



Government
of Canada

Gouvernement
du Canada

[Canada.ca](#) > [Canadian Heritage](#)

> [The Government's commitment to address online safety.](#)

Technical paper

The aim of this discussion paper is to present a proposed framework for an Act of Parliament. It reflects one of several possible approaches. The paper does not imply approval by any party of the approaches or concepts in it. Any eventual Act may be supplemented by regulations made under the Act.

On this page

- [Module 1\(A\): New legislative and regulatory framework](#)
 - [Interpretation](#)
 - [Application](#)
- [Module 1\(B\): New rules and obligations](#)
 - [General obligations](#)
 - [Incident response protocol](#)
 - [Reporting and preservation obligations](#)
 - [Publication of proposed regulations](#)
- [Module 1\(C\): Establishment of the new regulators](#)
 - [Digital safety Commissioner](#)
 - [Establishment and functions](#)
 - [Composition](#)
 - [Policy direction](#)
 - [Complaints regime](#)
 - [Digital Recourse Council of Canada](#)
 - [Establishment and functions](#)
 - [Composition](#)

- Complaints regime
- Rules
- Digital safety commission
- Regulatory charges
- Advisory board
- Reporting
- Module 1(D): Regulatory powers and enforcement
 - Compliance orders
 - Publishing decisions and orders
 - Information sharing
 - Inspection Powers
 - Administrative monetary penalties (AMPs)
 - Determination of violation and recommendation of an AMP
 - Issuance of an AMP
 - Due diligence defence
 - Submission of information
 - Responsibility
 - Publication and administration
 - Opt for AMP or prosecution
 - Debt due to the Crown
 - Regulation-making power of the Governor in Council
 - Entry into a compliance agreement
 - Offences
 - Exceptional recourse
 - Review of the Act
 - Coming into force
- Module 2: Modifying Canada's existing legal framework
 - An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service (*Mandatory Reporting Act* or MRA)
 - Centralized reporting

- Annual reporting
 - Broad application of MRA - Internet service
 - Extension of data preservation period
 - Information to assist with promoting compliance with the MRA
 - For greater certainty provision for application of privacy law use requirements
 - Provision of transmission data to police
 - Possible variation of no. 7 – provision of basic subscriber information
 - Other
- Canadian Security Intelligence Service Act (CSIS)

List of acronyms and abbreviations

CSIS

Canadian Security Intelligence Service

MRA

An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service referred to as the *Mandatory Reporting Act*

OCS

Online Communication Service

OCSF

Online Communication Service Provider

RCMP

Royal Canadian Mounted Police

AMP

Administrative Monetary Penalty

Tribunal

Personal Information and Data Protection Tribunal

Module 1(A): New legislative and regulatory framework

1. The Act should would be based on the following premises:
 - a. Recognize the many benefits that Online Communication Services (OCSs) bring to Canadian society, such as facilitating communication with friends and family and participation in public discourse, enabling companies to reach domestic and foreign markets, and providing space for activists, organizations, and civil society to organize and share their messages;
 - b. Recognize that OCSs can be used as a tool to spread harmful content;
 - c. Consider that the hatred spread online often has a disproportionate impact on women, Indigenous Peoples, members of racialized and religious minority communities and on LGBTQ2 and gender-diverse communities and persons with disabilities;
 - d. Consider that OCSs are used to spread propaganda, recruit, organize and incite violence, and that terrorist content online often leads to violence in the physical world;
 - e. Consider that OCSs are used to share content depicting real-world acts of violence in an effort to incite violence, intimidate the public or segments of the public, and damage societal cohesion;
 - f. Consider that OCSs are used to sexually exploit children online, and that such exploitation can have life-long consequences for victims;
 - g. Consider that OCSs are used to share the sexual content of others without their consent, resulting in life-long consequences

including re-victimization; and

- h. Respect and protect the ability of peoples in Canada to fully participate in public discourse free from harm, while protecting fundamental freedoms and human rights.

Interpretation

2. The Act should define the term Online Communication Service (OCS) as a service that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the internet. It should exclude services that enable persons to engage only in private communications.
3. The Act should provide that the Governor in Council may, after consultation with the Digital Safety Commissioner, make regulations (a) excluding a category of services from the definition of OCS; (b) specifying a category of services that is to be included by regulations, notwithstanding that it does not meet the definition of OCS, if the Governor in Council is satisfied that there is a significant risk that harmful content is being communicated on the category of services or that specifying the category of services would further the objectives of this Act; and (c) respecting the meaning of the term private communications for the purposes of the definition of OCS.
4. The Act should provide that Online Communication Service Provider (OCSP) means a person who provides an OCS. It should not include a person who provides only a telecommunications service, as those terms are defined in subsection 2(1) of the *Telecommunications Act*, by reason only that another person uses their telecommunications service or telecommunications facility to provide an OCS. It should not include a person who indicates the existence or location of content or hosts or caches the content or information about the

location of the content, by reason only that another person uses their services to provide an OCS.

5. The Act should ensure that the Digital Safety Commissioner may collect information from OCSPs to determine the application of the Act. The Act should ensure that the Digital Safety Commissioner is required to share the necessary information with the Minister, such as the nature of certain services, to help inform the regulations issued by the Governor in Council concerning the application of the Act.

Application

6. The Act should ensure that it applies to all regulated Online Communication Services (OCSs), and Online Communication Service Providers (OCSPs) that are the closest legal entity to a regulated OCS, that provide services to peoples in Canada.
7. The Act, including any statutory and regulatory obligation imposed on OCSPs, should apply with respect to the five (5) types of harmful content described below.
8. The Act should provide definitions for the five (5) types of harmful content according to the following concepts. The Act should ensure that the definitions borrow from the Criminal Code but are adapted to the regulatory context.

The concept of child sexual exploitation content should capture 1) criminal law offences in this area set out in the Criminal Code, in a manner adapted to a regulatory context, including child pornography and other sexual offences relating to children; and 2) material relating to child sexual exploitation activities that may not constitute a criminal offence, but when posted on an OCS is still harmful to children and victims (e.g., screen shots of videos that do

not include the criminal activity but refer to it obliquely; up-to-date photos of adults who were exploited/ abused as children being posted in the context of their exploitation and abuse as children).

The concept of terrorist content, should refer to content that actively encourages terrorism and which is likely to result in terrorism.

The concept of content that incites violence should refer to content that actively encourages or threatens violence and which is likely to result in violence.

The concept of hate speech should be defined in the same way as it is defined under the amended Canadian Human Rights Act, and hate speech should only be considered as harmful content for the purpose of the Act when communicated in a context in which it is likely to cause harms identified by the Supreme Court of Canada and in a manner identified by the Court in its hate speech jurisprudence.

The concept of non-consensual sharing of intimate images should consider criminal law offences in this area set out in the Criminal Code, in a manner adapted to the regulatory context, with the intent to capture the communication of an intimate image of a person that the person depicted in the image or video did not give their consent to distributing, or for which it is not possible to assess if a consent to the distribution was given by the person depicted in the image or video.

9. The Act should provide authority for the Governor in Council to, by regulation, further define certain specific terms used in the definitions of harmful content.

Module 1(B): New rules and obligations

General obligations

10. The Act should provide that an OCSP must take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada, as may be prescribed through regulations by the Digital Safety Commissioner, on approval by the Governor in Council.
 - a. The Act should provide that an OCSP must take measures to ensure that the implementation and operation of the procedures, practices, rules and systems, including any automated decision making, put in place for the purpose of moderating harmful content that is communicated on its OCS and that is accessible to persons in Canada, do not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act and in accordance with regulations.
11. [A] The Act should provide that an OCSP must address all content that is flagged by any person in Canada as harmful content, expeditiously after the content has been flagged.
 - a. [B] The Act should provide that for part [A], “expeditiously” is to be defined as twenty-four (24) hours from the content being flagged, or such other period of time as may be prescribed by the Governor in Council through regulations.
 - b. The Act should provide that in respect of part [A], “address” signifies that the OCSP must respond to the affected person stating that the content either a) does not meet the definition of harmful content, or b) does meet the definition of harmful content and has been made inaccessible to persons in Canada. In the latter situation, the OCSP must also make the content inaccessible in Canada within the timeframe required by part

[B], and assess that content with respect to its obligations under parts [E] and [F].

- c. The Act should provide that in prescribing a new timeframe as provided for in part [B], the Governor in Council may prescribe through regulations different timelines for different types or subtypes of harmful content. The Act should provide that the new timeframes could be either extended or shortened from the timeframe provided in part [B].

12. [C] The Act should provide that an OCSP must institute internal procedural safeguards providing users of the service in Canada with the following, as may be prescribed through regulations by the Digital Safety Commissioner, with the approval of the Governor in Council:

- a. accessible and easy-to-use flagging mechanisms for harmful content;
- b. notice of the OCSP's content moderation decision within twenty-four (24) hours of the content being flagged, unless the timeframe is changed by the Governor in Council;
- c. the accessible and easy-to-use opportunity to make representations, and compel an OCSP to promptly review and reconsider its decision; and
- d. notice of the OCSP's decision upon reconsideration, which must be provided without delay, including a notice of the recourse available to the Digital Recourse Council of Canada.

13. The Act should provide that an OCSP must publish clear content-moderation guidelines, applicable to the five (5) types of harmful content, as may be prescribed through regulations by the Digital Safety Commissioner.

14. The Act should provide that an OCSP must generate and provide reports on a scheduled basis to the Digital Safety Commissioner on Canada-specific data about:
- a. the volume and type of harmful content on their OCS;
 - b. the volume and type of content that was accessible to persons in Canada in violation of their community guidelines;
 - c. the volume and type of content moderated;
 - d. resources and personnel allocated to their content moderation activities;
 - e. their content moderation procedures, practices, rules, systems and activities, including automated decisions and community guidelines;
 - f. how they monetize harmful content;
 - g. when relevant, their responses to the activation of the Incident Response Protocol;
 - h. when relevant, information on their (a) notifications to the Royal Canadian Mounted Police (RCMP) or (b) reporting to law enforcement as provided for in part [E], including:
 - I. the volume and type of these reports or notifications;
 - II. anonymized and disaggregated information about the kinds of demographics implicated; and
 - III. the amount and kind of data and information that was preserved, as prescribed through regulations by the Digital Safety Commissioner.
15. The Act should provide that an OCSP must maintain records as necessary for the proper administration of the Act, in accordance with the requirements set out in the Act or prescribed through

regulations by the Digital Safety Commissioner, or as otherwise required by law.

16. The Act should provide that an OCSP may seek advice on content moderation processes and practices with respect to the five (5) types of harmful content from the Digital Safety Commissioner, as may be prescribed through regulations by the Digital Safety Commissioner, with the approval of the Governor in Council. The Act should ensure that the OCSP may not seek advice on specific content-moderation decisions.
17. The Act should provide that the Digital Safety Commissioner may make regulations regarding the manner in which OCSPs are to comply with legislated obligations contemplated by this section. The Act should ensure that the Digital Safety Commissioner is authorized to tailor regulatory requirements to different categories of OCSPs, prescribing, in regulations, the manner in which regulatory obligations are to be fulfilled, and recognizing the distinct business models, sizes, and resources of various OCSPs.

Incident response protocol

18. [D] The Act should provide the Digital Safety Commissioner with the authority, with the approval of the Governor in Council, to establish an Incident Response Protocol for the purpose of implementing the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online and reducing the online communication of content relating to terrorist activities. The Incident Response Protocol would respond to an act or omission as described in the definition of “terrorist content” tied to an emergent, ongoing, or recently concluded real-world attack in Canada, or outside of Canada when content is shared on one or more Canadian-based OCSs.

19. The Act should provide the Governor in Council with the authority to make regulations regarding the Incident Response Protocol, including but not limited to: further clarifying content subject to the Incident Response Protocol, the process for activating and concluding the protocol, as well as any other relevant aspects to ensure that the protocol meets its goals.

Reporting and preservation obligations

20. [E] The Act should either: ¹

- a. require that an OCSP notify the RCMP in circumstances where the OCSP has reasonable grounds to suspect that content falling within the five (5) categories of regulated harmful content reflects an imminent risk of serious harm to any person or to property, as may be prescribed through regulations established by the Governor in Council;
- or
- b. provide that an OCSP must report prescribed information in respect of prescribed criminal offences falling within the five (5) categories of regulated harmful content to prescribed law enforcement officers or agencies, as may be prescribed through regulations established by the Governor in Council.

The Act should ensure that the Governor in Council may specify, through regulations, the manner in which OCSPs are to comply with this obligation, such as the timing of (a) notifications or (b) reporting, the information that is to be contained in the (a) notifications or (b) reports, the thresholds and guidance for (a) determining if content falls within the obligation or (b) reporting different types of offences, and the format of the (a) notifications or (b) reports.

21. The Act should provide that if an OCSP is subject to domestic or foreign legislation that requires the reporting, notification and/or preservation of information in relation to certain offences (such as child pornography offences), they are to comply with that legislation and nothing in the Act trumps, detracts from, or alleviates the obligations that exist on OCSPs to report, notify and/or preserve in accordance with that legislation. The Act should provide that if an OCSP reports, notifies and/or preserves in accordance with that domestic or foreign legislation, they are deemed to have complied with their obligations under parts [E] and [F].
22. (approach (b) only) The Act should provide that an OCSP shall report information respecting terrorist content and content that incites violence that will be made inaccessible in accordance with this legislation to the Canadian Security Intelligence Service (CSIS) in a manner that conforms to Governor in Council regulations relating to the threshold, timing, format and any other requirements for such reports.
23. [F] The Act should provide that an OCSP must preserve data and information in their possession or control pertinent to (1) reports provided to law enforcement or notifications provided to the RCMP under part [E] and (2) potentially illegal content falling within the five (5) categories of regulated harmful content, as may be prescribed through regulations established by the Governor in Council. The Act should ensure that the Governor in Council may specify, through regulations, the manner in which OCSPs are to comply with this obligation, such as the nature of such data and information to be preserved, the time period for preservation, the format of the data and information, the security measures for preserved data, the threshold for what constitutes potentially illegal content, and the conditions under which it can be accessed. The Act should ensure that this data and information includes basic subscriber information.

The Act should ensure that the preservation obligation also extends to and includes content that is subject to the Incident Response Protocol in part [D]. The Act should ensure that OCSPs must preserve all data and information in their possession or control regarding content falling within the five (5) categories of regulated harmful content that reflects an imminent risk of serious harm to any person or to property or prescribed potentially illegal content, from the moment the content is identified or flagged as prescribed content on their respective OCSs.

24. The Act should provide that OCSPs must preserve data and information, as contemplated by part [F] in a secure-manner in cases where they are required to (a) notify the RCMP or (b) report to law enforcement and CSIS, as contemplated by part [E].
25. The Act should provide that after a prescribed period of time, determined by the Governor in Council through regulations, the OCSP must destroy preserved data and information, as contemplated by part [F], that would not be retained in the ordinary course of business, unless the OCSP is required by law to continue preserving that data or information.
26. The Act should provide that an OCSP must not disclose that it has (a) issued a notification to the RCMP or (b) issued a report to law enforcement and CSIS or disclose the contents of (a) a notification or (b) a report, if the disclosure could prejudice a criminal investigation, whether or not a criminal investigation has begun.
27. (approach (b) only) The Act should provide that an OCSP must not disclose that it has made a report to CSIS or disclose the contents of a report made to CSIS, if the disclosure could be injurious to national security.
28. The Act should ensure that it does not limit disclosures that might otherwise lawfully be made to law enforcement.

29. The Act should provide that an OCSP must take all reasonable measures, including by performing regular checks on its own activities, to ensure that its (a) notifications to the RCMP or (b) reports to law enforcement and CSIS, as contemplated by part [E], including its internal processes and automated systems, do not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act and in accordance with regulations.
30. The Act should provide that nothing in the Act requires or authorizes an OCSP to proactively seek out illegal content outside of the five (5) categories of regulated harmful content.
31. The Act should provide that OCSPs making (a) notifications to the RCMP or (b) reports to law enforcement and CSIS in good faith pursuant to the Act should have immunity from civil and criminal proceedings.
32. The Act should provide the Governor in Council with the authority to make regulations with respect to the use and subsequent disclosures of information provided to (a) the RCMP or (b) law enforcement and CSIS under part [E], depending on the privacy interests engaged by that information.
33. The Act should ensure that the Governor in Council may make regulations regarding the manner in which OCSPs are to comply with legislated obligations in relation to parts [E] and [F].

Publication of proposed regulations

34. The Act should provide that a copy of each regulation that the Digital Safety Commissioner proposes to make must be published in the Canada Gazette and a reasonable opportunity must be given to OCSPs and other interested persons to make representations to the Digital Safety Commissioner with respect thereto.

Module 1(C): Establishment of the new regulators

Digital safety Commissioner

Establishment and functions

35. The Act should provide for the establishment of the Digital Safety Commissioner, whose functions are to:

a. Oversee and improve online content moderation, by:

I. Administering and enforcing obligations;

II. Engaging with and considering the particular needs of and barriers faced by groups disproportionately affected by harmful online content such as women and girls, Indigenous Peoples, members of racialized communities and religious minorities and of LGBTQ2 and gender-diverse communities and persons with disabilities; and

III. Supporting platforms in reducing harmful content affecting peoples in Canada.

b. Engage in partnerships, education outreach activities, and research, to help fulfill the policy objectives of the Act.

Composition

36. The Act should provide that the Digital Safety Commissioner and Deputy Digital Safety Commissioner will be appointed by the Governor in Council on a full-time basis.

37. The Act should provide that the Digital Safety Commissioner and Deputy Digital Safety Commissioner will receive the remuneration that is fixed by the Governor in Council.

38. The Act should provide that a person appointed as Commissioner or Deputy Commissioner must declare any conflict of interest, and must not be a shareholder of an OCS or OCSP.

Policy direction

39. The Act should include a policy direction power granting the Governor in Council the ability to issue binding directions on the Digital Safety Commissioner, following consultations with the Digital Safety Commissioner, with respect to broad matters relating to the purposes of the Act.

Complaints regime

40. The Act should provide that an affected person may file written complaints over the Internet to the Digital Safety Commissioner concerning an OCSP's non-compliance with statutory and regulatory obligations concerning procedural safeguards, as contemplated by part [C].
41. The Act should provide that upon receiving a complaint, or detecting OCSP non-compliance with the Act, the Digital Safety Commissioner shall provide affected persons and the relevant OCSP with a notice of the complaint or of the detection of non-compliance, and a date by which to make representations.
42. The Act should provide that the Digital Safety Commissioner may dismiss a complaint it deems to be frivolous, trivial, vexatious, made in bad faith or on other grounds. The Act should provide that if the Digital Safety Commissioner dismisses a complaint, it must provide a notice to the complainant and the OCSP of its decision to dismiss it. The Act should ensure that the Governor in Council may make regulations prescribing other grounds of dismissal.
43. The Act should provide that the Digital Safety Commissioner may hold a hearing concerning any complaint made to it, any detected

non-compliance, or in connection with any other matter within its jurisdiction under this Act, if it is satisfied that it would be in the public interest to do so.

44. The Act should provide that the Digital Safety Commissioner must notify all affected persons of its decision, including their right to appeal a finding of non-compliance with the Personal Information and Data Protection Tribunal (the “Tribunal”), now part of Bill C-11. The Act should ensure that there is a timeline provided for associated with the affected person’s right to appeal the finding of non-compliance.

Digital Recourse Council of Canada

Establishment and functions

45. The Act should provide for the establishment of the Digital Recourse Council of Canada, whose functions are to:
- a. Receive and review complaints by affected persons in Canada stemming from content moderation decisions issued by OCSPs; and
 - b. Issue decisions on such complaints regarding whether content qualifies as harmful content, as defined in legislation.

Composition

46. The Act should provide that the Digital Recourse Council of Canada will be composed of no fewer than three (3) and no more than five (5) members, appointed by the Governor in Council. The Governor in Council will designate one (1) member as the Chairperson and may designate one (1) member as the Vice-Chairperson. The Act should provide that in appointing members, the Governor in Council shall take into consideration the importance of diverse subject-matter experts reflective of the Canadian population, particularly inclusive

of women, Indigenous Peoples, members of racialized communities and religious minorities, of LGBTQ2 and gender-diverse communities, and persons with disabilities.

47. The Act should provide that the Chairperson and Vice-Chairperson are appointed on a full-time basis, but that other members of the Digital Recourse Council of Canada may be appointed either on a full-time or on a part-time basis. The Act should provide that each member will receive the remuneration that is fixed by the Governor in Council.
48. The Act should provide that the Digital Recourse Council of Canada's members must declare any conflict of interest, and must not be a shareholder of an OCS or OCSP.

Complaints regime

49. The Act should provide that the Digital Recourse Council of Canada may receive written complaints sent over the Internet from affected persons concerning:
- a. An OCSP's decision to keep content accessible on its OCS that the complainant believes meets the definition of harmful content; and
 - b. An OCSP's decision to make content on its OCS inaccessible that the complainant believes does not meet the definition of harmful content.
50. The Act should provide that a complainant may only file a complaint with the Digital Recourse Council of Canada after they have gone through the relevant content moderation and reconsideration processes at the OCSP level, as contemplated by part [C].
51. The Act should provide that upon receiving a complaint the Digital Recourse Council of Canada shall provide affected persons and the

relevant OCSF with a notice of the complaint and the opportunity to make representations.

52. The Act should provide that the Digital Recourse Council of Canada may dismiss a complaint it deems to be trivial, frivolous, vexatious, made in bad faith or on other grounds. The Act should provide that if the Digital Recourse Council of Canada dismisses a complaint, it must provide a notice to the complainant and the OCSF of its decision to dismiss it. The Act should ensure that the Governor in Council may make regulations prescribing other grounds of dismissal.
53. The Act should provide that the Digital Recourse Council of Canada may hold a hearing concerning any complaint made to it, if it is satisfied that it would be in the public interest to do so.
54. The Act should provide that if the Digital Recourse Council of Canada finds that the content subject to the complaint does not constitute harmful content, it would communicate this decision to affected persons, including the OCSF. The OCSF would then decide whether to make the content accessible or not, subject to their own guidelines.
55. The Act should provide that if the Digital Recourse Council of Canada finds that the content does constitute harmful content, it would communicate this decision to affected persons, including the OCSF. It would also issue an order to the OCSF to make the content inaccessible to persons in Canada, if the OCSF has not already done so. The Act should ensure that the order contains a timeline for compliance.
56. The Act should provide that the Digital Recourse Council of Canada shall share the inaccessibility order with the Digital Safety Commissioner. The Act should provide that the Digital Safety

Commissioner will monitor OCSP compliance with the inaccessibility order.

Rules

57. The Act should provide that the Governor in Council may make regulations related to the complaint regimes for the Digital Recourse Council and the Digital Safety Commissioner, including timelines associated with complaints submitted.
58. The Act should provide that the Digital Safety Commissioner and the Digital Recourse Council of Canada may conduct hearings by electronic means.
59. The Act should provide that the Digital Safety Commissioner and the Digital Recourse Council of Canada may conduct hearings *in camera* where a public hearing would not be in the public interest, including where there is a privacy interest, national security interest, international relations interest, national defence interest, or confidential commercial interest.

Digital safety commission

60. The Act should provide for the establishment of the Digital Safety Commission for the purpose of supporting the Digital Safety Commissioner, the Digital Recourse Council of Canada, and the Advisory Board in fulfilling their mandates and performing their powers, duties, and functions.
61. The Act should provide for the appointment of a Chief Executive Officer by the Governor in Council. The Act should provide that the Chief Executive Officer is appointed on a full-time basis and paid the remuneration that is fixed by the Governor in Council.
62. The Act should provide that if the Chief Executive Officer is absent or incapacitated or the office of Chief Executive Officer is vacant, the

Minister may designate someone to act as Chief Executive Officer for a period of up to ninety (90) days, after which time Governor in Council approval would be required.

63. The Act should provide that the Chief Executive Officer must not give directions with respect to any particular decision, order or recommendation that is made by the Digital Safety Commissioner or the Digital Recourse Council.
64. The Act should provide that the Chief Executive Officer may engage on a temporary basis the services of persons having technical or specialized knowledge of any matter relating to the work of the Commission, the Digital Safety Commissioner, or the Digital Recourse Council of Canada.
65. The Act should provide that the Digital Safety Commission, Digital Safety Commissioner, and Digital Recourse Council are subject to the Access to Information Act and the Privacy Act.

Regulatory charges

66. The Act should provide that with the approval of the Treasury Board, the Digital Safety Commissioner may make regulations setting regulatory charges that one or more classes of OCSPs must pay, including the time and manner of payment, to recover the costs of the Commission, the Digital Safety Commissioner, and the Digital Recourse Council of Canada related to the administration of the Act. The charges must take into account the ability of the OCSPs to pay. The Act should provide that the Digital Safety Commissioner can set interest payable in respect of any overdue charges.
67. The Act should ensure that the Digital Safety Commissioner may collect information from OCSPs to determine their ability to pay and establish the actual or estimated Canadian revenue for a regulated OCS.

68. The Act should provide that the Digital Safety Commissioner, with the approval of the Governor in Council, may make regulations respecting any other matters as it deems necessary for the purposes of regulatory charges.
69. The Act should provide that subject to conditions imposed by the Treasury Board, the revenue from the regulatory charges received by the Commission, the Digital Safety Commissioner, and the Digital Recourse Council of Canada in a fiscal year for the conduct of their operations may only be spent by these entities for these purposes in that or, unless an appropriation Act provides otherwise, in the next fiscal year.
70. The Act should provide that any charges required to be paid under this section are debts due to Her Majesty the Queen in right of Canada and may be set-off or recovered in Federal Court.

Advisory board

71. The Act should provide for the establishment of an Advisory Board composed of no more than seven (7) members who are appointed by the Minister at pleasure. The Act should provide that the Minister consider the importance of inclusive membership of the Advisory Board reflective of the Canadian population, particularly inclusive of women, Indigenous Peoples, members of racialized communities and religious minorities, of LGBTQ2 and gender-diverse communities, and persons with disabilities.
72. The Act should provide that in appointing members, the Minister take into consideration the importance of having members that are knowledgeable about or have experience related to law, technology, equity and social science, and are drawn from advocacy groups, including civil liberties, equity or victim advocacy organizations, the online communication industry, and academia.

73. The Act should provide that each member of the Advisory Board is appointed on a part-time basis and is paid by the Governor in Council.
74. The Act should provide that the Minister will identify a member of the Advisory Board to be its Chair.
75. The Act should provide that the functions of the Advisory Board are to support and advise the Digital Safety Commissioner and the Digital Recourse Council of Canada by, reporting regularly, and publicly, on emerging industry trends and technologies and on content-moderation practices.

Reporting

76. The Act should provide that within three (3) months after the end of each fiscal year, both the Digital Safety Commissioner and the Digital Recourse Council of Canada must submit reports to the Minister on their activities for that fiscal year.
77. The Act should provide that the Digital Safety Commissioner's annual report must include information about the following, and must include any additional information requested by the Minister:
- a. Complaints received regarding an OCSP's procedural safeguards;
 - b. Decisions issued as a result of the complaints received regarding an OCSP's procedural safeguards;
 - c. Inspections conducted into an OCSP's compliance with statutory and regulatory obligations, including compliance with obligations concerning (a) notifications to the RCMP or (b) reporting to law enforcement or CSIS as contemplated by part [E] and data and information preservation as contemplated by part [F];

- d. Orders made under part [G] requiring OCSPs to comply with statutory and regulatory requirements;
- e. Orders and findings made in relation to the recommendation of an administrative monetary penalty as contemplated by part [H]; and
- f. Information on OCSP compliance with its obligations to (a) notify the RCMP of certain content or (b) report certain information to law enforcement or CSIS, as contemplated by part [E], including the volume and type of these (a) notifications or (b) reports, and anonymized and disaggregated information about the kinds of demographics implicated.

78. The Act should provide that the Digital Recourse Council of Canada's annual report must include information about the following, and must include any additional information requested by the Minister:

- a. Complaints received regarding an OCSP's content moderation decision; and
- b. Decisions issued as a result of the complaints received regarding an OCSP's content moderation decision.

79. The Act should provide that the Minister responsible for the Act may request reports from the Digital Safety Commissioner or the Digital Recourse Council of Canada on any matter within their jurisdiction.

Module 1(D): Regulatory powers and enforcement

Compliance orders

80. [G] The Act should provide that the Digital Safety Commissioner may, by order, require an OCSP to do any act or thing, or refrain from doing anything necessary to ensure compliance with any

obligations imposed on the OCSP by or under the Act within the time specified in the order.

81. The Act should provide that a compliance order may be appealed to the Tribunal (now part of Bill C-11).

Publishing decisions and orders

82. The Act should provide that the Digital Safety Commissioner's orders and decisions and the Digital Recourse Council of Canada's orders must be made in writing and be provided to all affected persons, as well as the affected OCSPs.
83. The Act should provide that the Digital Safety Commissioner and the Digital Recourse Council of Canada's decisions and orders must be made public, but both have discretion over whether to name the OCS and OCSP and the timing of the publication. The Act should provide that in making those decisions and orders public, the Digital Safety Commissioner and the Digital Recourse Council of Canada must not publish the name of the complainant, or poster, or any personal information that may be used to identify the complainant, poster, or an affected person, or any confidential, or commercially sensitive information, or information subject to privilege under the Canada Evidence Act or the CSIS Act.
84. The Act should provide that the Governor in Council may make regulations respecting the publication of the Digital Safety Commissioner and Digital Recourse Council of Canada's decisions and orders.

Information sharing

85. The Act should provide that the Digital Safety Commissioner and the Digital Recourse Council of Canada must share data and information with the Minister responsible for the Act, on request of the Minister,

while maintaining the protection over the information, including allowing OCSPs to designate certain information as confidential, and to further the objectives of this Act.

86. The Act should provide that the Digital Recourse Council of Canada can share information with the Digital Safety Commissioner in order to allow the Commissioner to monitor and determine compliance with the OCSPs' statutory and regulatory obligations.
87. The Act should ensure appropriate information sharing authorities for the Digital Safety Commissioner with respect to interactions with the RCMP and, to the extent advisable and necessary, other law enforcement, national security agencies, and relevant Federal entities, for all implicated entities to have the authority to enable information sharing necessary to the effective fulfillment of their respective mandates, including monitoring of OCSPs obligations under parts [E] and [F].

Inspection Powers

88. The Act should provide that the Digital Safety Commissioner may conduct inspections of OCSPs at any time, on either a routine or ad hoc basis, further to complaints, evidence of non-compliance, or at the Digital Safety Commissioner's own discretion, for the OCSP's compliance with the Act, regulations, decisions and orders related to a regulated OCS.
89. The Act should provide that an inspector may enter, at any reasonable time, any place in which they believe on reasonable grounds there is any document, information or any other thing, including computer algorithms and software, relevant to the purpose of verifying compliance and preventing non-compliance with the Act, regulations, decisions and orders, and examine the

document, information or thing or remove it for examination or reproduction, and:

- a. make use of, or cause to be made use of, any computer system at the place to examine any data contained in or available to the system;
- b. reproduce any document, or cause it to be reproduced, from the data in the form of a print-out, digital copy, or other intelligible output and take the print-out, digital copy, or other output for examination or copying; and
- c. use any copying equipment or means of communication in the place.

90. The Act should provide that an inspector may not enter a dwelling-house without the consent of the occupant or under the authority of a warrant.
91. The Act should provide that an inspector executing a warrant must not use force unless the inspector is accompanied by a peace officer and the use of force has been specifically authorized in the warrant.
92. The Act should provide that an OCSP and the owner or person in charge of a place entered by an inspector must provide all assistance that is reasonably required to enable the inspector to perform their functions under this Act, and must provide any information that is reasonably expected for that purpose.
93. The Act should provide that an inspector who believes that a person is in possession of information that the inspector considers necessary for the purpose of verifying compliance and preventing non-compliance with the Act, regulations, decisions, or orders, may, by notice, require that person to submit the information to the inspector in the form and manner and within the reasonable time that is stipulated in the notice.

Administrative monetary penalties (AMPs)

Determination of violation and recommendation of an AMP

94. [H] The Act should provide that AMPs may be imposed on an OCSP for a violation of the following:

- a. An OCSP does not comply with an inaccessibility order issued by the Digital Recourse Council of Canada;
- b. An OCSP does not comply with a compliance order issued by the Digital Safety Commissioner;
- c. An OCSP does not comply with a compliance agreement;
- d. An OCSP fails to submit information when required to do so by notice by a person designated by the Digital Safety Commissioner;
- e. An OCSP knowingly makes a material misrepresentation of fact or an intentional omission to state material facts to a person designated by the Digital Safety Commissioner;
- f. An OCSP resists or obstructs the Digital Safety Commissioner or its delegate, including an inspector in conducting its inspection powers; and
- g. Any other violations of the Act or regulations except [K].

95. The Act should provide that this recommendation would be made to the Tribunal, to be established under Bill C-11, which will be authorized to impose AMPs.

96. The Act should provide that the Digital Safety Commissioner must provide the OCSP, and the complainant, if there is one, with a notice providing for the opportunity to make representations. The Act should provide that following these representations, the Commissioner may issue a notice of decision and cause it to be

served on the relevant OCSP, and provide a copy to the complainant and the Tribunal.

97. The Act should provide that the Digital Safety Commissioner must issue a notice containing a decision on whether the OCSP committed a violation, which must include:

- a. the name the OCSP believed to have committed the violation;
- b. the violation and provision(s) at issue;
- c. the compliance order, if the Commissioner decides to issue one;
- d. the opportunity to enter into a compliance agreement;
- e. the AMP recommendation, including a recommended penalty amount, if the Commission decides to issue a recommendation; and
- f. the rights and obligations of the OCSP.

98. The Act should provide that the Digital Safety Commissioner must take the following factors into consideration when recommending whether the Tribunal should issue an AMP:

- a. the nature and scope of the violation;
- b. whether the OCSP has voluntarily paid compensation to a person affected by the contravention;
- c. the OCSP's ability to pay the penalty and the likely effect of paying it on the OCSP's ability to carry on its business;
- d. any financial benefit that the OCSP obtained from the contravention;
- e. the OCSP's history of compliance with the Act; and
- f. any other relevant factor.

99. The Act should provide that an OCSP served with a notice, or a complainant that receives a notice, may, within thirty (30) days,

appeal the finding of non-compliance, the compliance order, or the decision not to recommend an AMP to the Tribunal.

100. The Act should provide that if an OCSP does not appeal the finding of non-compliance or the compliance order within the time and manner specified in the notice, the Tribunal may proceed with the Digital Safety Commissioner's recommendation to issue an AMP.
101. The Act should provide that no proceeding in respect of a violation may be commenced later than one (1) year after the day on which the subject matter of the proceedings became known to the Digital Safety Commissioner. The Act should provide that the Commissioner may extend the time limit, for a period not exceeding one (1) year, by notifying the affected persons and the OCSP of the anticipate date on which the decision is to be made.

Issuance of an AMP

102. The Act should provide that the following provisions are to be harmonized with the possible coming into force of the *Personal Information and Data Protection Tribunal Act* (now part of Bill C-11).
103. The Act should provide that the mandate of the Tribunal is to provide an expedited process for appealing findings of non-compliance, compliance orders, and decisions not to recommend AMPs from the Digital Safety Commissioner, and to issue AMPs for violations of the Act following a recommendation from the Digital Safety Commissioner.
104. The Act should provide that, following a recommendation from the Digital Safety Commissioner to impose an AMP, the Tribunal will determine, on the basis of the Digital Safety Commissioner's findings, unless varied by the Tribunal on appeal, and in accordance with the factors set out in part [I], whether an AMP is appropriate. The Act should provide that the Tribunal may establish the amount

of the AMP in accordance with the factors set out in part [I], and in accordance with the amounts set out in part [J]. If the Tribunal determines that an AMP is appropriate, it may make an order for the OCSP to pay an AMP.

105. The Act should provide that the Tribunal may dismiss an appeal.
106. The Act should provide that the Tribunal's power to order AMPs is to promote compliance with the Act, its regulations and the decisions made by the Digital Safety Commissioner and the Digital Recourse Council of Canada under the Act, and not to punish.
107. [I] The Act should provide that the Tribunal must take the following factors into consideration when determining whether to issue an AMP, and the amount of an AMP if one is to be issued:
- a. the nature and scope of the violation;
 - b. whether the OCSP has voluntarily paid compensation to a person affected by the contravention;
 - c. the OCSP's ability to pay the penalty and the likely effect of paying it on the OCSP's ability to carry on its business;
 - d. any financial benefit that the OCSP obtained from the contravention;
 - e. the OCSP's history of compliance with this Act; and
 - f. any other relevant factor.
108. [J] The Act should provide that the Tribunal may order an AMP in respect of a matter in an amount up to three (3) percent of the OCSP's gross global revenue or up to ten million dollars (\$10,000,000), whichever is higher. The Act should provide that this amount is calculated based on the gross global revenue of the OCSP for the preceding fiscal year in which the decision is made.

109. The Act should provide that a decision of the Digital Safety Commissioner, the Digital Recourse Council of Canada, or the Tribunal that is final may be filed with the Federal Court of Canada and, after filing, the order is enforceable as a judgment or order of that Court.

Due diligence defence

110. The Act should provide that due diligence is a defence in an administrative proceeding resulting from an alleged violation of any prohibition described above, other than a violation containing a mental element.

Submission of information

111. The Act should provide that if the Digital Safety Commissioner believes that an OCSP is in possession of information that is reasonably considered to be relevant to verifying whether a violation has been committed, the Digital Safety Commissioner may, by notice, require that OCSP to submit the information in the form and manner and within the time that is stipulated in the notice.

Responsibility

112. The Act should provide that it is sufficient proof of a violation to establish that an employee or agent of an OCSP commits the violation.

Publication and administration

113. The Act should provide that the Digital Safety Commissioner may publish or require an OCSP to publish:

- a. the name of the OCSP who is deemed, or is found by Tribunal, to have committed a violation, the acts or omissions and provisions at issue and the amount payable as a result, if any; or

- b. the name of the OCSP who enters into a compliance agreement, the nature of the compliance agreement including the acts or omissions and provisions at issue, the conditions included in the compliance agreement and the amount payable under, if any.

Opt for AMP or prosecution

114. The Act should provide that where an act or omission may be enforced either as a violation or as an offence under this Act, proceeding in one manner precludes proceeding in the other.

Debt due to the Crown

115. The Act should provide that any unpaid amount of an AMP or unpaid amount under a compliance agreement, and any reasonable expenses incurred in an attempt to recover any such amount, is a debt due to the Crown and may be registered as a judgment of the Federal Court and, upon registration, may be enforced as a judgment of that Court.

Regulation-making power of the Governor in Council

116. The Act should provide that the Governor in Council may make regulations in relation to the AMPs regime, respecting compliance agreements entered into, and respecting service of documents required or authorized to be served.

Entry into a compliance agreement

117. The Act should provide that an OCSP may enter into a compliance agreement with the Digital Safety Commissioner at any time prior to the Tribunal issuing the AMP.
118. The Act should provide that a compliance agreement:
- a. can be accepted by the Digital Safety Commissioner;

- b. must identify every act or omission that is covered by the compliance agreement;
- c. must identify every statutory or regulatory provision at issue;
- d. may contain any conditions that the Digital Safety Commissioner considers appropriate; and
- e. may include a requirement to pay a specified amount.

Offences

119. [K] The Act should provide that every OCSP that fails to comply with a compliance agreement entered into with the Digital Safety Commissioner, that fails to adhere to an inaccessibility order issued by the Digital Recourse Council of Canada or an order issued by the Digital Safety Commissioner or its delegates, that resists or obstructs the Digital Safety Commissioner or its delegate, including an inspector in conducting its inspection powers or that knowingly makes a false or misleading statement, either orally or in writing, to the Digital Safety Commissioner, the Digital Recourse Council of Canada, or their delegates, including to an inspector, can be found guilty of

- a. an offence punishable on summary conviction and liable to a fine not exceeding four (4) percent of global revenues in the financial year that precedes the date of sentencing or twenty million dollars (\$20,000,000), whichever is higher; or
- b. an indictable offence and liable to a fine not exceeding five (5) percent of gross global revenues in the financial year that precedes the date of sentencing or twenty-five million dollars (\$25,000,000), whichever is higher.

Exceptional recourse

120. The Act should provide the Digital Safety Commissioner with the authority to apply to the Federal Court for an order requiring relevant Telecommunications Service Providers, as defined in subsection 2(1) of the *Telecommunications Act*, to block access in whole or in part to an offending OCS in Canada, if:
- a. an OCSP repeatedly demonstrates persistent non-compliance with orders solely with respect to removing the following harmful content:
 - I. child sexual exploitation content, or
 - II. terrorist content; and
 - b. all enforcement measures have been exhausted.
121. The Act should ensure that, for the purposes of each court application, the order that the Digital Safety Commissioner seeks is proportionate in the circumstances, considering the level of non-compliance and potential effects of the order, such as excessive blocking.
122. The Act should provide that the Governor in Council may make regulations generally to carry out the purposes and provisions related to the exceptional recourse, and to establish additional conditions or factors to be taken into account by the Commissioner in determining whether to apply to the Federal Court.
123. The Act should provide a correlating provision to ensure that the prohibition set out in section 36 of the *Telecommunications Act* does not apply to Canadian carriers that comply with a blocking order referred to in this section.

Review of the Act

124. The Act should provide that the Minister must, two (2) years after the day on which this provision comes into force, undertake a review

of the provisions and operation of the Act. The Act should provide that the Minister must publicly announce that it will undertake this review.

125. The Act should provide that the Minister must, no later than one (1) year after the day on which the review is undertaken, cause a report on the review to be tabled in each House of Parliament.

Coming into force

126. The Act should provide that it will come into force on a date or dates to be determined by the Governor in Council.

Module 2: Modifying Canada's existing legal framework

An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service (*Mandatory Reporting Act* or MRA)

Centralized reporting

1. The Act should amend the *Mandatory Reporting Act* to create a regulation making power in respect of designating a law enforcement body for the purpose receiving reports made under section 3 of the *Mandatory Reporting Act*. The intent would be to centralize reporting by designating the National Child Exploitation Crime Centre (NCECC), which is the relevant expert group within the RCMP, in the *Mandatory Reporting Act* regulations.

Annual reporting

2. The Act should amend the *Mandatory Reporting Act* to create a regulation making power in relation to the duties and the functions of the law enforcement body designated by the regulations for the

purpose of receiving reports under section 3 of the *Mandatory Reporting Act*. The intent would be to create obligations for annual reports by the RCMP NCECC under the regulations.

Broad application of MRA - Internet service

3. The Act should amend the *Mandatory Reporting Act* to ensure that it applies broadly to all types of Internet services and that definitions are sufficiently flexible and non-exhaustive to encompass rapidly evolving technological developments.

Extension of data preservation period

4. The Act should amend the *Mandatory Reporting Act* to change the requirement for data preservation in subsection 4(1) and the requirement for destruction of preserved computer data in subsection 4(2) to replace twenty-one (21) days with three-hundred and sixty-five (365) days or one (1) year.

Information to assist with promoting compliance with the MRA

5. The Act should amend the *Mandatory Reporting Act* to ensure there is authority for a person designated in regulations to collect information to determine the application of the *Mandatory Reporting Act*. The intent is that the person designated for this function would be the Digital Safety Commissioner.

For greater certainty provision for application of privacy law use requirements

6. The Act should ensure that there is no uncertainty that, when using personal information obtained pursuant to the *Mandatory Reporting Act*, the police would be bound by the use limitations in federal legislation (the *Privacy Act*) for federal police and comparable provincial legislation for provincial and municipal police.

Provision of transmission data to police

7. The Act should amend the *Mandatory Reporting Act* to require provision of relevant transmission data, as defined by section 487.011 of the *Criminal Code*, related to the reported offence, when making a report to the designated law enforcement body under section 3 of the *Mandatory Reporting Act*. Transmission data would only be provided in relation to section 3 reports where it was clearly evident that the material related to the offence was child pornography.

Possible variation of no. 7 – provision of basic subscriber information

8. The Act should amend the *Mandatory Reporting Act* to require provision of relevant basic subscriber information such as name, address, telephone number and IP address with date and time, as well as other basic identifiers that the company may have at its disposal, related to the reported offence, when making a report to the designated law enforcement body under section 3. The basic subscriber information would only be provided in relation to section 3 reports where it was clearly evident that the material related to the offence was child pornography.

Other

9. The Act should make any amendments to the regulatory authorities in the *Mandatory Reporting Act* that may be required.
10. The Act should make any other transitional provisions required.
11. The Act should make any other consequential amendments found necessary and advisable.

Canadian Security Intelligence Service Act (CSIS)

The Government is seeking feedback about the possibility of amending the CSIS Act as follows:

1. The Act should make changes to the Canadian Security Intelligence Service Act to create a new judicial authorization for obtaining identifying information (also referred to as “basic subscriber information” in other contexts) through a more simplified process in order to empower CSIS to assist in the investigation of online harms.
2. The Act should amend section 21 of the CSIS Act to establish a new regime for obtaining identifying information through a judicial authorization modelled after the General Production Order provision in the Criminal Code (section 487.014).
3. The Act should provide for a more expedient process to ensure timely investigations and greater flexibility than the section 21 regime currently provides, particularly by simplifying the procedures as compared to section 21.
4. The Act should provide for applications to be made to the Federal Court on a “reasonable grounds to believe” threshold that there is a threat to the security of Canada and obtaining identifying information would assist with the investigation of this threat.
5. The Act should prescribe the form of these applications, modelled after Form 5.004 in the Criminal Code.
6. The Act should prescribe the form of orders to be issued by the Federal Court.

Footnotes

- 1 The Government is considering two approaches to reporting/notification to law enforcement.

Date modified:

2022-04-29

