LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

PRELIMINARY VERSION

UNEDITED

Legislative Summary

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

44-1-C63-E

20 March 2024

Mahdi Benmoussa, Isabelle Chénier, Michaela Keenan-Pelletier, Robert Mason, Moly Robichaud, Liane Tanguay, Dominique Valiquet and Julian Walker

Research and Education

AUTHORSHIP

20 March 2024	Mahdi Benmoussa	Economics, Resources and Environment
	Isabelle Chénier	Legal, Social and Indigenous Affairs
	Michaela Keenan-Pelletier	Legal, Social and Indigenous Affairs
	Robert Mason	International Affairs and Integrated Reference Services
	Moly Robichaud	Legal, Social and Indigenous Affairs
	Liane Tanguay	Economics, Resources and Environment
	Dominique Valiquet	Legal, Social and Indigenous Affairs
	Julian Walker	Economics, Resources and Environment

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 Research and Education, 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**.

Legislative Summary of Bill C-63
(Preliminary version)

44-1-C63-E

Ce document est également publié en français.

CONTENTS

LEGISLATIVE SUMMARY 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

1 BACKGROUND

1.1 BRIEF OVERVIEW OF BILL C-63

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),[1] was introduced in the House of Commons on 26 February 2024 by the Honourable Arif Virani, Minister of Justice. The bill is divided into four main parts.[2]

In Part 1, Bill C-63 establishes the Digital Safety Commission of Canada, the position of the Digital Safety Ombudsperson of Canada and the Digital Safety Office of Canada. It provides a mandate for the Commission and the Ombudsperson to ensure the protection of the public from harmful content published on social media and to ensure that operators of this type of service have a duty with regard to content. It establishes duties for operators of social media services, which are required to (i) be accountable for some of their business practices through reports; (ii) be accountable for the use they make or that third parties make of technical tools they make available to Canadians via access to research data; and (iii) mitigate the risks associated with exposing Canadian users to certain types of harmful content.

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

- content that foments hatred;
- content that incites violence;
- content that incites violent extremism or terrorism;
- intimate content communicated without consent;

- content that induces a child to harm themselves;
- content that sexually victimizes a child or revictimizes a survivor; and
- content used to bully a child.

Part 2 of Bill C-63 creates a new hate crime offence in the *Criminal Code*[3] (the Code), introducing a legislative definition of "hatred" in the Code and increasing the maximum sentences for the hate propaganda offences. Furthermore, the bill amends various provisions of the Code to ensure that a person may apply for a court order if they have reasonable grounds to believe that another person is committing a hate propaganda or hate crime offence.

Part 3 of Bill C-63 introduces a legislative definition of hate speech in the *Canadian Human Rights Act* (CHRA).[4] This Act is also amended in order to reintroduce a transformed version of former section 13, seeking to give victims of hate speech civil remedy through the Canadian Human Rights Commission. The Commission is given the power to commence legal proceedings before the Canadian Human Rights Tribunal or to impose remedies against persons who communicate or cause to be communicated "hate speech by means of the Internet or any other means of telecommunication."

In Part 4, Bill C-63 amends the *Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service* (Mandatory Reporting Act)[5] 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.

1.2 ONLINE HARMS IN CANADA

Social media platforms have facilitated communication and connectivity on a global scale. At the same time, they have enabled the spread of a range of harmful content that can pose significant threats to individual well-being, to public safety and even to the integrity of democratic institutions. Attempts to address online harms through legislation have gained traction in recent years, with the United Kingdom (U.K.), the European Union (EU), and Australia, among other jurisdictions, enacting or advancing legislative frameworks to impose certain legal responsibilities upon online service platforms.

In Canada, some 94% of adults have at least one social media account.[6] 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. The same year, in 2022, the Uniform Crime Reporting Survey reported 219 cyber-related hate crimes, up from 92 reported incidents in 2018.[7] Additionally:

- between 2014 and 2022, police reported 15,630 incidents of online sexual offences against children, and 45,816 instances of child pornography;[8]
- in 2022, police in Canada received 2,524 reports of non-consensual distribution of intimate images online;[9] and
- a 2020 study by the U.K.-based Institute for Strategic Dialogue found Canadians were sharing white supremacist, misogynistic and other radical content in more than 6,600 online channels, and that Canadians were proportionally more active in such channels than American and British users.[10]

The COVID-19 pandemic precipitated an increase in online harms of various kinds, including hate and harassment. In 2020, a *New York Times* investigation revealed an "infestation" of child sexual abuse material on Pornhub and similar platforms.[11] The attack at the Centre Culturel Islamique du Québec in 2017 and the Toronto van attack of 2018, as well as other high-profile incidents,[12] have demonstrated the real-world effects of hateful and extremist content originating online.

1.3 THE PATH TO BILL C-63

1.3.1 Developing a Framework

The Government of Canada articulated its commitment to regulating online platforms in respect of harmful content in the 2019 and 2021 mandate letters for the Minister of Canadian Heritage and the Minister of Justice, as well as the 2020 Speech from the Throne.

On 23 June 2021, then Minister of Justice, the Honourable David Lametti, tabled Bill C-36, An Act to amend the Criminal Code and the Canadian Human Rights Act and to make related amendments to another Act.[13] The Department of Justice stated that, among other measures, the bill would amend existing legislation to define a new discriminatory practice of online hate speech and add a new definition of "hatred" to the Code.[14] When the 2nd Session of the 43rd Parliament was dissolved on 15 August 2021, Bill C-36 died on the *Order Paper*. As outlined below, parts 2 and 3 of Bill C-63 are substantially similar to former Bill C-36.[15]

In July 2021, the federal government presented a technical paper on online harms as well as a discussion guide for consultation and feedback. The technical paper proposed a legislative framework for addressing five specific types of harmful content:

- child sexual exploitation content;
- terrorist content;
- content that incites violence;
- hate speech; and
- non-consensual sharing of intimate images.

The framework proposed imposing certain moderation obligations on online platforms with respect to such content, including an obligation to take all reasonable measures to identify harmful content and make certain content inaccessible to Canadians; to establish flagging, notice, and appeal mechanisms; and to publish clear and transparent content moderation guidelines. It would also require providers to report certain types of illegal content to law enforcement and the Canadian Security Intelligence Service.

Additionally, it proposed establishing a Digital Safety Commissioner to oversee and improve content moderation. The Commissioner would have proactive inspection powers, and providers would have to provide the Commissioner with regular reports on their content moderation procedures and activities. A Digital Recourse Council would be established to receive, review and issue decisions on complaints arising from content moderation decisions. Finally, the paper proposed amending the Mandatory Reporting Act to designate the RCMP's National Child Exploitation Crime Centre to receive reports concerning child pornography offences, and to require such reports to include transmission data.[16]

The government held public consultations on its technical paper from 29 July to 25 September 2021. Though most respondents supported the idea of a legislative and regulatory framework for addressing online harms, many were concerned about implications for freedom of expression, privacy rights and the rights of certain marginalized groups, as well as compliance with the *Canadian Charter of Rights and Freedoms* (the Charter) more generally. Respondents felt the framework's focus on content moderation was particularly problematic, as were potential requirements to report certain types of content to police or intelligence services.[17]

In March 2022, the government established an Expert Advisory Group to advise the Minister of Canadian Heritage on how to design the framework and incorporate the feedback from the consultations. The group was composed of 12 experts and

specialists on platform governance, civil liberties, tech regulation and national security. Among other things, experts recommended a risk-based approach based on a "duty to act responsibly" that would require providers to identify and assess risks posed by their service, take measures to mitigate these risks and report on their identification and mitigation tools. They also recommended:

- ensuring any framework include a specific duty to protect children;
- ensuring any framework include a broad range of services;
- establishing a regulator with robust audit and enforcement powers as well as adequate resourcing;
- requiring a content review and appeals process at the platform level;
- ensuring that historically marginalized groups be protected from unintended consequences; and
- establishing an ombudsperson independent from government, platforms and law enforcement.[18]

Between July and November 2022, the Minister of Heritage conducted 19 roundtable discussions, including 13 regional roundtables and six thematic roundtables on antisemitism, Islamophobia, anti-Black racism, anti-Asian racism, gender-based violence and Big Tech. While participants expressed overall support for the creation of an independent regulator and the risk-based approach advanced by the Expert Advisory Group, they also expressed reservations about the potential role of law enforcement in any new legislative framework. They agreed with the experts that platforms should have a special duty to protect children.[19]

Finally, the Canadian Citizens' Assemblies on Democratic Expression were held between 2020 and 2022 to examine "how the Government of Canada should regulate digital service providers to create a safe environment where Canadians can express themselves and be protected from a range of harms."[20] The third Assembly, in 2022, was empanelled by the Minister of Canadian Heritage to review the recommendations from the Expert Advisory Group and provide detailed guidance on the best approach to regulating online harms. The Assembly's final report offers 43 recommendations, including establishing an arm's-length regulator and an ombudsperson, and requiring providers to conduct a wide range of risk assessments, with particular regard to impacts on children, marginalized groups, human rights and emotional or psychological harms.[21]

1.3.2 Parliamentary Studies

During the same period, parliamentary committees conducted several relevant studies and made recommendations for regulating online platforms in respect of harmful content.

In 2019, the House of Commons Standing Committee on Justice and Human Rights conducted a study on online hate and recommended in its final report that the Government of Canada:

- formulate a definition of "hate" or "hatred" consistent with Supreme Court jurisprudence;
- develop a working group to establish a civil remedy for those who assert that their human rights have been violated under the *Canadian Human Rights Act*; and
- establish requirements for online platforms and service providers with respect to monitoring and addressing incidents of hate speech, and removing hateful content.[22]

In 2020–2021, the House of Commons Standing Committee on Access to Information, Privacy and Ethics conducted a study on the protection of privacy and reputation on platforms such as Pornhub, in light of reports of child sexual abuse material and other non-consensual content appearing on the site. In its February 2021 report, the Committee recommended that the Government of Canada:

- explore means to hold online platforms liable for failure to delete or prevent the upload of child sexual abuse material or non-consensual image distribution;
- amend sections 3 and 11 of the Mandatory Reporting Act;
- develop mechanisms for victims of non-consensual image distribution to flag content for removal; and
- create a legal framework for online providers of pornographic content in respect of illegal content.[23]

In 2022, the House of Commons Standing Committee on Public Safety and National Security conducted a study on ideologically motivated violent extremism (IMVE) in Canada and recommended that the Government of Canada:

- study the feasibility of a regulator structure to hold platforms accountable for enforcing their terms of service and which could include the creation of a Digital Safety Commissioner;
- work with platforms to encourage algorithmic transparency and reduce online use by terrorist entities;

- explore models like those of the U.K. and Australia to tackle IMVE and online hate;
- consult with law enforcement and affected communities to identify gaps in law and law enforcement regarding harmful online content.[24]

Finally, in 2023, the Standing Senate Committee on Human Rights conducted a study of Islamophobia in Canada and recommended that the Department of Justice:

- introduce amendments to create specific *Criminal Code* offences for hate-motivated crimes; and
- introduce legislation to provide a mechanism for human rights complaints similar to former section 13 of the *Canadian Human Rights Act*.[25]

1.4 OTHER JURISDICTIONS

In developing the Online Harms Act, the Government of Canada considered frameworks being developed in other jurisdictions and noted that "[in] Australia, the United Kingdom, and under the European Commission we see approaches that emphasize the importance of measures to enhance transparency and accountability of platform decision-making" and that "stress the benefits of on-regulatory mechanisms, including the creation of partnerships and the pursuance of collaboration with platforms, civil society organizations and users."[26]

France and Germany, by contrast, developed "robust requirements for social media platforms to remove broad categories of content in short time periods defined with broad definitions."[27] The French and German frameworks drew heavy criticism for their impacts upon freedom of expression, with the French law ruled unconstitutional immediately following its passage; both have now been superseded by the European *Digital Services Act* (DSA).[28]

1.4.1 European Union

In the European Union, the DSA came into force on 16 November 2022 and became fully applicable across the EU on 17 February 2024. Its key goals are to strengthen protections for users and their rights online, to establish a transparency and accountability framework for online platforms, and to foster innovation, growth and competitiveness. The obligations of different providers vary according to their role, size and impact in the online ecosystem.[29] The DSA imposes a series of obligations including, among others,

- measures to counter illegal goods, services, or content online;
- effective safeguards for users;

- a ban on certain types of targeted advertisements;
- transparency measures, including on algorithms used for recommendations; and
- obligations for very large platforms and search engines to prevent the misuse of their systems by taking risk-based action and by independent audits of their risk-management systems.[30]

Enforcement of the DSA is shared between the European Commission and Digital Service Coordinators (DSC) designated by each member state. According to the European Commission, the DSA "sets out a high standard for the independence" of DSCs, who "should remain fully independent in their decision-making and not seek instructions from their governments or other bodies, particularly online platforms."[31]

1.4.2 Germany

In Germany, the *Network Enforcement Act* (NetzDG) has regulated illegal content on social media services in Germany since 2017. Under the NetzDG, platforms with more than 2 million users are required to remove posts that are "manifestly illegal" within 24 hours, including hate speech and disinformation, and maintain an effective and transparent complaints procedure. It has seen several amendments, including one requiring platforms to forward suspected illegal content to law enforcement. The law was controversial because of its implications for freedom of expression.[32] It was superseded by the EU *Digital Services Act* on 17 February 2024.[33]

1.4.3 France

In 2020, the Law on Countering Online Hatred[34] (Avia Law) amended the 2004 *Digital Economy Law* to incorporate many elements of the NetzDG into French law. Immediately after its adoption, the law was challenged by a group of 60 senators at the Constitutional Council, the highest constitutional authority in France, and found to be unconstitutional, in particular for its restrictive takedown obligations.[35] Like Germany's law, the Avia Law was superseded by the EU *Digital Services Act*.[36]

1.4.4 United Kingdom

In the United Kingdom, the *Online Safety Act*[37] received Royal Assent on 26 October 2023. It creates a new framework and series of regulations to address illegal, harmful, and unsafe online content. It designates the Office of Communications, the U.K.'s telecommunications regulator, as the online safety regulator and covers a range of content including terrorism, racism, child sexual exploitation, suicide, eating disorders, misogyny and revenge pornography.

Broadly, the Act requires illegal content to be removed, places a legal responsibility on social media platforms to enforce their terms of service, and empowers users to filter out harmful content that they do not wish to see. Additionally, social media companies must take measures to prevent children from accessing harmful content, ensure the risks to children are more transparent, and offer ways for parents and children to report problems that do arise.[38]

As of 1 April 2024, most of the Act's provisions are in force.[39]

1.4.5 Australia

In 2015, Australia adopted the *Enhancing Online Safety Act 2015*.[40] While the Act originally focused on enhancing the protection of children online, amendments in 2017 made it applicable to the safety of all Australians. The Act created an eSafety Commissioner, whose responsibility is to promote and enhance online safety.

In 2021, the *Online Safety Act 2021*[41] "expanded and strengthened" the existing law, including by instituting new regulatory schemes and industry codes and conferring upon the Commissioner targeted powers to require providers to block access to "material showing abhorrent violent conduct."[42]

1.4.6 United States

In the United States, section 230 of the *Communications Decency Act*[43] protects online platforms from liability for content posted by users. However, the *Stop Enabling Sex Traffickers Act* and the *Allow States and Victims to Fight Online Sex Trafficking Act*, combined into one law in 2018, clarified that the platforms' immunity does not extend to the "knowing" facilitation of coerced or child sex trafficking.[44]

2 DESCRIPTION AND ANALYSIS

Bill C-63 has 52 clauses, divided into four main parts: enacting the Online Harms Act (Part 1); amending the *Criminal Code* (Part 2) and the *Canadian Human Rights Act* (Part 3) regarding hate crimes and hate speech; and amending *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service* (Part 4).

This section touches on the most important aspects of Bill C-63 without listing every provision. Before each part of the bill is described in detail, a brief overview of the current legal context is provided.

2.1 PART 1: ONLINE HARMS ACT

2.1.1 Current Legal Context: Regulation of Online Harms in Canada

There is currently no framework for regulating or holding online platforms accountable in Canada with respect to content posted by users. Platform liability for illegal content is 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.[45] However, *Criminal Code* provisions respecting uttering threats, hate propaganda, terrorist propaganda, obscene material, non-consensual distribution of intimate images, and some forms of cyberbullying and cyberstalking can be applicable to online content.[46]

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." Although the provisions make no specific reference to online speech, 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.

The Code also includes provisions on the publication of terrorist propaganda, defined as "any writing, sign, visible representation or audio recording that counsels the commission of a terrorism offence."[47] 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 covering child pornography; the distribution of intimate images without consent became a criminal offence with the *Protecting Canadians from Online Crime Act*[48] in 2014. It is worth noting that deepfakes[49] may not be captured by the provision on non-consensual distribution of intimate images,[50] except where the person depicted is or appears to be under the age of 18.[51]

Content bullying a child and content encouraging 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 frameworks are enforceable only through the court system and are thus not effective in curbing the proliferation of online harms.

No provisions exist in current law for content that is "legal but harmful." There is also no body with the authority to regulate online platforms in respect of harmful content, illegal or otherwise. The Canadian Radio-Television and Telecommunications Commission explains that it "does not regulate internet content because consumers can already control access to unsuitable material on the internet using filtering software. Any potential illegal content on the internet can be addressed with civil action, existing hate crime legislation, and the courts."[52]

Bill C-63 establishes the Online Harms Act in clause 1, which sets out obligations for social media service operators to reduce exposure to seven categories of harmful content, to completely block certain types of online content in Canada, and to disclose the steps they are taking to protect users from harmful content. The Online Harms Act contains 143 sections, divided into 10 parts. The general purposes of the Act are to promote online safety; protect Internet users, children, and others, by blocking or reducing exposure to harmful online content and its associated harms; and ensure online platforms are transparent and accountable in how they are fulfilling these responsibilities. The Act establishes the Digital Safety Commission to enforce the new regulatory framework and the Digital Safety Ombudsperson to increase public awareness and help individuals navigate the new framework.

2.1.2 Definitions
(Section 2 of the Online Harms Act)

"Harmful content" is defined as:

- intimate or sexual content, including deepfakes, 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;
- content that sexually victimizes a child (child pornography), or identifies a survivor/victim of child pornography and links them to 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 physical violence, and could cause a person to seriously harm or endanger another person, or seriously risk the health or safety of the public. This type of content is shared for a political, religious or ideological purpose and with the intention of intimidating the public, a group, a government, or organization.

For the purposes of the Online Harms 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 such as Facebook, Twitch, and Pornhub. It does not include search engines, unlike the European *Digital Services Act*.

A "regulated service" is a social media service with a certain number of users, as determined by regulation (section 3(1)). Different regulations may apply based on the number of users, with smaller social media services not required to meet the same obligations under the Act (section 3(2)). Regulations can 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 (section 3(3)). Services where users cannot communicate content to the public (section 5), and content that is shared through private messaging, are excluded from regulation (section 6).

Under section 2 of the Act, the definition of a "person" includes an individual, a corporation or another unincorporated group. An "operator" is a person who 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 7).

2.1.3 Digital Safety Commission of Canada (Sections 10 to 28 of the Online Harms Act)

Part 1 of the Online Harms Act establishes the Digital Safety Commission of Canada (the Commission) (section 10), composed of three to five full-time members, including a chairperson and potentially a vice-chairperson (section 12) who are appointed by the Governor in Council for renewable terms of up to five years (section 13). The Commission's mandate is to promote online safety in Canada and reduce harms caused by certain online content by (section 11):

- administering and enforcing the Online Harms 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 and other interested parties with the Commission's activities; and
- collaborating with operators, individuals with professional, technical or specialized knowledge, the Commission's international counterparts.

The Commission has the power to make regulations and issue guidelines and codes of conduct for social media service operators (section 26). The Commission must also hold hearings or make reports on any issue within its mandate when requested by the Governor in Council (section 28).

2.1.4 Digital Safety Ombudsperson of Canada (Sections 29 to 38 of the Online Harms Act)

Part 2 of the Online Harms Act creates the role of Digital Safety Ombudsperson of Canada (Ombudsperson). Like Commission members, the Ombudsperson is appointed by the Governor in Council to a full-time position for a renewable term of up to five years (sections 29 and 30).

The Ombudsperson's mandate is to "provide support to users of regulated services and advocate for the public interest with respect to systemic issues related to online safety" (section 31). To this end, the Ombudsperson's powers and duties include collecting information relating to online safety and harmful content, including the perspectives of users of regulated services and victims of harmful content; highlighting issues related to online safety and publishing relevant collected information; and directing users to relevant resources (section 37).

2.1.5 Digital Safety Office of Canada (Sections 39 to 53 of the Online Harms Act)

Part 3 of the Online Harms Act establishes the Digital Safety Office of Canada (the Office), responsible for supporting the Commission and the Ombudsperson in fulfilling their mandates (sections 39 and 40). The Chief Executive Officer (CEO) of the Office is appointed by the Governor in Council for a renewable term of up to five years (section 44). The CEO can contract for or hire employees, legal counsel or others to advise or assist the Commission or the Ombudsperson in their work (section 43). Neither the Commission nor the Ombudsperson have their own staff; any necessary support is provided by the Office.

2.1.6 Duties of Operators of Regulated Services (Sections 54 to 72 of the Online Harms Act)

Part 4 of the Online Harms Act sets out duties for operators of a regulated service:

- the duty to protect children;
- the duty to keep records;
- the duty to act responsibly; and
- the duty to make certain content inaccessible.

The duty to protect children requires operators to ensure their site includes any design features related to the protection of children, as provided by regulation (sections 64 to 65). These could include requiring providers to implement parental controls, rules about targeted content or advertisements directed at children, or content warning labels.

Operators have a duty to keep any records needed to show whether the operator is complying with the Act (section 72). The duty to act responsibly and the duty to make certain content inaccessible are described below.

2.1.6.1 Duty to Act Responsibly (Sections 54 to 63 of the Online Harms Act)

The duty to act responsibly requires operators to implement measures to reduce the risk that users will be exposed to harmful content on their service (section 54). These include measures initiated by the operator, as well as measures required by regulation (section 56). 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 55). Operators must publish user guidelines that describe the risk mitigation measures implemented, and a standard of conduct for users with respect to harmful content (section 57). Operators must also provide users with tools to block other users (section 58).

Operators must implement tools and processes to flag harmful content. Users must be able to flag to the operator any harmful content accessible on the site. 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 59).

Operators must ensure that a resource person is available to receive user concerns about harmful content and any related measures implemented by the operator, and to provide information and guidance to users to address these concerns, including through internal complaints mechanisms, the Commission or law enforcement (section 61).

Operators of a regulated service must publish a digital safety plan online and submit a copy of the plan to the Commission. The plan must detail how the operator has complied with requirements under the Act (section 62) and must include:

- a risk assessment related to user exposure to harmful content in the site;
- a description of measures implemented to mitigate the risk, the effectiveness of implemented measures and factors considered when assessing effectiveness;
- resources allocated to complying with the duty to act responsibly;
- the volume and type of harmful content that was accessible on the site, including how harmful content was moderated, and the quantity and type of content that was moderated;
- the number of times users flagged various types of harmful content on the site, how the operator assessed the flags, whether and when the operator undertook measures to respond to flagged content;
- 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; and
- other information, including information required by regulation.[53]

Operators who block content that incites violence, violent extremism or terrorism must temporarily preserve the content in case it is required as evidence for a criminal charge. Absent a court order or preservation demand, the operator must destroy the content after one year (section 63). These requirements align with amendments to the Mandatory Reporting Act, contained in Part 4 of Bill C-63 and discussed below in section 2.4.

2.1.6.2 Duty to Make Certain Content Inaccessible (Sections 67 to 71 of the Online Harms Act)

An operator 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 67 and 68). 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 68).

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 68(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 69). 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 70). The timelines for this process will be set out in regulation.

2.1.7 Access to Inventories and Electronic Data (sections 73 to 77 of the Online Harms Act)

The Online Harms Act provides for a mechanism granting access to inventories and electronic data of the operators of social media services subject to the Act (sections 73 to 77).

Access may be given only to a person accredited by the Commission (section 73(2)). Accreditation may be granted to persons, other than an individual, conducting research or engaging in education, advocacy or awareness activities related to the purposes of the Act (section 73(1)). The Commission may revoke or suspend a person's accreditation after giving them a reasonable opportunity to make representations if it determines that they failed to comply with conditions (section 73(3)).

If an accredited person submits a request for access, the Commission may make an order requiring the operator to give access to the content requested (section 74(1)). At the request of the operator, the Commission may amend or revoke the order if it determines that the operator is unable to comply with the order or that complying with it would cause the operator undue hardship (section 75). If the operator fails to comply with the order, the accredited person may make a complaint to the Commission (section 76(1)).

The Commission may publish a list of accredited persons and a description of the research projects in question (section 77).

2.1.8 Remedies – Complaints Respecting Certain Content (Sections 78 to 85 of the Online Harms Act)

Anyone in Canada may file a complaint with the Commission if they believe that a regulated service is allowing access to content that sexually victimizes a child or revictimizes a survivor or is intimate content shared without consent (section 81). The resulting process is similar to the steps under an operator's duty to make certain content inaccessible, described above.

The Commission must assess each complaint and notify the complainant if it is dismissed. If the complaint is not dismissed, the Commission must notify the relevant operator and order the disputed content blocked at least until the Commission's decision review process is complete (section 81). The user who posted or shared the content and the complainant user may each make submissions for the Commission to consider as part of its review of the decision to block the disputed content. Depending on the Commission's final decision, the original order to block the content is either revoked or made permanent (section 82). The Commission may review its decision only once.

2.1.9 Administration and Enforcement (Sections 86 to 95 of the Online Harms Act)

The Commission's investigators have the power to enter any place where they have reason to believe there is evidence or information related to verifying compliance or preventing non-compliance with the Act (section 91). This includes accessing a place remotely or online, if the owner or person in charge of the place has been informed. A warrant is required for an investigator to enter a dwelling-place where the owner or occupant did not or would not consent for the investigator to enter. The owner or person in charge must assist the investigator in every reasonable way and provide any document or other information relevant to the investigator's mandate.

When verifying compliance with the Act, the Commission has the power to summon witnesses and compel them to testify or produce any necessary documents, administer oaths, and make any relevant decision related to procedure or evidence (section 86). The Commission can use any relevant and available evidence in making a decision, and it is not bound by the rules of evidence that would apply in a court (section 87).

The Commission may hold a hearing in connection with a complaint or an operator's compliance. Hearings are public by default or can be held in private under certain circumstances (section 88).

The Commission may issue a compliance order to an operator where there are reasonable grounds to believe that the operator is contravening or has contravened the Act (section 94). A compliance order filed with the Federal Court has the same weight and enforceability as a court order (section 95).[54]

2.1.9.1 Administrative Monetary Penalties and Offences (Sections 96 to 124 of the Online Harms Act)

Violations of the Act may result in fines or administrative monetary penalties, depending on the circumstances and whether the accused is an operator.

An administrative monetary penalty is a civil penalty imposed by the Commission, and functions as a financial deterrent for contravening the Act. A continuing violation is treated as separate violation for each day it continues (section 97). The purpose of the administrative monetary penalty regime is to encourage compliance with the Act, not to punish (section 98). It is not a fine, which requires a pleading or finding of guilt in a court. There is no trial for an alleged violation, nor does it result in a criminal record. The person subject to the notice of violation, which includes the penalty to be paid, may submit arguments to the Commission within a set timeline (section 104). The person is not liable if they can show they and their employees or agents exercised due diligence in attempting to comply with the Act (section 113). The Commission decides on a balance of probabilities whether the person is liable for the violation (section 104). A person subject to a notice of violation who fails to respond to the notice on time, or who pays the penalty, is deemed to have committed the violation (sections 103 and 105).

Administrative monetary penalties can be as high as either 6% of the gross global revenue of the person who committed the violation or $10 million, whichever is greater (section 101).[55] Factors in determining the amount of the penalty include the nature and scope of the violation, the person's history of compliance, their ability to pay and any benefit they received by committing the violation (section 102).

An operator who commits a violation or an offence under the Act may be subject to either[56] administrative monetary penalties (section 96) or fines (section 120) for:

- contravening a Commission order or certain requirements;[57]
- contravening an undertaking entered into with the Commission;
- obstructing the Commission or an inspector in their work; or
- making a false or misleading statement to the Commission or an inspector as it relates to their work.

Operators may also face an administrative monetary penalty, but not a fine, for contravening a provision of the Act or related regulations, or for failing to provide an inspector with information or documents related to verifying compliance as required under the Act[58] (section 96).

A person who runs an unregulated social media service may be subject to administrative monetary penalties (section 96) for:

- failing to provide the Commission with requested information related to the social media service's size (to determine whether the service should be regulated);
- failing to provide an inspector with requested information or documents related to verifying compliance under the Act;

- obstructing the Commission or an inspector in their work; or
- making a false or misleading statement to the Commission or an inspector as it relates to their work.

A person other than an operator may be subject to fines if they fail to assist an inspector as required, or fail to provide an inspector with requested information or documents needed to verify compliance under the Act.

An operator who is convicted of an offence by way of indictment faces a fine of up to 8% of the operator's gross global revenue or $25 million, whichever is greater. The maximum fine is lowered to either 7% or $20 million for a summary conviction (section 120).

A person other than operator who is convicted of an offence by way of indictment faces a fine of up to 3% of their gross global revenue or $10 million, or a fine at the discretion of the court if the guilty party is an individual and not a corporation. The fines are lowered to 2% or $5 million for a summary conviction, or a fine of up to $50,000 for an individual (section 121).

2.1.10 Protections, Reports and Information Sharing (Sections 126 to 138 of the Online Harms Act)

Part 8 of the Online Harms Act sets out the management of confidential information. Confidential information is defined as "information that is a trade secret; or financial, commercial, scientific or technical information that is confidential and that is treated consistently in a confidential manner by the person who submitted it or the person to whose business or affairs it relates" (section 127(1)).

Any person who had access to confidential information while working for the Commission, the Ombudsperson or the Office is prohibited from disclosing this information, either directly or indirectly, unless the designation of confidential is withdrawn (sections 127(3) and 127(4)).

However, there are exceptions to this prohibition of disclosure. For the purposes of fulfilling their respective mandates, the Commission and the Ombudsperson may exchange information designated as confidential with each other (section 135). Information designated as confidential that is submitted in the course of proceedings before the Commission may be disclosed by the Commission if it determines that the disclosure is in the public interest (section 127(5)). Other information designated as confidential that is submitted to or obtained by the Commission may not be disclosed, unless the disclosure would be both in the public interest and relevant to the determination of a matter before it (section 127(6)). Information designated as confidential may also be disclosed by the Commission or the Ombudsperson to the

Minister if the Minister has reasonable grounds to believe that the information is relevant for the making of regulations or for the purpose of ensuring that the Act and the regulations are effective (section 138).

The bill also provides for the production of annual reports by the Commission and the Ombudsperson (sections 130 and 131) to be presented to Parliament by the Minister (section 134). The Minister may also request additional reports as needed (section 132).

2.1.11 General Provisions and Coming into Force (Sections 139 to 143 of the Online Harms Act)

Part 9 of the Online Harms Act provides that the Governor in Council may make regulations for the purpose of recovering costs incurred by the Commission, the Ombudsman and the Office from regulated social media platforms (section 139), it outlines the areas in which the Commission and the Governor in Council may make regulations (sections 140 and 141), and it sets out the five-year review of the Act (section 142). The review is undertaken at the Minister's initiative and is not a parliamentary review as such.

Part 10 of the Online Harms Act provides that the Act shall come into force on a day or days to be fixed by order of the Governor in Council (section 143).

2.1.12 Consequential and Coordinating Amendments (Clauses 2 to 10)

Bill C-63 makes a number of consequential and coordinating amendments. For example, the bill amends the *Access to Information Act*, the *Financial Administration Act*, the *Privacy Act* and the *Public Service Superannuation Act* to add references to the Digital Safety Commission of Canada, the Digital Safety Office of Canada and the Digital Safety Ombudsperson of Canada.

Clause 8 makes coordinating amendments to the Online Harms Act to provide for information sharing, consultation and research coordination between the Commission, the Artificial Intelligence and Data Commissioner under the *Artificial Intelligence and Data Act*, and the Canadian Radio-television and Telecommunications Commission. These amendments apply when the Digital Charter Implementation Act, 2022 [59] receives Royal Assent.

2.2 PART 2: AMENDMENTS TO THE *CRIMINAL CODE* AND RELATED AMENDMENTS

2.2.1 Current Legal Context: *Criminal Code* and Hate Crimes

Provisions addressing hate crimes in Canada date back to the 1960s.[60] After the Second World War, various international treaties were ratified by Canada, which involved obligations to incorporate provisions into Canada's legislation that sought to prohibit all hate propaganda inciting discrimination or violence.[61] Canada reports regularly to the United Nations on measures taken to ensure the implementation of the *International Convention on the Elimination of All Forms of Racial Discrimination*.[62]

In recent years, many segments of the Canadian population have been targeted by hate speech and hate crime because they belong to an identifiable group based on characteristics such as race, skin colour, religion, sexual orientation, ethnic origin, sex and gender identity or expression. The harmful effects of hate crimes extend far beyond those directly targeted and encompass all the groups to which they belong, conveying a message designed to frighten and marginalize them.[63]

Unfortunately, data on hate crimes and hate speech, whether in the form of expressive acts or not, are difficult to collect and may vary considerably from one year to the next for various reasons. For example, increased public awareness of this type of offence could lead to a significant increase in reporting, without it corresponding to a marked increase in the violence experienced by the groups targeted. Similarly, while a significant increase in violence may be experienced by the groups concerned, the public may not be aware of it, which reduces the likelihood that the general population will report this type of event to the police.[64]

Two groups of offences under the Code address expressions of hatred:

- hate propaganda or hate speech; and
- other crimes motivated by hate.

Whether an act, expressive or not, is characterized as hateful depends on the status of the person targeted – whether they are part of an "identifiable group" within the meaning of the law – and on the intention to target that person because they are part of that group.[65] Since these provisions were adopted, debate has focused more on the provisions addressing hate speech than crimes motivated by hate.

The Supreme Court of Canada considered the key provisions for addressing hate propaganda in the Code, as well as in the former section 13 of the *Canadian Human Rights Act* and section 14 of the former version of the *Saskatchewan Human*

Rights Code.[66] It concluded that, although these provisions infringed on the right to freedom of expression guaranteed under section 2(b) of the Charter, the infringement was reasonable and justifiable.[67]

The Supreme Court also developed a framework to determine whether content constitutes hate speech or not.[68] To be considered hatred, speech must be both extreme and likely to lead to discriminatory or violent acts toward members of the group.[69]

Part 2 of Bill C-63 amends the Code to create a new hate crime offence and a new recognizance to keep the peace. It also increases the maximum sentences for hate propaganda offences, repeals a related offence, and defines "hatred" in the context of these offences.

2.2.2 Defining Hatred and Increasing Maximum Sentences for Hate Propaganda Offences (Clauses 13 and 14)

Clauses 13 and 14 of Bill C-63 amend sections 318 and 319 of the Code to increase the maximum sentences for four offences relating to hate propaganda. The maximum sentence for advocating genocide (section 318(1)) is increased from five years to life imprisonment. The maximum sentences for public incitement of hatred (section 319(1)), wilful promotion of hatred (section 319(2)), and wilful promotion of antisemitism (section 319(2.1)) are each increased from two years to five years' imprisonment.

When determining the appropriate sentence in any given case, a sentencing judge will consider the full circumstances of the case and the purpose and principles of sentencing,[70] including the fundamental principle that sentences "must be proportionate to the gravity of the offence and the degree of responsibility of the offender" (section 718.1).

Clause 14 adds a definition of hatred for the purpose of the new hate crime offence and existing hate propaganda offences. Under new section 319(7) of the Code, hatred "means the emotion that involves detestation or vilification and that is stronger than disdain or dislike." For greater certainty, new section 319(8) adds that a statement does not incite or promote hatred "solely because it discredits, humiliates, hurts or offends."

These new sections aim to clarify the scope of criminal hate speech laws to ensure that any speech that merely expresses dislike or disdain, or that discredits, humiliates, hurts or offends someone is not subject to criminal penalties.[71] This is consistent with Supreme Court of Canada jurisprudence on section 2(b) of the Charter, which has

emphasized "the need to avoid finding that the accused intended to promote hatred merely because the expression is distasteful."[72] As explained by the Court in a case that upheld a prohibition on hate publications under Saskatchewan's human rights code:

> "detestation" and "vilification" aptly describe the harmful effect that the *Code* seeks to eliminate. Representations that expose a target group to detestation tend to inspire enmity and extreme ill-will against them, which goes beyond mere disdain or dislike. Representations vilifying a person or group will seek to abuse, denigrate or delegitimize them, to render them lawless, dangerous, unworthy or unacceptable in the eyes of the audience. Expression exposing vulnerable groups to detestation and vilification goes far beyond merely discrediting, humiliating or offending the victims.[73]

2.2.3 New Hate Crime Offence (Clause 15)

Current section 718.2(a)(i) of the Code provides that if any offence is "motivated by *bias, prejudice or hate* based on race, national or ethnic origin, language, colour, religion, sex, age, mental or physical disability, sexual orientation, or gender identity or expression, or on *any other similar factor*," that motivation should be considered an aggravating circumstance for sentencing. [Author's emphasis]

Clause 15 of Bill C-63 enacts new section 320.1001 of the Code, which sets out a specific hate crime offence that applies when any offence under the Code or another Act of Parliament is motivated by race, national or ethnic origin, language, colour, religion, sex, age, mental or physical disability, sexual orientation, or gender identity or expression. This new offence carries a maximum sentence of life imprisonment.

Unlike section 718.2(a)(i), new section 320.1001 is limited to crimes motivated by hate, and it does not include the seemingly lower threshold of "bias" or "prejudice."[74] Similarly, new section 320.1001 does not include the expression "any other similar factor,"[75] which suggest that it provides an exhaustive list of grounds. Although case law on the scope of section 718.2(a)(i) is limited, there have been some cases in which sentencing judges have found that hatred toward political beliefs, against police officers, and against homeless people could be considered aggravating factors in sentencing based on this provision.[76] These types of hatred do not appear to fall within the scope of new section 320.1001.

2.2.4 Repealing a Related Offence (Clause 16)

Clause 16 repeals section 430(4.1) of the Code, which set out a specific offence, carrying a maximum sentence of ten years' imprisonment, for mischief in relation to certain property – such as places of worship – that was motivated by bias, prejudice or hate.

Similar conduct continues to be prohibited through existing section 430(1) of the Code, and – if motivated by hate – is subject to a maximum sentence of life imprisonment pursuant to new section 320.1001.

2.2.5 Recognizances for Hate Propaganda and Hate Crimes (Clause 17)

Clause 17 of the bill adds new section 810.012(1) to the Code, which allows a person to seek a recognizance[77] – also called a peace bond or a surety to keep the peace – if they obtain the consent of the Attorney General and have reasonable grounds to fear that another person will commit a hate propaganda or hate crime offence. New sections 810.012(2) to 810.012(11) provide further details about the new recognizance and procedural elements relevant to it.

New section 810.012(2) allows a provincial court judge to require the informant and the defendant to appear before them. If, after reviewing the evidence, the judge is satisfied that there are reasonable grounds to fear that a hate propaganda offence or the new hate crime offence will be committed, the judge may order the defendant to enter into a recognizance to keep the peace and be of good behaviour under new section 810.012(3). The recognizance can be for a period of up to 12 months, unless the defendant was already convicted of an offence referenced in section 810.012(1), in which case it can be extended to up to two years (new section 810.012(4)).

New sections 810.012(6) to 810.012(8) cover the types of conditions that may be attached to the recognizance. Section 810.012(6) provides a non-exhaustive list of conditions that, if ordered, require the defendant to wear an electronic monitoring device, remain at their residence at specified times, stay away from specified places or not communicate with a person, among other things. Existing section 810(3.02) already states that the justice or court may "add any reasonable conditions to the recognizance that the justice or court considers desirable to secure the good conduct of the defendant." The Supreme Court has explained that the conditions must have a nexus with the specific fear expressed by the informant and should not be so onerous as to effectively set up the defendant to fail (for example, impose a condition to abstain from consuming drugs and alcohol on a defendant known to have a substance use disorder).[78]

New sections 810.012(6)(c) and 810.012(6)(e) allow a judge to require the defendant to abstain from consuming intoxicating substances, drugs not medically prescribed and alcohol, and to provide a sample of a bodily substance, as required, to persons designated under regulations. Samples can be required at regular intervals to ensure compliance with the order or when a designated person has reason to believe the defendant has breached the condition. Additional rules for handling these samples are provided in clauses 18 to 20.[79]

New section 810.012(11) states that existing section 810(5) applies to recognizances ordered under it. The latter states that "the provisions of this Part apply, with such modifications as the circumstances require, to proceedings under this section." When it examined this section, the Supreme Court explained that section 810(5) incorporates all provisions of Part XXVII of the Code (Summary Convictions), adding that, "Parliament has chosen a rather circuitous route to incorporate the necessary procedures to cause the parties to appear."[80] In brief, incorporating the full part into the procedures for recognizances means that sections on various additional rules and options, such as the rules for laying an information or for appearing by video or audioconference, apply to the new recognizances.

The maximum sentence for breaching this new recognizance is the same as for other types of recognizances: four years of imprisonment (for an indictable offence) or a fine of $5,000 and/or imprisonment for no more than two years less a day (on summary conviction) (section 811 of the Code).

Clause 12 amends section 264(4) of the Code to allow a judge to consider an offender's contravention of the terms and conditions of a recognizance under section 810.012 to be an aggravating factor in sentencing for the offence of criminal harassment.

2.2.6 Related and Coordinating Amendments, and Coming into Force (Clauses 24 to 32)

Clauses 24 and 25 of Bill C-63 amend Schedules 1 and 2 of the *Criminal Records Act* so that a person convicted of an offence that was motivated by hatred (new section 320.1001 of the Code) is subject to the same record suspension restrictions as a person who commits the same underlying offence without being motivated by hatred.

Similarly, clause 26 amends Schedule 1 of the *Corrections and Conditional Release Act* (CCRA) so that a person convicted of an offence that was motivated by hatred (new section 320.1001 of the Code) is subject to the same restrictions for release as a person who commits the same underlying offence without being motivated by hatred. Offences listed in Schedule 1 and 2 of the CCRA are offences considered to be deserving special denunciation. Practically, being incarcerated for a schedule offence could potentially delay the conditional release of the offender.[81]

Clauses 27 and 28 amend the *Youth Criminal Justice Act* (YCJA), which provides the framework for a justice system designed for youth aged 12 to 17. While the offences in the Code apply to youth, their cases are handled in accordance with the YCJA. These amendments allow a youth justice court to make orders requiring a young person to enter into a recognizance under new section 810.012 of the Code, adding to existing recognizances under sections 14(2) and 142(1)(a) of the YCJA.

Clauses 29 to 31 set out coordinating amendments that take effect if certain other Acts come into force. Clause 32 provides that all the other amendments to the Code in Bill C-63 come into force on the 90th day after the bill receives Royal Assent.

2.3 PART 3: AMENDMENTS TO THE *CANADIAN HUMAN RIGHTS ACT*

2.3.1 Current Legal Context: Canadian Human Rights Act

Adopted by Parliament and assented to on 14 July 1977, the *Canadian Human Rights Act* (CHRA) prohibits discrimination in areas of federal jurisdiction (e.g., federal departments and agencies, banking, transportation and telecommunications), based on certain illicit grounds associated with characteristics such as race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics, disability or conviction for an offence for which a pardon has been granted or in respect of which a record suspension has been ordered.

The Canadian Human Rights Commission was established under the CHRA, as was the Canadian Human Rights Tribunal. The Commission deals with complaints about alleged discriminatory practices that fall within its jurisdiction. It is empowered to investigate discrimination complaints and serves as a gatekeeper in the process. If the Commission determines that an inquiry is warranted, the complaint may proceed to the Tribunal. The Tribunal then conducts an inquiry to determine whether discrimination has occurred, and if it has, what remedy is appropriate.

Until it was repealed in 2013, section 13 of the CHRA set out a mechanism for dealing with hate promoted by way of telecommunications.[82] Section 13 was adopted in response to the use of telephone hate messages by neo-Nazi sympathizers in the 1970s. Beginning in the 1990s, section 13 was also used to address hate posted on websites and to deal with those who operated such sites.

The possibility of introducing an amended version of section 13 was raised before Parliament in 2012 when a parliamentary committee was studying Bill C-304, which repealed the provision.[83] However, some people[84] believed that the provision was being misused for various reasons, which led to section 13 being repealed in its entirety, despite the objections expressed by other stakeholders, including the Commission itself.[85]

2.3.2 Hate Speech as a Discriminatory Practice (Clauses 34, 35, 37, 41, 43)

Clause 34 of Bill C-63 reinstates a modified version of former section 13 of the CHRA. This section defines the discriminatory practice of communicating hate speech. Specifically, under new section 13 of the CHRA:

> It is a discriminatory practice to communicate or cause to be communicated hate speech by means of the Internet or any other means of telecommunication in a context in which the hate speech is likely to foment detestation or vilification of an individual or group of individuals on the basis of a prohibited ground of discrimination.

Hate speech is considered to be communicated so long as it remains public, and the person has the ability to remove or block access to it (new section 13(2)).

New section 13(8) defines hate speech as a communication expressing "detestation or vilification of an individual or group of individuals on the basis of a prohibited ground of discrimination." New section 13(9) further explains that communication does not constitute hate speech "solely because it expresses disdain or dislike or it discredits, humiliates, hurts or offends." As with the definition of hatred added to the Code in clause 14, this definition is consistent with the Supreme Court's interpretation of the version of section 13 of the CHRA that was repealed in 2013 and the definition of hatred in the case law.

Clause 34 also specifies the types of communication that do not constitute hate speech for the purpose of new section 13. Section 13 does not apply to:

- individuals who merely host, cache or indicate the location of hate speech (section 13(3));
- telecommunications service providers whose service or facility is used by another person for hate speech (section 13(4));
- private communications (section 13(5));[86]
- broadcasting undertakings, as defined in section 2(1) of the *Broadcasting Act* (section 13(6));[87] and
- operators of social media services or other websites or applications "whose primary purpose is to facilitate interprovincial or international online communication among users of the website or application by enabling them to access and share content" (section 13(7)).[88]

Clause 41 adds new section 53.1 to the CHRA, which sets out the orders that the Canadian Human Rights Tribunal can make against a person who engages in the discriminatory practice of communicating hate speech. These include an order to cease the practice and take measures to redress that practice or prevent it from recurring, pay up to $20,000 in compensation to any victim personally identified in the hate speech communication, and pay an additional fine of up to $50,000, depending on such factors as the extent and gravity of the hate speech and the intent of the person who communicated it, among others. Clause 41 also adds new section 53.2 to the CHRA, allowing the Tribunal to award costs for abuse of process.

Under section 41(1) of the CHRA, the Canadian Human Rights Commission is already empowered to decline to deal with complaints that appear to be "trivial, frivolous, vexatious or made in bad faith." Clause 37 adds new section 41(1.1) to the CHRA to clarify that the Commission will decline to deal with a section 13 complaint if it is evident to the Commission that the complaint relates to conduct that does not constitute hate speech. The possibility of costs for abuse of process could further discourage parties from bringing forward frivolous or bad faith complaints under new section 13.

Clause 43 amends section 60(1) of the CHRA so that contravening an order made under section 52(1) or 52(2) is an offence punishable on summary conviction by a fine of up to $50,000.

2.3.3 Confidentiality Protections for Victims (Clauses 36 and 39)

Clause 36 adds new section 40(8) to the CHRA, which allows the Canadian Human Rights Commission to deal with a complaint under new section 13 without disclosing the identity of the alleged victim, the complainant or other persons who have assisted the Commission, where "there is a real and substantial risk that any of those individuals will be subjected to threats, intimidation or discrimination."

Similarly, new sections 40(9) and 40(10) to the CHRA allow the Commission to order a person who has learned the identity of an alleged victim, complainant or other person who has assisted the Commission not to reveal that person's identity, unless doing so is required by law or is necessary for the purposes of an investigation, a conciliation or a settlement under the CHRA. Clause 43(1) makes it a criminal offence to contravene an order under section 40(9); a person who does so is liable on summary conviction to a fine of up to $50,000.

Similarly, although inquiries are generally to be conducted in public, clause 39 amends section 52 of the CHRA to allow the Tribunal to take measures, upon request, to ensure the confidentiality of the inquiry, if there is "a real and substantial

risk" that the alleged victim, the complainant or an individual who gives evidence or otherwise assists the inquiry in any way "will be subjected to threats, intimidation or discrimination."

2.3.4 Miscellaneous Amendments and Coming into Force (Clauses 38, 42 and 44)

Clause 38 amends section 48.1 of the CHRA to increase the number of Tribunal members from 18 to 20.

Clause 42 makes an incidental amendment to section 57 of the CHRA to allow orders under new sections 53.1 and 53.2 to be enforced as orders of the Federal Court, in the same manner as orders under section 53.

Clause 44 provides that the amendments to the CHRA come into force on a day or days to be fixed by the Governor in Council.

2.4 PART 4: AMENDING AN ACT RESPECTING THE MANDATORY REPORTING OF INTERNET CHILD PORNOGRAPHY BY PERSONS WHO PROVIDE AN INTERNET SERVICE

2.4.1 Current Legal Context: Mandatory Reporting Act

The Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service (Mandatory Reporting Act) requires an Internet service provider to report if their service is being used to commit a child pornography offence. If advised of such an offence during service provision, the service provider must report the offending Internet Protocol (IP) address or Uniform Resource Locator (URL) to the Canadian Centre for Child Protection. In addition, pursuant to section 3 of the Act, if the service provider has reasonable grounds to believe that its service is being used to commit a child pornography offence, it must "notify an officer, constable or other person employed for the preservation and maintenance of the public peace" as soon as possible, as prescribed by sections 10 to 12 of the *Internet Child Pornography Reporting Regulations*.[89]

According to Public Safety Canada,

> Since the Mandatory Reporting Act came into force in 2011, the way that the Internet is used and how crimes are committed online has evolved. The RCMP has been actively working with its federal partners to identify ways in which the Act could be updated to address gaps and increase its effectiveness in protecting children from victimization. This includes examining: the scope of the Act and what entities are subject to the obligations under the Act; powers for better monitoring

> compliance with the Act; the information that must be reported to police when companies have grounds to believe that their Internet service is being used to commit a child pornography offence; and how to address issues around loss of evidence due to short retention periods of service providers.[90]

Part 4 of Bill C-63 amends or replaces several sections of the Mandatory Reporting Act. Legislative changes include correcting various technical aspects of the Act to make it easier to manage flagging, investigations and criminal prosecutions involving child pornography. However, the bill does not expand the scope of the Act to other types of material, such as the publication of intimate content without consent (also known as "revenge porn"). It maintains its current scope of application, which is child pornography.

However, the bill does require increased transparency from the designated body.

2.4.2 Definition of "Internet Service" (Clause 45)

Clause 45 amends the definition of "Internet service" so that it is no longer restricted to "a service providing Internet access, Internet content hosting or electronic mail." This list is now preceded by the word "includes," indicating that it is a non-exhaustive list that may change over time.[91]

Clause 45 also clarifies the scope of the second and third types of Internet service mentioned. It specifies that "Internet service" includes providing Internet content hosting, "regardless of the originator of the content or the manner by which the content is made accessible." Furthermore, the third type of service is no longer restricted to electronic mail services – it includes more broadly "facilitating interpersonal communication over the Internet."

2.4.3 Duties of Persons Providing Internet Service

2.4.3.1 Notifying the Law Enforcement Body Designated by the Regulations (Clause 46)

Currently, a person who provides an "Internet service" to the public who has reasonable grounds to believe[92] that their Internet service is being used to provide access to child pornography has a duty to notify a police *officer* or *constable*. Clause 46 of Bill C-63 amends section 3 of the Mandatory Reporting Act to require instead that the notification be made to a "law enforcement body." The body will be designated in future regulations.

In 2021, the House of Commons Standing Committee on Access to Information, Privacy and Ethics, in its study of non-consensual intimate images on Pornhub, made several recommendations for amending the Mandatory Reporting Act, including making the National Child Exploitation Coordination Centre, housed within the Royal Canadian Mounted Police, the designated law enforcement agency for the purposes of reporting under section 3 of the Act to "concentrate reports to one organization and assist in addressing duplication or conflict."[93]

2.4.3.2 Submitting Transmission Data and Preserving Computer Data (Clause 46)

Furthermore, if the person who provides an Internet service believes that the content in question is *manifestly* child pornography, they must include with the notification a document containing any "transmission data"[94] associated with the content that could assist in the investigation. For now, the content of the mandatory reporting, provided for in the regulations, does not appear to refer to either transmission data or computer data.[95]

Currently, the person who provides Internet service who submits a report to the police must preserve all "computer data"[96] in their possession or control for 21 days. Under clause 46, this time frame is increased to one year from the day on which the notification is made to the designated law enforcement agency (section 4(1) of the Mandatory Reporting Act).

2.4.4 Limitation Period (Clause 48)

Clause 48 provides that the limitation period to pursue a prosecution against a person for an offence committed under the Mandatory Reporting Act is increased from two years to five years (section 11 of the Mandatory Reporting Act).

2.4.5 Regulations (Clause 49)

In clause 49, new regulatory powers are granted to the Governor in Council for the application of the Mandatory Reporting Act. For example, the Governor in Council may require the designated law enforcement body to submit to the Minister of Justice and the Minister of Public Safety an annual report (new section 12(d.1) of the Mandatory Reporting Act). The Governor in Council may also specify the form and content of this report, as well as the manner and time of its submission.

2.4.6 Coordinating Amendments and Coming into Force (Clauses 50 and 51)

Coordinating amendments are outlined in the event that Bill C-291[97] receives Royal Assent (clause 50). They provide that the term "child pornography" be replaced by the term "child sexual abuse and exploitation material."[98]

Part 4 of Bill C-63, which amends the Mandatory Reporting Act, comes into force six months after the bill receives Royal Assent (clause 51).

NOTES

1. 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.
2. Part 5 of Bill C-63 outlines a coordinating amendment with Bill C-291 should it come into force.
3. *Criminal Code* (the Code), R.S.C. 1985, c. C-46.
4. *Canadian Human Rights Act*, R.S.C. 1985, c. H-6.
5. *Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*, S.C. 2011, c. 4.
6. Philip Mai et al., *The State of Social Media in Canada 2022*: *A Census-balanced Survey About Social Media Adoption and Use in Canada*, Social Media Lab Toronto Metropolitan University, 2022, p. 4.
7. Statistics Canada, "Online hate and aggression among young people in Canada," *The Daily*, 27 February 2024.
8. Laura Savage, Statistics Canada, *Online child sexual exploitation: A statistical profile of police-reported incidents in Canada, 2014 to 2022*, 12 March 2022. Another alarming statistic: Cybertip.ca reports an increase of 815% in reports of online sexual luring in five years (an offence under section 172.1 of the *Criminal Code*). See also Canadian Centre for Child Protection, *An Analysis of Financial Sextortion Victim Posts Published On R/Sextortion*, November 2022.
9. Statistics Canada, *Table 5: Police-reported crime for selected offences, Canada, 2021 and 2022*.
10. Jacob Davey, Cécile Guerin and Mackenzie Hart, *An Online Environmental Scan of Right-wing Extremism in Canada*, Institute for Strategic Dialogue, 19 June 2020, p. 5.
11. Nicholas Kristof, "The Children of Pornhub," *The New York Times*, 4 December 2020.
12. See also, for example: *R. v. Veltman*, 2024 ONSC 1054; where Ontario Superior Court in London, Justice Pomerance found that the crimes Nathaniel Veltman constituted a "terrorist activity."
13. Bill C-36, An Act to amend the Criminal Code and the Canadian Human Rights Act and to make related amendments to another Act (hate propaganda, hate crimes and hate speech), 43rd Parliament, 2nd Session.
14. Department of Justice Canada, *Government of Canada takes action to protect Canadians against hate speech and hate crimes*, News release, 23 June 2021.
15. See Robert Mason and Julian Walker, *Legislative Summary of Bill C-36: An Act to amend the Criminal Code and the Canadian Human Rights Act and to make related amendments to another Act (hate propaganda, hate crimes and hate speech)*, Publication no. 43-2-C36-E, Library of Parliament, 8 September 2021.
16. Government of Canada, *Technical paper*.

17. Government of Canada, *What We Heard: The Government's proposed approach to address harmful content online*.

18. Government of Canada, *Concluding Workshop Summary*.

19. Government of Canada, *What We Heard: 2022 Roundtables on Online Safety*.

20. 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.

21. Ibid.

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

23. 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.

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

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

26. Government of Canada, "Questions and Answers – Online Harms," *Appearance of the Honourable Steven Guilbeault Before the Standing Committee on Access to Information, Privacy and Ethics (ETHI), Online Harms, on June 7, 2021*.

27. Ibid.

28. 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)*, *Official Journal* L 277.

29. European Commission, *Europe fit for the Digital Age: Commission proposes new rules for digital platforms*, 15 December 2020.

30. Ibid.

31. European Commission, *Digital Services Act: Questions and Answers*, 3 April 2024.

32. Human Rights Watch, *Germany: Flawed Social Media Law*, 14 February 2018.

33. European Commission, *Questions and answers on the Digital Services Act*, 23 February 2024.

34. France, *Loi nº 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet*.

35. Constitutional Council, *Décision nº 2020-801 DC du 18 juin 2020*. See Nicolas Boring, *France: Constitutional Court Strikes Down Key Provisions of Bill on Hate Speech*, Library of Congress, 29 June 2020.

36. European Commission, *Questions and answers on the Digital Services Act*, 23 February 2024.

37. United Kingdom, *Online Safety Act 2023*.

38. United Kingdom, *A guide to the Online Safety Bill*, 30 August 2023.

39. United Kingdom, *The Online Safety Act 2023 (Commencement No. 2) Regulations 2023*, s. 240.

40. The *Enhancing Online Safety Act 2015* is no longer in force. It seems to have been replaced by the *Online Safety Act 2021*.

41. Australian Government, *Online Safety Act 2021*.

42. Australian Government, eSafety Commissioner, *Learn about the Online Safety Act*, 18 March 2024.

43. *United States Code*, "Protection for private blocking and screening of offensive material," Title 47, c. 5, §230.

44. United States, House of Representatives, *H.R. 1865 – Allow States and Victims to Fight Online Sex Trafficking Act of 2017*, 115th Congress, 2018 (subsection (e)(5), Public Law 115-164, added par. (5)).

45. 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).

46. 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 (s. 4(8)).

47. *Criminal Code*, s. 83.222(8).

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

49. A deepfake is an image or recording that has been altered to convincingly make an individual look or sound like someone else. See Government of Canada, *Deepfakes: A Real Threat to a Canadian Future*.

50. See section 162.1(2) of the Code.

51. Because the material would be considered "child pornography" (see section 163.1(1) of the Code).

52. Canadian Radio-television and Telecommunications Commission, *Frequently asked questions*.

53. Under the European *Digital Services Act*, very large online platforms and very large online search engines must give access to their algorithmic systems (articles 40(3), 69(2)(d), 69(5) and 72(1)).

54. *Federal Courts Rules*, SOR/98-106, s. 429. Failure to abide by a compliance order may result in asset confiscation or time in custody for the order recipient, meaning the owner or the director or officer of the corporation if the offender is a corporation. Under the European *Digital Services Act*, when the infringement entails a criminal offence involving a threat to the life or safety of persons, a member state can restrict access to the platform in that country (articles 51(3) and 82).

55. Penalties are enforceable through the Federal Court, like a court judgment (section 112). Penalties are paid to the federal government and not the Commission itself (section 111).

56. Online Harms Act, s. 116. The Commission can proceed by either an administrative monetary penalty (violation) or a fine (if charged as an offence), but not both, with respect to a single act or omission. The accused person or operator is not subject to double jeopardy.

57. The Commission can require an operator to provide information related to determining their gross global revenue or whether they committed a violation (section 117), or require a person that has committed a violation to publish a notice containing their name, the act or omission that caused the violation, and any penalty imposed (section 119). Failure to comply with these requirements can result in an administrative monetary penalty or a fine.

58. Online Harms Act, s. 93.

59. Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (Digital Charter Implementation Act, 2022), 44th Parliament, 1st Session.

60. Hate propaganda offences were largely inspired by provisions addressing sedition and defamation (Special Committee on Hate Propaganda in Canada, *Report to the Minister of Justice of the Special Committee on Hate Propaganda in Canada*, 1965, pp. 61 and 73). Over the years, these offences have been modified somewhat, for example by changing the definition of "identifiable group" or what is an acceptable defence. Recently, in 2022, section 319(2.1) (wilful promotion of antisemitism) was added to the Code.

61. The *International Convention on the Elimination of All Forms of Racial Discrimination* was adopted on 21 December 1965 and ratified by Canada, see Article 4. Other treaties with obligations to address hateful content include the *Convention on the Prevention and Punishment of the Crime of Genocide* and the *International Covenant on Civil and Political Rights*.

62. Government of Canada, *International Convention on the Elimination of All Forms of Racial Discrimination: Nineteenth and Twentieth Reports of Canada*, 2011, pp. 21–24; Committee on the Elimination of Racial Discrimination, *Consideration of reports submitted by States parties under article 9 of the Convention: Twenty-first to twenty-third periodic reports of States parties due in 2015*, United Nations, 8 June 2016 (date received: 13 May 2016), p. 4; and Committee on the Elimination of Racial Discrimination, *Concluding observations on the combined twenty-first to twenty-third periodic reports of Canada*, United Nations, 13 September 2017, paras. 11–14(e). The Committee on the Elimination of Racial Discrimination notes that the legislative framework is not yet in place across Canada and that detailed information on hate crimes, particularly within the legal system, is lacking.

63. Anna Ndegwa and Susan McDonald, "Hate crimes in Canada," in *Victims of Crime Research Digest*, Catalogue no. J12-3E-PDF, Department of Justice Canada, 2023, p. 10.

64. Statistics Canada, *Police-reported hate crimes*, 2022, p. 2 (see first inset).

65. Section 318(4) of the Code defines "identifiable group."

66. *Saskatchewan Human Rights Code*, S.S. 1979, c. S-24.1, has since been replaced by the *Saskatchewan Human Rights Code, 2018*, S.S. 2018, c. S-24.2, s. 14.

67. *Saskatchewan (Human Rights Commission) v. Whatcott*, 2013 SCC 11; *Canada (Human Rights Commission) v. Taylor*, [1990] 3 S.C.R. 892; *R. v. Keegstra*, [1990] 3 S.C.R. 697; and *R. v. Andrews*, [1990] 3 S.C.R. 870.

68. *Saskatchewan (Human Rights Commission) v. Whatcott*, 2013 SCC 11, paras 39-46; *Canada (Human Rights Commission) v. Taylor*, [1990] 3 S.C.R. 892; *R. v. Keegstra*, [1990] 3 S.C.R. 697; and *R. v. Andrews*, [1990] 3 S.C.R. 870.

69. *Saskatchewan (Human Rights Commission) v. Whatcott*, 2013 SCC 11, para. 44:

> In the years following *Taylor*, there has been considerable human rights jurisprudence and academic commentary about what constitutes hate speech. The types of expression and devices used to expose groups to hatred were summarized as the "hallmarks of hate" enumerated in *Warman v. Kouba*, 2006 CHRT 50 (CanLII), at paras. 24–81.
>
> …
>
> [The] courts have been guided by the *Taylor* definition of hatred and have generally identified only extreme and egregious examples of delegitimizing expression as hate speech. This approach excludes merely offensive or hurtful expression from the ambit of the provision and respects the legislature's choice of a prohibition predicated on "hatred."

70. See *Criminal Code*, ss. 718–718.21.

71. Canadian Heritage, *Backgrounder – Government of Canada introduces legislation to combat harmful content online, including the sexual exploitation of children*, 26 February 2024.

72. *R. v. Keegstra*, [1990] 3 S.C.R. 697.

73. *Saskatchewan (Human Rights Commission) v. Whatcott*, 2013 SCC 11, para. 41.

74. Expressed as "des préjugés" in the French version of the Code.

75. In the French version of the Code, this is expressed by preceding the list of grounds with the phrase "des facteurs tels que."

76. Kundera Provost-Yombo, Cynthia Louden and Susan McDonald, *Hate as an Aggravating Factor at Sentencing: A Review of the Case Law from 2007–2020*, Department of Justice Canada, 2020.

77. A recognizance is not the same as a restraining order; the latter is most often ordered through the family courts and under provincial rules, rather than through the criminal courts. For more information, see Government of Canada, "Peace Bonds Fact Sheet," *Victims' Rights in Canada*.

78. See *R. v. Penunsi*, 2019 SCC 39, paras. 78–80.

79. Part 3 of the *Samples of Bodily Substances Regulations* (SOR/2014-304) sets out various procedural elements that concern samples of bodily substances provided by defendants in compliance with conditions added to a recognizance. Other related regulations under the Code include: *Blood Drug Concentration Regulations*, SOR/2018-148; *Approved Drug Screening Equipment Order*, SOR/2018-179; *Approved Breath Analysis Instruments Order*, SI/85-201; *Order Approving Blood Sample Containers*, SOR/2005-37; and *Approved Screening Devices Order*, SI/85-200.

80. *R. v. Penunsi*, 2019 SCC 39, paras. 28 and 29.

81. For example, an individual who has committed such an offence can be subject to the post-statutory release detention provisions found at sections 129 to 132 of the *Corrections and Conditional Release Act*.

82. *An Act to amend the Canadian Human Rights Act (protecting freedom)* S.C. 2013, c. 37 (Bill C-304). See the version of section 13 before it was repealed.

83. House of Commons, Standing Committee on Justice and Human Rights, *Evidence*, Meeting 032, 26 April 2012, 1115.

84. Richard Moon, Canadian Human Rights Commission, *Report to the Canadian Human Rights Commission Concerning Section 13 of the* Canadian Human Rights Act *and the Regulation of Hate Speech on the Internet*, October 2008.

85. Minister of Public Works and Government Services, *Special Report to Parliament: Freedom of Expression and Freedom from Hate in the Internet Age*, Canadian Human Rights Commission, June 2009.

86. This addresses one of the major criticisms of the previous version of section 13. See *Canada (Human Rights Commission) v. Taylor*, [1990] 3 S.C.R. 892, McLachlin, J (dissenting in part).

87. Existing obligations under the *Broadcasting Act* (S.C. 1991, c. 11) include restrictions on licensees distributing abusive content that "is likely to expose an individual or group or class of individuals to hatred or contempt on the basis of race, national or ethnic origin, colour, religion, sex, sexual orientation, age or mental or physical disability." (Section 8(1) of the *Broadcasting Distribution Regulations* (SOR/97-555))

88. Pursuant to clause 35, this exception will be replaced, on a date to be fixed by an order in council, to instead reference the substantially similar definition of "social media service" set out in section 2(1) of the Online Harms Act.

89. *Internet Child Pornography Reporting Regulations*, SOR/2011-292.

90. Public Safety Canada, *Mandatory Reporting Act and Jurisdiction Challenges*, 30 March 2021.

91. Clause 49 provides that the Governor in Council may specify the services included in the definition of "Internet service."

92. Reasonable grounds to *believe* involve believing in the *probability* that certain facts or a certain situation exists. It is a higher standard of proof than that of reasonable grounds to *suspect*, which engages simply *possibility* rather than probability. See *R. v. Chehil*, 2013 SCC 49, paras. 27 and 28. This belief may be supported by their own conclusions or by a notice sent by a member of the public or an organization.

93. 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, p. 30.

94. Transmission data is defined in section 487.011 of the *Criminal Code* as relating to the telecommunication functions of routing and addressing, as well as date and time. Transmission data does not reveal the contents of the communication. The Supreme Court of Canada's decision in *R. v. Bykovets* (2024 SCC 6) could affect the application of this bill, as it restricts the police's power to investigate by extending a reasonable expectation of privacy to IP addresses. In the United States, Internet service providers may include in their reports many additional types of information (see *United States Code*, "Sexual Exploitation and Other Abuse of Children," 18 USC, c. 110, section 2258A(b)).

95. *Internet Child Pornography Reporting Regulations*, SOR/2011-292, s. 11.

96. Section 1(1) of the Mandatory Reporting Act defines quite broadly what constitutes "computer data." The same definition is provided in section 342.1(2) of the *Criminal Code*.

97. Bill C-291, An Act to amend the Criminal Code and to make consequential amendments to other Acts (child sexual abuse and exploitation material), 44th Parliament, 1st Session.

98. The use of the term "child pornography" is to be avoided, as it may suggest that the offence resulted from an act carried out with the child's consent. It may also lead to a representation of the child engaging in sexually explicit behaviour, disassociating the child from their status as a victim of sexual exploitation and abuse. The association between the words "pornography" and "child" may detract from the seriousness of the crime experienced by the child. The term "material" would be more accurate, referring to the methods by which sexual violence is shared (audio, written, video and image files) while expressing that each of these materials captures a situation of abuse experienced by a child. See Royal Canadian Mounted Police, *Online child sexual exploitation*; and Interagency Working Group on the Sexual Exploitation of Children, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, 2016.