Criminal Code* was amended in 2014 to clarify that, where an offence has an element of communication, this includes communications made by any means of telecommunication, such as the Internet (section 4(8)).

25. *Combatting Hate Act*, S.C. 2026, c. 15.

26. During his appearance before the House of Commons Standing Committee on Justice and Human Rights on Bill C-9, the Combatting Hate Act, the Minister of Justice and Attorney General of Canada, the Honourable Sean Fraser, confirmed that this legislation would equally apply on the Internet. See House of Commons, Standing Committee on Justice and Human Rights, *Evidence*, 9 October 2025.

27. In this regard, see section 320.1 of the *Criminal Code*.

28. *Protecting Canadians from Online Crime Act*, S.C. 2014, c. 31.

29. *Protecting Victims Act*, S.C. 2026, c. 19.

30. Office of the Prime Minister, Rt. Hon. Justin Trudeau, P.C., *Minister of Canadian Heritage Mandate Letter*, 13 December 2019; Office of the Prime Minister, Rt. Hon. Justin Trudeau, P.C., *Minister of Justice and Attorney General of Canada Mandate Letter*, 13 December 2019; Office of the Prime Minister, Rt. Hon. Justin Trudeau, P.C., *Minister of Canadian Heritage Mandate Letter*, 16 December 2021; and Office of the Prime Minister, Rt. Hon. Justin Trudeau, P.C., *Minister of Justice and Attorney General of Canada Supplementary Mandate Letter*, 15 January 2021.

31. Government of Canada, *Speech from the Throne*, 23 September 2020.

32. Canadian Heritage, *Technical paper*.

33. *An Act respecting the mandatory reporting of Internet child sexual abuse and exploitation material by persons who provide an Internet service*, S.C. 2011, c. 4.

34. Canadian Heritage, *Concluding Workshop Summary*.

35. Canadian Heritage, *What We Heard: 2022 Roundtables on Online Safety*.

36. 3rd Canadian Citizens' Assembly on Democratic Expression, *Canadian Citizens' Assembly on Democratic Expression: Recommendations for reducing online harms and safeguarding human rights in Canada*, Public Policy Forum, September 2022.

37. Bill C-63, An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts, 44th Parliament, 1st Session.

38. House of Commons, Standing Committee on Justice and Human Rights, *Subject Matter of Bill C-63, An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts*, 44th Parliament, 1st Session.

39. Canadian Heritage, *Government of Canada reconvenes the expert advisory group on online safety*, News release, 12 March 2026.

40. House of Commons, Standing Committee on Justice and Human Rights, *Taking Action to End Online Hate*, Twenty-ninth report, June 2019.

41. House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Ensuring the Protection of Privacy and Reputation on Platforms such as Pornhub*, Third report, June 2021.

42. House of Commons, Standing Committee on Public Safety and National Security, *The Rise of Ideologically Motivated Violent Extremism in Canada*, Sixth report, June 2022.

43. Senate, Standing Committee on Human Rights, *Combatting Hate: Islamophobia and its Impact on Muslims in Canada*, November 2023.

44. House of Commons, Standing Committee on Justice and Human Rights, *Islamophobia on the Rise: Taking Action, Confronting Hate and Protecting Civil Liberties Together*, Twenty-sixth report, December 2024.

45. House of Commons, Standing Committee on Justice and Human Rights, *Heightened Antisemitism in Canada and How to Confront It*, Twenty-seventh report, December 2024.

46. House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Oversight of Social Media Platforms: Ensuring Privacy and Safety Online*, Sixteenth report, December 2024.

47. House of Commons, Standing Committee on Canadian Heritage, *Harms Caused by Illegal Sexually Explicit Material Online*, Fourteenth report, November 2024.

48. House of Commons, Standing Committee on the Status of Women, *Confronting Antifeminist Ideologies in Canada*, Sixth report, June 2026.

49. House of Commons, Standing Committee on Canadian Heritage, *The Effects of Influencers and Social Media Content on Children and Adolescents*, Eighth report, June 2026.

50. Senate, Standing Committee on Human Rights, *Standing United Against Antisemitism: Protecting Communities and Strengthening Canadian Democracy*, April 2026.

51. Senate, Standing Committee on Social Affairs, Science and Technology, *Fuelled by Technology, Powered by Humanity: An interim report on a human-centred approach to AI in Canada*, June 2026.

52. Bill S-210, An Act to restrict young persons' online access to sexually explicit material, 44th Parliament, 1st Session. A substantially similar bill was previously introduced as Bill S-203, An Act to restrict young persons' online access to sexually explicit material, 43rd Parliament, 2nd Session.

53. Bill S-209, An Act to restrict young persons' online access to pornographic material, 45th Parliament, 1st Session. For additional information see Dana Phillips, *Legislative Summary of Bill S-209: An Act to restrict young persons' online access to pornographic material*, Preliminary version (unedited), Library of Parliament, 21 May 2026.

54. Clause 17 of Bill C-36 would add to privacy rights, in section 18, "and, to the extent it considers appropriate, the purpose of the *Protecting Privacy and Consumer Data Act*."

55. It is worth noting that age verification and age estimation measures have raised certain concerns for stakeholders around privacy and equal access. In *Age Assurance – Policy Note* (2026), the Office of the Privacy Commissioner of Canada observes that age assurance may require collection and processing of identity documents, facial images and other personal information, potentially exposing individuals to data breaches, profiling and tracking in ways that could disproportionately impact some groups. The Privacy Commissioner also notes, in *Designing age assurance to be privacy-protective – Guidance for age assurance developers*, that facial age-estimation systems may be less accurate depending on skin tone and gender identity, and that verification techniques requiring government-issued documents may not recognize Indigenous-government credentials and may also unduly impact groups such as unhoused people, newcomers, and people using shared or public devices.

    It has also been noted that the social media age restriction could raise concerns about expression. In France, on 14 August 2026, the Constitutional Council struck down a ban on social media for children under 15, saying it infringes freedom of expression and communication for under-15s (France, Conseil constitutionnel, *Décision n° 2026-911 DC du 14 août 2026: Loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux*, 14 August 2026). Such a ban can also impact youth who rely on online spaces for information, community, and support: in *Drawing a line in digital spaces: Age-based restriction of social media* (2025), UNICEF notes that age restrictions can limit access to educational and health information and impact "children in rural or disadvantaged settings and children most discriminated against who rely on social media for resources and opportunities," while also redirecting young users to less regulated spaces.

56. As provided for in the regulations (sections 42, 58 and 59).

PRELIMINARY VERSION
UNEDITED

57. The term “person” is defined in section 2(1) of the Digital Safety Act. A person “includes a corporation and a trust, a partnership, a fund, a joint venture and any other unincorporated association or organization.”

58. The purposes of the Digital Safety Act are set out at section 14, and include the promotion of safety and the protection of children’s physical and mental health.

59. The term “Minister” is defined in section 2(1) of the Digital Safety Act. The Minister “means the member of the King’s Privy Council for Canada designated under section 13 or, if no member is designated, the Minister of Canadian Heritage.”

60. Clause 18 of Bill C-36 would repeal section 122 of the Digital Safety Act, which requires the Commission and the Privacy Commissioner of Canada to consult with each other. Clause 18 requires the Commission to consult the Privacy Commissioner before issuing guidelines, including those relating to age-verification and age-estimation measures, or making regulations, and to take their recommendations into account.

61. Note that clauses 8 and 9 of Bill C-36 would amend the long and alternative titles of the Digital Safety Commission of Canada Act by adding “and Data Protection” after “Digital Safety” and before “Commission of Canada” and by making the Commission responsible for enforcing the Protecting Privacy and Consumer Data Act as well as the Digital Safety Act.

62. Clause 13 of Bill C-36 would amend section 10 of the Digital Safety Commission of Canada Act so that the Commission consists of five full-time members.

63. Clause 12 of Bill C-36 would add a new section 6(1.1), providing that the Commission exercise the powers and perform the duties and functions conferred on it under the Protecting Privacy and Consumer Data Act.