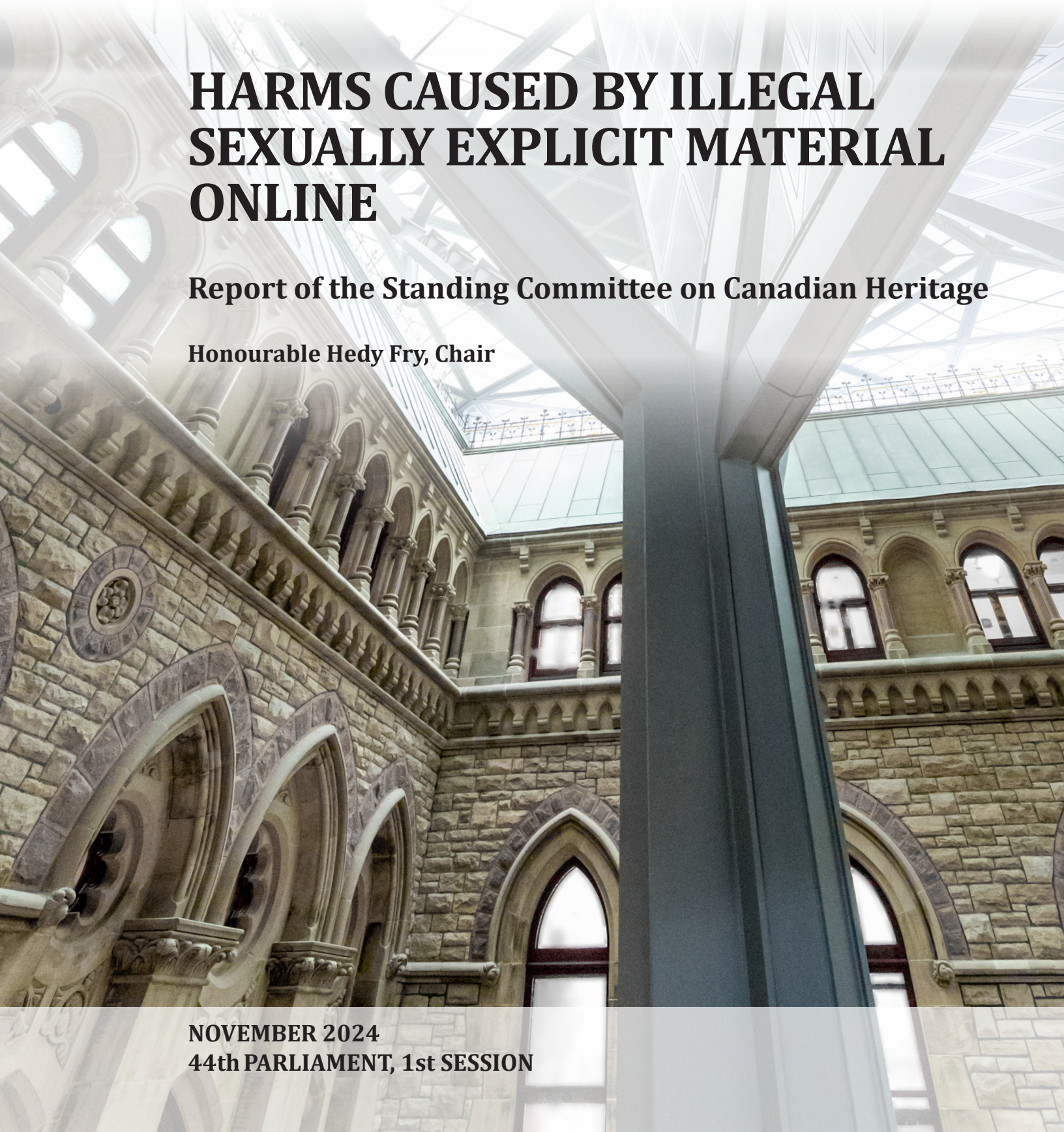
HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA



HARMS CAUSED BY ILLEGAL SEXUALLY EXPLICIT MATERIAL ONLINE

Report of the Standing Committee on Canadian Heritage

Honourable Hedy Fry, Chair

NOVEMBER 2024
44th PARLIAMENT, 1st SESSION

HARMS CAUSED BY ILLEGAL SEXUALLY EXPLICIT MATERIAL ONLINE

Report of the Standing Committee on Canadian Heritage

Hon. Hedy Fry
Chair

NOVEMBER 2024

44th PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committees presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

To assist the reader:
A list of abbreviations used in this report is available on page ix

STANDING COMMITTEE ON CANADIAN HERITAGE

CHAIR

Hon. Hedy Fry

VICE-CHAIRS

Kevin Waugh
Martin Champoux

MEMBERS

Niki Ashton
Michael Coteau
Anju Dhillon
Anna Gainey
Jacques Gourde
Jamil Jivani
Damien C. Kurek
Patricia Lattanzio
Taleeb Noormohamed

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Parm Bains
Rachel Bendayan
Kelly Block
Peter Fragiskatos
Iqwinder Gaheer
Philip Lawrence
Rachael Thomas
Salma Zahid

CLERKS OF THE COMMITTEE

Geneviève Desjardins
Danielle Widmer

LIBRARY OF PARLIAMENT

Research and Education

Marion Ménard, Analyst

Liane Tanguay, Analyst

THE STANDING COMMITTEE ON CANADIAN HERITAGE

has the honour to present its

FOURTEENTH REPORT

Pursuant to its mandate under Standing Order 108(2), the committee has studied the harms caused to children, women and men by the ease of access to, and online viewing of, illegal sexually explicit material and has agreed to report the following:

TABLE OF CONTENTS

LIST OF ACRONYMS

AI	Artificial Intelligence
C3P	Canadian Centre for Child Protection
CHPC	Standing Committee on Canadian Heritage
CSAM	Child Sexual Abuse Material
ETHI	House of Commons Standing Committee on Access to Information, Privacy and Ethics
GBV	Gender-based violence
NCDII	Non-consensual distribution of intimate images
SQ	Sûreté du Québec
TFGBV	Technology-facilitated gender-based violence
WAGE	Women and Gender Equality Canada

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

Recommendation 1

That the collection of, and access to, local and national intersectional data related to the non-consensual distribution of intimate images be supported, particularly by creating a database in collaboration with federal and provincial statistics services. 31

Recommendation 2

That an awareness campaign be launched with the objective of informing children and teens, in addition to equipping educators and parents, about

- **the consequences of viewing sexually explicit content depicting violent and abusive sexual behaviour, particularly for minors;**
- **the impact on victims of the non-consensual distribution of intimate images, including the creation and distribution of sexually explicit deepfakes; and**
- **tools to address sextortion. 31**

Recommendation 3

That measures be put in place to improve victims' access to resources, particularly with regard to reporting..... 32

Recommendation 4

That digital platforms implement processes for detecting and reporting illegal, sexually explicit content, such as child sexual abuse material and the non-consensual distribution of intimate images (including deepfakes), and that such content be removed immediately once it has been identified, under threat of penalty..... 32

HARMS CAUSED BY ILLEGAL, SEXUALLY EXPLICIT MATERIAL ONLINE

INTRODUCTION

Motion Passed by the House of Commons Standing Committee on Canadian Heritage

On 14 February 2022, the House of Commons Standing Committee on Canadian Heritage (CHPC) adopted the following motion:

> That, pursuant to Standing Order 108(2), the committee undertake a study on the harms caused to children, women, and men by the ease of access to, and online viewing of, illegal sexually explicit material, and the extent to which online access to illegal sexually explicit material contributes to the prevalence of violence against women and girls and sex trafficking in Canada; that the committee hear from organizations, victims, and law enforcement experts; that the committee hold a minimum of two meetings to that end; that the committee consider legal frameworks to prevent the harm caused by online access to illegal sexually explicit material; and that the committee report its findings and recommendations to the House.[1]

The Committee held meetings on 11 and 13 June 2024, heard from 12 witnesses and received two briefs. Given the short duration of the study, the Committee did not hear directly from survivors of online gender-based violence.

CONTEXT OF THE STUDY

Online Harms

Social media platforms have facilitated connectivity and communication on a global scale. At the same time, they have enabled the spread of a wide range of harmful and illegal content, including child sexual abuse material (CSAM) and the non-consensual distribution of intimate images (NCDII). More recently, the rise of generative artificial intelligence (AI) has enabled the creation and distribution of sexually explicit

1 House of Commons Standing Committee on Canadian Heritage, *Minutes of Proceedings*, 14 February 2022.

deepfakes—images, audio, and video digitally altered or fully generated by AI—that include CSAM and non-consensual intimate images.

The circulation of and ease of access to illegal, sexually explicit material can cause direct and grievous harm to victims. In 2012, Amanda Todd, a teenager from Port Coquitlam, British Columbia, took her own life after enduring relentless cyberbullying and harassment arising from an incident in which she inadvertently exposed herself to an online predator.[2] Just a year later, Rehtaeh Parsons, a 17-year-old from Nova Scotia, died by suicide after enduring cyberbullying and harassment following a sexual assault.[3] While these are extreme examples, the circulation of CSAM and non-consensual intimate images, including AI-generated deepfakes, is a growing problem in Canada and worldwide.

Online child sexual exploitation and abuse "encompasses a broad range of behaviours, including those related to child sexual abuse material, sexting materials (often distributed without consent), sextortion, grooming and luring, live child sexual abuse streaming and made-to-order content."[4] It is known to be highly underreported, with "only a fraction of incidents brought to the attention of police and the courts,"[5] but has shown a marked upward trend "since national data first became available in 2014."[6] Statistics Canada reports that, between 2014 and 2022, there were "15,630 incidents of police-reported online sexual offences against children and 45,816 incidents of online child pornography" and that "the rate of child pornography increased 290%" in the same period.[7]

NCDII "involves the sharing of intimate images, often of a former partner, with third parties … without the consent of the person depicted in the image."[8] It constitutes a form of technology-facilitated gender-based violence (TFGBV)[9] that Justice Canada explains "can occur in various situations involving adults and youth, including

2 Amanda Todd Legacy Society.

3 Rehtaeh Parsons Society.

4 Statistics Canada, *Online child sexual exploitation and abuse: Criminal justice pathways of police-reported incidents in Canada, 2014 to 2020*, 9 March 2023.

5 Public Safety Canada, *About online child sexual exploitation*, 08 August 2023.

6 Ibid.

7 Laura Savage, *Online child sexual exploitation: A statistical profile of police-reported incidents in Canada, 2014 to 2022*, Statistics Canada, 12 March 2024.

8 Department of Justice Canada, *CCSO Cybercrime Working Group Report to the Federal/Provincial/Territorial Ministers Responsible for Justice and Public Safety, Cyberbullying and the Non-consensual Distribution of Intimate Images*, June 2013, p. 3.

9 United Nations Regional Information Centre for Western Europe, *How Technology-Facilitated Gender-Based Violence Impacts Women and Girls*, 29 November 2023.

relationship breakdown and cyberbullying."[10] The prevalence of this activity is difficult to determine, but in 2023, Statistics Canada documented 1,168 reports to police of NCDII.[11]

Deepfake technology, which uses generative AI to create images and videos, is increasingly used to create sexually explicit material using the likenesses of real individuals, typically without consent. Such images can then be shared on easily accessed social media platforms and pornography sites, among others.[12] The Canadian Security Intelligence Service notes that "the most frequent application of deepfakes is in pornography," and that in 2022, "[over] 90 per cent of deepfakes available online are non-consensual pornographic clips of women."[13] Moreover, the technology itself has become widely accessible, to the point that school-aged children are easily able to create deepfake pornographic images of their classmates.[14]

Legal Context

The *Criminal Code*

While it is legal to produce and distribute pornography in Canada, the *Criminal Code* places some restrictions on its content and distribution. CSAM and NCDII are two examples of sexually explicit material that is illegal under the *Criminal Code*.

Specifically, section 162(1) of the *Criminal Code* makes it an offence to record (by photography, film or video) a person who is nude, who is exposing their genital organs, anal region or breasts, or who is engaged in sexual activity, where that person had a reasonable expectation of privacy at the time of the recording.[15] Similarly, it is an

10 Department of Justice Canada, *CCSO Cybercrime Working Group Report to the Federal/Provincial/Territorial Ministers Responsible for Justice and Public Safety, Cyberbullying and the Non-consensual Distribution of Intimate Images*, June 2013, p. 14.

11 Statistics Canada, *Police-reported cybercrime, by cyber-related violation, Canada (selected police services)*, Database, accessed 12 July 2024.

12 Eliza Strickland, "Deepfake Porn Is Leading to a New Protection Industry", *IEEE Spectrum*, 16 July 2024.

13 Canadian Security Intelligence Service, *Deepfakes: A Real Threat to a Canadian Future*, 16 November 2023.

14 See, for instance, Natasha Singer, "Teen Girls Confront an Epidemic of Deepfake Nudes in Schools", *The New York Times*, 8 April 2024.

15 *Criminal Code*, R.S.C. 1985, c. C-46, s. 162(1).

offence for anyone to distribute such content or to possess such content for distribution if that person knows the content was recorded under circumstances listed in 162(1).[16]

The Code also makes it an offence to distribute[17] an intimate image[18] of a person if the distributor knows that person did not consent to the image's distribution or is reckless as to whether consent was obtained.[19] This type of distribution was made a federal offence in 2015.

Section 163.1 of the Code specifically makes it an offence to make, distribute, possess or access child pornography.[20] It defines child pornography as follows:

> (a) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,
>
> (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or
>
> (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years;
>
> (b) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act;

16 A person commits an offence related to distribution under this section if that person "prints, copies, publishes, distributes, circulates, sells, advertises or makes available the recording, or has the recording in his or her possession for the purpose of printing, copying, publishing, distributing, circulating, selling or advertising it or making it available." Ibid., s. 162(4).

17 A person commits an offence related to distribution under this section if that person "publishes, distributes, transmits, sells, makes available or advertises" an intimate image. Ibid., s. 162.1.

18 In this section, an intimate image means a photographic, film or video recording of a person in which that person is "nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity" and who had a reasonable expectation of privacy at the time of recording and when the offence was committed. Ibid., s. 161.1(2).

19 Ibid., s. 161.1.

20 For the purposes of this section, a person commits an offence related to distribution if that person "transmits, makes available, distributes, sells, advertises, imports, exports or possesses for the purpose of transmission, making available, distribution, sale, advertising or exportation" child pornography. Ibid., s. 163.1.

(c) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act; or

(d) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act.[21]

It is important to note that deepfakes, or images generated by artificial intelligence, may not be currently captured by the *Criminal Code* provisions on non-consensual distribution of intimate images, except where the person depicted is or appears to be under the age of 18.[22]

An Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service

In 2011, Parliament adopted *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*, which requires Internet service providers to report if their service is being used to commit a child pornography offence. If advised of such an offence, service providers must report the offending Internet Protocol address or Uniform Resource Locator to the Canadian Centre for Child Protection (C3P). In addition, 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*.[23]

21 Ibid., s. 163.1(1).

22 See Mahdi Benmoussa et al., *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,* Preliminary (unedited) version, Library of Parliament, 20 March 2024, p. 10.

23 *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*, S.C. 2011, c. 4, ss. 2–3. For the purpose of section 2, section 9 of the Act provides the following: "a person who has reported information in compliance with an obligation to report child pornography under the laws of a province or a foreign jurisdiction is deemed to have complied with section 2 of this Act in relation to that information."

Government Initiatives to Tackle Illegal, Sexually Explicit Material Online

The Government of Canada has implemented a number of measures, including but not limited to the following, to combat CSAM and NCDII in collaboration with law enforcement, non-profit organizations and international partners.

The National Strategy for the Protection of Children from Sexual Exploitation on the Internet, launched in 2004 and renewed and expanded in 2009 and 2019, rests on four pillars: prevention and awareness; pursuit, disruption and prosecution; protection of victims; and partnerships, research and strategic support.[24] The most recent consultation with stakeholders to improve the Strategy took place in 2018,[25] and Budget 2019 committed $22.24 million over three years to its expansion.[26] Budget 2022 committed an additional $41.6 million over five years, and $8.9 million ongoing, to support prevention and awareness activities; enhance Canada's ability to pursue and prosecute offenders; and expand and share knowledge and enhance collaboration with partners and stakeholders.[27]

Among the non-profit partners involved in the National Strategy is the Canadian Centre for Child Protection (C3P), a charity organization committed to reducing child victimization. C3P is responsible for Cybertip.ca, a national tipline for reporting the online sexual exploitation of children, and Project Arachnid, a tool that detects known images of CSAM and issues removal notices to electronic service providers.[28] C3P also delivers programs, services and resources for families, educators, survivors, child-serving organizations, law enforcement, and others.[29]

In June 2017, the Government of Canada announced its Strategy to Prevent and Address Gender-Based Violence, led by Women and Gender Equality Canada (WAGE). The Strategy is based on three pillars: prevention, support for survivors and their families, and promoting responsive legal and justice systems. Through Budgets 2017 and 2018, Public Safety Canada received $11.4 million over five years, and $2.3 million ongoing, to support

24 Public Safety Canada, *Actions to Combat Online Child Sexual Exploitation*, 23 August 2023.

25 Government of Canada, *Countering Online Child Sexual Exploitation: Sharing Knowledge, Enhancing Safety – Closed consultation*, 9 May 2018.

26 Public Safety Canada, *Evaluation of the Expansion to the National Strategy for the Protection of Children from Sexual Exploitation on the Internet*, 24 May 2022.

27 Public Safety Canada, *Actions to Combat Online Child Sexual Exploitation*, 23 August 2023.

28 Canadian Centre for Child Protection, *Global tool disrupting international distribution of child sexual abuse imagery marks five years*, 17 January 2022.

29 Canadian Centre for Child Protection, *About the Canadian Centre for Child Protection*.

the implementation of the Strategy by enhancing efforts to address online child sexual exploitation through public awareness, policy coordination and research, and support for Project Arachnid.[30] In total, the Government of Canada has invested over $800 million, and $44 million per year ongoing, to seven federal departments and agencies in support of the Strategy,[31] which recognizes TFGBV among other types of abuses.[32]

The 10-year National Action Plan to End Gender-Based Violence aims to engage people in Canada in changing the norms, attitudes and behaviours that contribute to gender-based violence (GBV); address social and economic factors contributing to GBV; establish a framework for timely and reliable access to culturally appropriate and accessible protection and services; and improve health, social, economic and justice outcomes of people impacted by GBV.[33] Budget 2021 committed $601.3 million over five years towards advancing the new action plan, and Budget 2022 proposed $539.3 million over five years to support provinces and territories in their efforts to implement it.[34] Since 2022, bilateral agreements totaling $525 million over four years have been signed with all provinces and territories.[35]

The Department of Canadian Heritage led the development of a legislative framework to address online harms, beginning with public consultations in 2021, the appointment of an Expert Advisory Panel in 2022, a series of roundtable discussions in 2022 and the Canadian Citizens' Assemblies on Democratic Expression from 2020 to 2022.[36] The resulting legislation, Bill C-63, addresses both CSAM and NCDII, including deepfakes, and is discussed in more detail below.

30 Public Safety Canada, *The National Action Plan to End Gender-Based Violence*, 20 October 2020.

31 Women and Gender Equality Canada, *Facts, stats and WAGE's impact: Gender-based violence*, 9 July 2024.

32 Women and Gender Equality Canada, *Gender-based violence glossary*.

33 Women and Gender Equality Canada, *National Action Plan to End Gender-Based Violence*, 24 July 2023.

34 Women and Gender Equality Canada, *National Action Plan to End Gender-Based Violence Backgrounder*, 11 April 2024.

35 Women and Gender Equality Canada, *Facts, stats and WAGE's impact: Gender-based violence*, 9 July 2024.

36 See Mahdi Benmoussa et al., *Bill C-63: An Act to Enact the Online Harms Act, to Amend the Criminal Code, the 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*, Preliminary Legislative Summary, Library of Parliament, 20 March 2024.

International Efforts

The Government of Canada participates in several working groups and alliances dedicated to the fight against sexually explicit and illegal material.

Canada is a member of the G7 Child Sexual Exploitation and Abuse Working Group, which monitors progress on the G7 Action Plan to Combat Child Sexual Exploitation and Abuse. The plan "aims to encourage industry to play its part, strengthen domestic regimes, strengthen law enforcement cooperation, and protect children around the world."[37]

Canada worked with its Five Eyes[38] partners to develop and launch the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, which "provide a common and consistent framework to combat online sexual crimes against children" and "drives collective action between governments and industry partners."[39]

Canada is also a member of the WePROTECT Global Alliance to End Sexual Exploitation Online, an alliance of countries, industry partners and civil society working to assess the global threat environment, raise awareness, increase international cooperation and support member countries in adopting globally aligned legislative measures to prevent and combat online child sexual exploitation.[40] In 2022, Canada joined WePROTECT's Global Taskforce on Child Sexual Abuse Online.[41]

Chaired by the United Kingdom's National Crime Agency, the Virtual Global Taskforce is an international alliance comprising 15 law enforcement agencies, including the Royal Canadian Mounted Police.[42]

Led by Global Affairs Canada, the third National Action Plan on Women, Peace and Security, part of Canada's ongoing response to United Nations Security Council Resolution 1325 on Women, Peace and Security, includes a focus on "reducing sexual

37 Public Safety Canada, *International Efforts and Cooperation*, 23 August 2023.

38 The Five Eyes is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States.

39 Public Safety Canada, *International Efforts and Cooperation*, 23 August 2023.

40 Ibid.

41 Ibid.

42 Virtual Global Taskforce, *Tackling the global threat from child sexual abuse*.

and gender-based violence—including online—in conflict, post-conflict, and humanitarian contexts," both in Canada and abroad.[43]

In 2022, as chair of the Freedom Online Coalition, Canada "committed to working with its partners to address online gender-based violence through research and advocacy efforts."[44] The same year, Canada also joined the Global Partnership for Action on Gender-Based Online Harassment and Abuse, an alliance of countries, international organizations, civil society and the private sector aimed at addressing TFGBV.[45]

On 8 July 2024, Canada announced $5 million in funding over three years to the United Nations Population Fund's "Making All Spaces Safe" programme, which "aims to ensure that women and girls can enjoy the benefits of technology, free from violence and discrimination." Canada is the "first national contributor to this flagship programme."[46]

Previous Parliamentary Studies

In 2017, the House of Commons Standing Committee on Health examined "the public health effects of the ease of access and viewing of online violent and degrading sexually explicit material on children, women and men."[47] Its report recommended that the Public Health Agency of Canada update the *Canadian Guidelines for Sexual Health Education*; develop a Canadian sexual health promotion strategy; and compile a list of best practices and tools for parents on protecting children from exposure to online sexually explicit material. It also recommended that technology companies and software and browser developers create better content filters and tools to respect individual privacy while allowing parents to protect children online.[48]

In 2021, The House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) studied the protection of privacy and reputation on platforms such as

43 Global Affairs Canada, *Canada's National Action Plan on Women, Peace and Security*, 28 March 2024.

44 Government of Canada, *Advancing gender equality in the digital age: Programs work to address technology-facilitated violence*, 03 March 2023.

45 Tech for Democracy, *The Global Partnership for Action on Gender-Based Online Harassment and Abuse*.

46 United Nations Population Fund, *UNFPA and Canada launch a global programme to tackle technology-facilitated gender-based violence*, 08 July 2024.

47 House of Commons, Parliament of Canada, "Motion," *Journals*, 1st Session, 42nd Parliament, 8 December 2016.

48 House of Commons, Standing Committee on Health, *Report on the Public Health Effects of the Ease of Access and Viewing of Online Violent and Degrading Sexually Explicit Material on Children, Women, and Men*, 1st session, 42nd Parliament, June 2017, p. 13.

Pornhub. The study looked at Pornhub/Mindgeek's[49] response to non-consensual material and other illegal content posted on Pornhub, and its alleged failure to prohibit and remove illegal videos from its site. In its report, ETHI recommended that the Government develop regulations requiring "age verification of all individuals in uploaded pornographic content" and impose certain legal obligations on Internet service providers hosting pornographic content around the moderation and removal of illegal content.[50]

WHAT THE COMMITTEE HEARD

Scale of the Problem and Harms Caused

Witnesses told the Committee about the prevalence of CSAM and NCDII, as well as some of the reasons for its proliferation on the Internet.

Carol Todd is a Canadian educator and mental health and cyberbullying advocate, and the mother of Amanda Todd, the teenaged girl whose suicide in October 2012 drew international attention to the issues of cyberbullying and online harassment. Following Amanda's death, Ms. Todd founded the Amanda Todd Legacy Society, an organization dedicated to raising awareness about the effects of bullying, mental health issues, and the dangers of online exploitation.

Ms. Todd told the Committee that "the prevalence of sexually explicit material has increased due to the widespread use of the internet … and the volume grows exponentially day by day."[51] She explained:

> Over the past decade, we've observed rapid changes in the technology landscape. Technology primarily used to be used as a communication tool … and now we have seen the [evolution] of applications for fun. They were explained as safe, but now we know differently, because they have increased the chaos, concern and undesirable behaviours online for Canadians and for all … It's a global problem.[52]

Dianne Lalonde, a Research and Knowledge Mobilization Specialist with the Centre for Research and Education on Violence Against Women and Children, described both NCDII and deepfake sexual abuse—discussed in more detail below—as "forms of violence"

---

49 Mindgeek was acquired by Ethical Capital Partners in 2023 and is now known as Aylo.

50 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, 43rd Parliament, 2nd Session, June 2021.

51 CHPC, *Evidence*, 11 June 2024, 1720 (Carol Todd, Founder and Mother, Amanda Todd Legacy Society).

52 Ibid.

that are "increasing in the Canadian context" and noted that 92% of the 295 Canadian cases reported to police in 2016 involving the targeting of women. She added that while "we are lacking intersectional Canadian data," studies in the United States and Australia show that NCDII "disproportionately targets Black, Indigenous, 2SLGBTQIA+ individuals and people with disabilities" as well.[53]

Ms. Lalonde described the link between NCDII and "other forms of violence." She said perpetrators use NCDII to "control, monitor and harass their current or past intimate partner" or "as a tactic to advertise, recruit, and maintain control over individuals who experience sex trafficking."[54] She added that many people, "especially young boys," engage in NCDII "because of social pressures they face relating to traditional masculinity and expectations around sexual experience."[55]

Marc-Antoine Vachon, a Lieutenant with the Sûreté du Québec (SQ), told the Committee about the prevalence of CSAM in that province as well as his organization's efforts to combat it. He said, "[s]ince 2019 … we have noted a 295% increase in the number of reports received and processed, from 1,137 to 4,493" and that the SQ has arrested "more than 1,100 individuals and [identified] more than 230 real victims" in the same period.[56]

Monique St. Germain is General Counsel for C3P. She told the Committee that Cybertip.ca "averages over 2,500 reports a month" and has processed "over 400,000 reports" since its inception in 2002,[57] while Project Arachnid "issues roughly 10,000 requests for removal each day and some days over 20,000." Ms. St. Germain said that since its launch in 2017, Project Arachnid has issued "over 40 million notices … to over 1,000 service providers."[58]

Witnesses also discussed the impacts of NCDII and CSAM on victims and survivors as well as those accessing it.

Ms. Lalonde drew attention to the intersectional impacts of TFGBV, noting that "sexual double standards result in women … being more likely to be blamed, discredited and stigmatized due to sexual imagery online." She added that "2SLGBTQIA+ individuals have

53 CHPC, *Evidence*, 11 June 2024, 1725 (Dianne Lalonde, Research and Knowledge Mobilization Specialist, Centre for Research and Education on Violence Against Women and Children).

54 Ibid.

55 Ibid.

56 CHPC, *Evidence*, 11 June 2024, 1735 (Marc-Antoine Vachon, Lieutenant, Sûreté du Québec).

57 CHPC, *Evidence*, 13 June 2024, 1555 (Monique St. Germain, General Counsel, Canadian Centre for Child Protection Inc.).

58 CHPC, *Evidence*, 13 June 2024, 1555 (Monique St. Germain).

identified that [NCDII] has been a tool to 'out' their sexual orientation and their gender identity."[59]

Ms. Lalonde said the impacts of NCDII, including deepfakes, were "emotional, economic, physical and social" and that survivors "have likened these forms of violence to additional forms of sexual violence wherein their autonomy is denied."[60] She added that according to survivors, "one thing that's distinct about online harms is the way in which the harm becomes crowdsourced"[61] as users share and re-share the violent experience. Ms. St. Germain agreed, noting that "CSAM of adolescents is ending up on pornography sites, where it is difficult to remove"[62] and that its "continued availability" is "ruining lives. Survivors tell us time and again that the endless trading in their CSAM is a barrier to moving forward. They are living in constant fear of recognition and harassment."[63]

Similarly, in a brief submitted to the Committee, Defend Dignity, a national organization working to end sexual exploitation in Canada, described the trauma for survivors of "losing control over non-consensual intimate images of themselves":

> The platforms hosting the abuse are profiting from their pain, while users of the service view, comment, and sometimes further share the abusive content for their own pleasure. It's an impossible fight to get the content permanently removed from the Internet, and they never know when or where it will resurface. There is also the dread of not knowing who will view the abusive content—will they be recognized by a stranger? Will their children see it? … This abuse can severely harm overall well-being, including long-term impacts on mental, social, physical, and relational health.[64]

Some witnesses pointed to broader public health impacts of the circulation of material like CSAM. Ms. St. Germain said that "more sexual violence is occurring among children"[65] as a result of exposure to it, which she said can "normalize harmful sexual acts, lead to distorted beliefs about the sexual availability of children and increase aggressive behaviour." She cited a review of Canadian case law showing that "61% of offenders who produced CSAM also collected it."[66] Defend Dignity also linked the

59 CHPC, *Evidence*, 11 June 2024, 1725 (Dianne Lalonde).

60 Ibid.

61 Ibid.

62 CHPC, *Evidence*, 13 June 2024, 1555 (Monique St. Germain).

63 Ibid.

64 Defend Dignity, *Submission to the Standing Committee on Canadian Heritage*, 19 April 2024, pp. 7–8.

65 CHPC, *Evidence*, 13 June 2024, 1555 (Monique St. Germain).

66 Ibid.

availability of CSAM to an "increased risk of seeking to abuse children," with luring incidents increasing 815% between 2018 and 2022, and offenders reporting exposure to CSAM as a factor in their own offenses.[67]

AI-generated Deepfakes

Several witnesses, including Chloe Rourke and Shona Moreau, recent graduates from the Faculty of Law at McGill University, focused their observations on the problem of deepfake pornography.

Ms. Moreau told the Committee that AI-generated deepfakes have "become increasingly sophisticated and harder to distinguish from real-life footage," that "lifelike deepfakes can now be generated using just a single photo of a person" and that the technology's "most common use is for non-consensual porn," which "overwhelmingly [features] female subjects."[68] Ms. Moreau explained:

> [T]his gendered and sexualized use of the technology is not new. The term deepfake actually originated in 2017 stemming from the practice of using online tools to switch female celebrities' faces onto pornographic videos. In other words non-consensual porn has kind of been central to the technology since its very beginning.[69]

Ms. Moreau said that such content is "a significant threat [to] people and [to] human dignity" that "can be produced quickly and with minimal effort and skills" and that "[inflicts] real emotional, societal and reputational harm on victims."[70] She added that "even children … have found themselves the subject of pornographic deepfakes made and shared by their own classmates."[71]

Ms. Rourke described deepfakes as "a whole new wave of content that [the platforms] will have to account for in their current [moderation] systems."[72] She told the Committee that she is shocked by "just how accessible this technology is"[73] and said that "there are no

---

67 Defend Dignity, *Submission to the Standing Committee on Canadian Heritage*, 19 April 2024, p. 5.

68 CHPC, *Evidence*, 13 June 2024, 1600 (Shona Moreau, BCL/JD, Faculty of Law, McGill University, As an Individual).

69 Ibid.

70 Ibid.

71 Ibid.

72 CHPC, *Evidence*, 13 June 2024, 1700 (Chloe Rourke, BCL/JD, Faculty of Law, McGill University, As an Individual).

73 CHPC, *Evidence*, 13 June 2024, 1705 (Chloe Rourke).

control mechanisms on there to ensure that any of the images being used are being used in a consensual manner."[74]

Ms. St. Germain added that deepfakes circumvent "the systems that detect this type of material," such as Project Arachnid: "The fake material doesn't have those hash values [digital fingerprints] in the databases that are being relied on, so removal of them becomes an incredible challenge."[75]

Dr. Heidi Tworek, an Associate Professor at the University of British Columbia, agreed that deepfakes are a serious and growing problem, noting that while they are not new, "generative AI has significantly lowered the barrier for entry." She told the Committee that "the number of deepfake videos increased by 550% from 2019 to 2023" and added that "one-third of deepfake tools enable a user to create pornography, which comprises over 95% of all deepfake videos."[76]

Ms. Lalonde told the Committee that "many of these forms of applications and technology only work on women and girls' bodies" and that "a study of 95,000 deepfake videos in 2023 found that 98% were sexually explicit, and of those, 99% targeted women."[77] She added that sex workers are also harmed by deepfakes: "[they] have their likenesses stolen and used to inflict violence, and … then face stigma and criminalization in response."[78]

Ms. Rourke said that deepfakes "exacerbate" the pre-existing problem of NCDII "because anyone is able to create and distribute such content," and that they are "already being used to target, harass, and silence female journalists and politicians." She warned that "if unchecked, deepfakes threaten to rewrite the terms of participation in the public sphere for women."[79]

Regulating Illegal, Sexually Explicit Material

Witnesses spoke to the Committee about the prospects and challenges of regulating illegal, sexually explicit material online. They discussed measures such as age assurance, amending the *Criminal Code* to include reference to deepfakes, and imposing legal

74 Ibid.

75 CHPC, *Evidence*, 13 June 2024, 1625 (Monique St. Germain).

76 CHPC, *Evidence*, 13 June 2024, 1550 (Dr. Heidi Tworek, Associate Professor, University of British Columbia, As an Individual).

77 CHPC, *Evidence*, 11 June 2024, 1725 (Dianne Lalonde).

78 Ibid.

79 CHPC, *Evidence*, 13 June 2024, 1605 (Chloe Rourke).

responsibilities upon online platforms to prevent, address and remove such material, which is the focus of part 1 of Bill C-63, the government's proposed online harms legislation.

Witnesses broadly agreed that the current lack of regulation is unacceptable. Ms. St. Germain told the Committee that "for years, our laws in the off-line world protected [children], but we abandoned that with the Internet."[80] She added, "[t]he burden of managing Internet harms has fallen largely to parents. This is unrealistic and unfair."[81] Dr. Emily Laidlaw, Associate Professor and Canada Research Chair in Cybersecurity Law at the University of Calgary, agreed, saying that "safety has generally taken a back seat to other interests," that "[social] media has always been lightly regulated" and that "online safety has only been addressed if companies felt like it or they were pressured by the market." She said, "[there] are no minimum standards and no ways to hold companies accountable."[82]

Ms. Todd said, "Amanda died in 2012. We are now in 2024. We're almost 12 years." She blamed "roadblocks … put up by one political party versus another political party" for the ongoing lack of regulation or other solutions.[83] She said,

> I have sat on six standing committees since 2012, on technology-facilitated violence, on gender-based violence, on exploitation against children and young people, on other ones on intimate images, and now this one.
>
> I could copy and paste facts that I talk about: more funding, more legislation, more education, more awareness. Standing committees then come out with a report. We see those reports, but we never know what happens at the end: Do these things really happen? Is there more funding in law enforcement for training officers and for their knowledge? Are there changes in legislation? …
>
> We are harming Canadians, our children and our citizens when things don't get passed … We are a first world country, and our Canadians deserve to be protected.[84]

80 CHPC, *Evidence*, 13 June 2024, 1555 (Monique St. Germain).

81 Ibid.

82 CHPC, *Evidence*, 11 June 2024, 1710 (Dr. Emily Laidlaw, Associate Professor and Canada Research Chair in Cybersecurity Law, University of Calgary, As an Individual).

83 CHPC, *Evidence*, 11 June 2024, 1830 (Carol Todd).

84 Ibid.

Age Assurance and Verification

According to the Office of the Privacy Commissioner of Canada, age assurance is "a term that refers to a variety of processes by which the age (or age group) of a user is determined with varying levels of specificity and certainty."[85] One of these processes is age verification, which requires users to prove their age, either directly by means of government-issued identification, or indirectly via a third-party service.[86] Another is age estimation, which uses analysis of biometrics or behaviours in order to determine a user's age.[87] The most common methods currently available require users to share sensitive information such as official identification cards, banking details, or biometric data (e.g. facial scans), which in the case of pornography websites, is then linked to data on pornography consumption.[88] Critics have noted that apart from privacy and data security concerns, such laws are easily circumvented through the use of a virtual private network or VPN.[89]

A number of U.S. states already have various age verification laws in place,[90] but these have met legal challenges and are widely controversial.[91] Pornhub has blocked access to its site in states requiring users to provide ID to verify their ages, which it says is a threat to user privacy and security,[92] and civil society groups have also warned that such laws undermine First Amendment protections for freedom of speech.[93] The Texas law is currently before the U.S. Supreme Court.[94]

Two bills concerning age verification are currently before Parliament. One is *Bill S-210, An Act to restrict young persons' online access to sexually explicit material*, which would

85 Office of the Privacy Commissioner of Canada, *Privacy and age assurance – Exploratory consultation*, 10 June 2024.

86 Ibid.

87 Ibid.

88 Lauren Lefer, "Online age verification laws could do more harm than good", *Scientific American*, 16 April 2024.

89 Ibid.

90 John Hanna and Sean Murphy, "Kansas moves to join Texas and other states in requiring porn sites to verify people's ages", *The Associated Press*, 26 March 2024.

91 Lauren Lefer, "Online age verification laws could do more harm than good", *Scientific American*, 16 April 2024.

92 Pornhub, *Age Verification in the US*, 2 July 2024.

93 American Civil Liberties Union, *Free Speech Coalition, Inc. v. Paxton*, 3 July 2024.

94 Andrew Chung, "US Supreme Court to hear challenge to Texas age verification for online porn", Reuters, 2 July 2024.

make it an offence for organizations to make sexually explicit material available to young persons on the Internet and empowers Governor in Council to make regulations prescribing age-verification methods.[95] At the time of writing, Bill S-210 is at report stage in the House of Commons.

The other is Bill C-270, *An Act to amend the Criminal Code (pornographic material)*, which would make it an offence to make, distribute or advertise pornography for commercial purposes without having first ensured that each person whose image is depicted was 18 years of age and gave their express consent at the time the pornography was made. Under Bill C-270, an accused cannot claim to have believed a participant was 18 years of age or older unless they "attempted to verify the person's age by asking for and examining a piece of identification issued by a federal or provincial authority or a foreign government—or any other documentation prescribed by regulation—containing the person's photograph, date of birth and signature."[96] At the time of writing, Bill C-270 has been referred to the House of Commons Standing Committee on Justice and Human Rights.

Dr. Laidlaw said that Bill S-210 was both "flawed" and "unnecessary," describing age verification as an "evolving" technology whose use "must be scrutinized closely" in light of democratic commitments to "freedom of expression, privacy and cybersecurity."[97]

Likewise, Mr. Krishnamurthy pointed out that "the age verification laws that have been enacted in the United States" have been "ineffective," partly because of VPNs. He shared Dr. Laidlaw's concerns, noting that existing age verification methods "[require] you to divulge personal details, which means that your Internet activities are being tracked by somebody in some way," and that the use of biometrics "[suffers] from significant inaccuracies" all while "[collecting] a very sensitive form of information."[98] He said that while the technology "may be better" in future, "the Senate bill [S-210] is ill-considered at this time."[99]

Dr. Jocelyn Monsma Selby is a clinical therapist and a researcher specialising in forensic sexology and addiction as well as the Chair of Connecting to Protect, a global initiative to

95 *Bill S-210, An Act to restrict young persons' online access to sexually explicit material*, 44th Parliament, 1st session.

96 *Bill C-270, An Act to amend the Criminal Code (pornographic material)*, 44th Parliament, 1st session.

97 CHPC, *Evidence*, 11 June 2024, 1710 (Emily Laidlaw).

98 CHPC, *Evidence*, 11 June 2024, 1820 (Vivek Krishnamurthy, Associate Professor of Law, University of Colorado Law School, As an Individual).

99 Ibid.

address children's access to online pornography. She was in favour of age verification measures but stated a preference for "device-level controls operating at the point of online access through Google, Apple or Microsoft." She said this approach was "technologically possible and relatively quick to implement," and would have "far greater reach and effectiveness" than that proposed by Bill S-210.[100] She explained that "if you do a device-level control that has an age assurance technology, then you'll get the majority of platforms," whereas there are too many different sites to regulate individually: "you need to have a tool at the device level that hits all of these sites … People are finding explicit sexual content all over the place on the regular Internet, not on the dark web."[101] She agreed with Mr. Krishnamurthy that age-verification laws implemented in certain U.S. states, such as Texas, had "not been proven effective."[102]

According to a brief submitted by the organization Defend Dignity, "there are a wide range of age assurance methods available" that do not "identify the user." The organization recommends adopting Bill S-210 with criteria "to ensure the age assurance technology used is effective and privacy-preserving."[103] Defend Dignity also recommends the adoption of Bill C-270 "as soon as possible."[104]

Amending the *Criminal Code* to Include Deepfakes

Some witnesses told the Committee that the *Criminal Code* should be amended to account for deepfake pornography.

Chloe Rourke said that section 162.1 of the Code, which proscribes the non-consensual distribution of intimate imagery, "should be reviewed and extended to include altered images such as deepfakes" and that doing so "would send a clear message that it is wrong and must be denounced."[105]

Ms. Lalonde told the Committee that the United Kingdom had seen some success with criminalization of deepfakes, noting that "one of the biggest websites of deepfake sexual

100 CHPC, *Evidence*, 11 June 2024, 1730 (Dr. Jocelyn Monsma Selby, Clinical therapist, Researcher Specialising in Forensic Sexology and Addiction, and Chair, Connecting to Protect).

101 CHPC, *Evidence*, 11 June 2024, 1835 (Dr. Jocelyn Monsma Selby).

102 CHPC, *Evidence*, 11 June 2024, 1840 (Dr. Jocelyn Monsma Selby).

103 Defend Dignity, *Submission to the Standing Committee on Canadian Heritage*, 19 April 2024, p. 10.

104 Ibid., p. 9.

105 CHPC, *Evidence*, 13 June 2024, 1600 (Chloe Rourke).

abuse was taken down in the U.K." following criminalization.[106] She said that doing the same thing in Canada "would signal [deepfakes] as a form of violence, given how much it is doubted." By way of illustration, she referred to a study that "assessed 95,000 different deepfake videos and also asked people, 'Do you feel guilty watching these?', and overwhelmingly people said no."[107]

Keita Szemok-Uto, a lawyer who has studied deepfake pornography in relation to privacy law, pointed out certain challenges associated with the criminalization of deepfakes under section 162.1 of the Code, citing "the 'reasonable expectation of privacy' element" of the provision: "When you take somebody's social media photo, which is taken and posted publicly, it's questionable whether they had a reasonable expectation of privacy when it was taken."[108]

Mr. Szemok-Uto also said that "the standard of beyond a reasonable doubt … would play into limiting who is convicted of these crimes, as well as the scope and resources that would be required to actually provide and enforce criminal prohibitions of this kind of behaviour."[109] He said that in his studies of deepfake pornography, he "discovered that there is really no adequate system of law yet that protects victims from this kind of privacy invasion" and that it is "something that really is only now being addressed somewhat with [Bill C-63, the government's proposed online harms legislation]."[110]

Ms. Rourke agreed with Mr. Szemok-Uto, adding that, "unlike a real recording, deepfakes are not tied to a specific time, location or sexual partner. They can easily be produced and distributed anonymously. Therefore, in practice, it will often be difficult to identify perpetrators and hold them legally accountable, which will limit the deterrent effect of such provisions."[111]

Ms. Rourke added that even where a perpetrator could be identified and charged, "criminal or civil penalties cannot restore a victim's privacy, dignity or sense of safety, particularly when the content continues to circulate in the public domain."[112] She said that "to address these ongoing harms, we must consider the role and responsibility of

106 CHPC, *Evidence*, 13 June 2024, 1810 (Dianne Lalonde).

107 Ibid.

108 CHPC, *Evidence*, 13 June 2024, 1610 (Keita Szemok-Uto, Lawyer, As an Individual).

109 CHPC, *Evidence*, 13 June 2024, 1640 (Keita Szemok-Uto).

110 CHPC, *Evidence*, 13 June 2024, 1610 (Keita Szemok-Uto).

111 CHPC, *Evidence*, 13 June 2024, 1600 (Chloe Rourke).

112 Ibid.

digital platforms," since they "are the ones that have control over the algorithms … and they are the ones that can take the content down—at least make it less visible, if not remove it entirely."[113] Indeed, for Ms. Rourke, the Code provisions "that currently exist and apply to actual real recordings of intimate images … are an incomplete remedy" even setting aside the issue of deepfakes. She said, "our bigger priority is about what accessible remedies there are that can be implemented in the vast majority of cases … That's why I think involving the platforms is really important."[114]

Bill C-63 (the Online Harms Act)

Platform accountability is the focus of Part 1 of Bill C-63, the government's proposed online harms legislation, tabled in Parliament on 26 February 2024 and currently at Second Reading in the House of Commons. The Act was the product of, among other things, consultation and policy work led by the Department of Canadian Heritage between 2019 and 2023.[115] The Department of Justice assumed the lead on the file in late 2023.[116]

According to the government, Bill C-63 would "hold online platforms … accountable for the design choices made that lead to the dissemination and amplification of harmful content on their platforms and ensure that platforms are employing mitigation strategies that reduce a user's exposure to harmful content."[117]

Among other things, it creates requirements for removing "content (1) that sexually victimizes a child or revictimizes a survivor, and (2) is intimate content posted without consent," including deepfakes; for providing accessible tools for flagging content and blocking users; and for implementing measures to protect children and "reduce exposure" to harmful content for everyone. The bill also amends the *Criminal Code* and the *Canadian Human Rights Act* to address online hate and enhances the *Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*. Finally, it establishes a Digital Safety Commission to oversee and enforce the Act as well as a

113 CHPC, *Evidence*, 13 June 2024, 1615 (Chloe Rourke).

114 CHPC, *Evidence*, 13 June 2024, 1620 (Chloe Rourke).

115 See Mahdi Benmoussa et al., *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,* Preliminary (unedited) version, Library of Parliament, 20 March 2024, pp. 3–5.

116 See Ian Campbell, "Canadian government must legislate to promote online safety, says Facebook whistleblower", *The Hill Times*, 27 November 2023.

117 Department of Canadian Heritage, *Government of Canada introduces legislation to combat harmful content online, including the sexual exploitation of children*, News release, 26 February 2024.

Digital Safety Ombudsperson to "act as a resource and advocate for the public interest with respect to online safety."[118]

Witnesses appeared to be broadly supportive of the bill. Dr. Laidlaw, who served on the government-appointed Expert Advisory Panel that assisted in developing the legislation,[119] said the Act "aligns with global approaches" and "is the number one avenue to address illegal sexually explicit content and sexual exploitation."[120]

Mr. Krishnamurthy, who also served on the Expert Advisory Panel, told the Committee that the bill "offers a good approach to dealing with one part of the distribution challenge" by creating "'a duty to act responsibly,' which gets to the systemic problem of how platforms curate and moderate content," thus "[reducing] the risk that this kind of content does get distributed on their platforms."[121] He added that the duty to remove illegal content "to the extent that platforms' own moderation efforts or user reports flag that content as being unlawful" is a "very sensible approach" that is "compliant with the [Charter of Rights and Freedoms] in its broad strokes."[122]

Dr. Signa Daum Shanks also served on the Expert Advisory Panel. She told the Committee that the "duty of acting responsibly" imposed by the *Online Harms Act* "[makes the legislation] stronger and the need for lawsuits less likely."[123] She said such legislation is "capable of paralleling the benefits of private law" while "avoiding some of [its] limitations"[124] and that it "hopefully stops most intentional harm before it happens."[125]

Dr. Tworek, who also served on the Expert Advisory Panel, noted that Bill C-63 addresses "the question of deepfakes," and that the "duty to act responsibly" is "certainly capacious enough to be able to deal with these kinds of updates." She added that "if we're thinking about generative AI companies, they too will have a duty to act responsibly."[126]

---

118 Ibid.

119 Department of Canadian Heritage, *Government of Canada announces expert advisory group on online safety*, News release, 30 March 2022.

120 CHPC, *Evidence*, 11 June 2024, 1710 (Emily Laidlaw).

121 CHPC, *Evidence*, 11 June 2024, 1700 (Vivek Krishnamurthy).

122 Ibid.

123 CHPC, *Evidence*, 13 June 2024, 1605 (Dr. Signa Daum Shanks, Associate Professor, University of Ottawa, Faculty of Law, As an Individual).

124 Ibid.

125 Ibid.

126 CHPC, *Evidence*, 13 June 2024, 1625 (Dr. Heidi Tworek).

Mr. Szemok-Uto said that Bill C-63 "goes in the right direction" by "[putting] a duty on operators to police and regulate what kind of material is online" and that "the inclusion of the word 'deepfake' in the legislation" is "a good step forward in trying to … get up to date with the definitions that are being used."[127] He noted, however, that "no definition [of deepfakes] is provided" in the bill and referred to legislation recently passed in Pennsylvania[128] as offering a model for such a definition.[129]

Marc-Antoine Vachon of the Sûreté du Québec told the Committee that Bill C-63 was "a very good start" and that "people who host computer data should be required to know what they are hosting."[130] He agreed with the bill's 24-hour takedown provisions, noting that "in the case of removal requests relating to complaints made through the Canadian Centre for Child Protection website, replies are not always received." He added that "it is also important to impose fines to penalize service providers that do not comply with the time limit"[131] for content removal.

Witnesses also supported the idea of establishing a new regulatory body, namely the Digital Safety Commissioner, as well as a Digital Safety Ombudsman, under Bill C-63. Dr. Laidlaw pointed out that "[c]ourts are never going to be fast to resolve the kinds of disputes here and they're costly," whereas "the power of the commissioner to order the removal of the worst forms of content is crucial to provide access to justice."[132] She added that the courts are "ill-suited to oversee safety by design as well, which is necessarily an iterative process between the commission and the companies."[133] Dr. Daum Shanks said she sees the idea of a new regulator as "similar to the idea of duty of care: having a place where individuals have a way to talk about what their harm is in a way that perhaps has never been heard before."[134]

In a brief submitted to the Committee, the organization Defending Dignity observed that while the provisions in the bill regarding "more complex issues such as hate" would "require additional consideration," those "addressing CSAM and [NCDII] could be dealt

127 CHPC, *Evidence*, 13 June 2024, 1645 (Keita Szemok-Uto).

128 The General Assembly of Pennsylvania, *Senate Bill No. 1213*, 4 June 2024.

129 CHPC, *Evidence*, 13 June 2024, 1645 (Keita Szemok-Uto).

130 CHPC, *Evidence*, 11 June 2024, 1825 (Marc-Antoine Vachon).

131 CHPC, *Evidence*, 11 June 2024, 1845 (Marc-Antoine Vachon).

132 CHPC, *Evidence*, 11 June 2024, 1710 (Emily Laidlaw).

133 Ibid.

134 CHPC, *Evidence*, 13 June 2024, 1720 (Dr. Signa Daum Shanks).

with expeditiously" and said that the two harms should be "[separated] … into their own legislation that could be addressed urgently."[135]

Witnesses were also aware of some of the challenges and limitations of any online harms legislation, including Bill C-63.

Mr. Krishnamurthy noted that it was "hard to determine before the fact how effective" such legislation is, "because of issues with determining both the numerator [the rate at which platforms remove illegal content] and the denominator [the overall prevalence of such content]."[136] He also explained the difficulties of regulating all platforms on which illegal content might appear, using the analogy of "elephants" and "mice":

> There are some elephants in the room, which are large, powerful and visible actors. These are your Metas and your TikToks, or even a company like Pornhub, which has a very large and significant presence. These are players that can't hide from the law, but what is difficult in this space is that there are many mice. Mice are small, they're furtive and they reproduce very quickly. They move around in darkness. The law is going to be very difficult to implement with regard to those kinds of actors, the ones we find on the darker corners of the internet.[137]

Dr. Tworek spoke to Mr. Krishnamurthy's point, suggesting that smaller platforms that are "being abused" could receive support from the bill's digital safety commissioner to remove offending content, while the "more nefarious smaller-firm actors," or "tools that are only really being put up in order to create deepfakes," might be addressed by an expanded bill requiring such sites to be shut down.[138]

Witnesses also noted that Bill C-63 does not capture encrypted messaging services such as WhatsApp and Messenger, which according to Mr. Krishnamurthy are "a primary vector by which this kind of content moves." While Mr. Krishnamurthy thought leaving messaging services out of scope was "a good call," he said their use for sharing illegal content is a problem that "requires further study."[139] Ms. Laidlaw agreed, adding that "one way to bring private messaging into the bill and avoid undermining [privacy and cybersecurity] protections" would be "to impose safety obligations on the things that

135 Defend Dignity, *Submission to the Standing Committee on Canadian Heritage*, 19 April 2024, p. 9.

136 CHPC, *Evidence*, 11 June 2024, 1700 (Vivek Krishnamurthy).

137 Ibid.

138 CHPC, *Evidence*, 13 June 2024, 1625 (Dr. Heidi Tworek).

139 CHPC, *Evidence*, 11 June 2024, 1700 (Vivek Krishnamurthy).

surround private messaging … such as complaints mechanisms, suspicious friend requests, and so on."[140]

Dr. Tworek noted that "We've talked as if all the individuals creating harm would be located in Canada, but the truth is that many of them may be located outside of Canada. I think we need to think about what international cooperation looks like … Taking things down in Canada only will potentially lead to revictimization, as something might be stored in a server in another country and then continually reuploaded."[141]

Ms. Moreau pointed out that "more work is going to be coming down the pipeline [to address online harms]" and that legislators should "be able to do that work quickly to keep up." She explained that "when we're making legislation now, we have to be looking five to 10 years or even sometimes 25 years out. We can't just be working on current issues. We almost have to be working on future issues."[142]

Dr. Daum Shanks said that "there's not just going to be this bill that takes care of this issue … There will be other pieces of legislation that can be tweaked to match the purposes of what we're talking about right now."[143] She explained to the Committee that "the idea of slowing down is unthinkable" even if the bill is "not … in the perfect form" and said, "one of the hopes I have is that everyone realizes that this is just the beginning, and this bill is not the end of it."[144]

Support for Survivors

Some witnesses identified support for survivors of online sexual exploitation and NCDII, including deepfakes, as a critical part of any approach to dealing with such harms, including Bill C-63. Dianne Lalonde said, "much of the focus on legislation has been on regulation and removal of content" but "we … need to recognize … the survivors and who survivors are going to. They are going to gender-based violence services in order to cope and heal from these harms. An added dimension when we're talking about addressing online harms is making sure we're supporting the gender-based violence agencies who are doing the work to support survivors":

140 CHPC, *Evidence*, 11 June 2024, 1710 (Emily Laidlaw).

141 CHPC, *Evidence*, 13 June 2024, 1625 (Dr. Heidi Tworek).

142 CHPC, *Evidence*, 13 June 2024, 1715 (Shona Moreau).

143 CHPC, *Evidence*, 13 June 2024, 1715 (Dr. Signa Daum Shanks).

144 Ibid.

> Unless [the safety commission and the ombudsperson] have a mandate to support survivors—which would be new, and they'd have to build relationships with that community—what we need is to have support for the gender-based violence sector to continue uplifting survivors and promoting healing opportunities … [The] legislation talks so much about regulation, which would require survivors to be the ones who report the violence that they're experiencing. How do we even get to know about the violence unless we're supporting survivors to report it and to heal from it?"[145]

Ms. Shona Moreau told the Committee that it would be "beneficial" for victims to have mental health support, "wherever it comes from," and that it should be funded and made "more accessible to the public."[146]

Dr. Daum Shanks felt this could be addressed through the creation of a digital safety ombudsperson as proposed in Bill C-63. She said, "[t]he thing I'm most concerned with is that people feel like they can be themselves—people who have less access to legal counsel and people who are working with whatever commissioner ombuds office is functioning … That's probably my biggest bailiwick—to think … someone can call an official space, whether it's a toll-free number or filing a written report or something, that they feel like the support system is right there." She said that in criminal law, "that first stage of getting things going is incredibly intimidating to people not trained in law" and that "I want to find as many ways to avoid that as possible."[147]

Education and Awareness

Witnesses emphasized the importance of educating children, youth and adults on the dangers of online sexual exploitation, the impacts of non-consensual intimate image distribution, including creating and sharing deepfake pornography, and the wider social context of gender inequity and gender-based violence.

Marc-Antoine Vachon, a lieutenant with the Sûreté du Québec, emphasized the importance of education as a preventive strategy and credited his organization's outreach efforts with "increasing the number of reports made and processed by police officers"[148]:

> The Sûreté du Québec now makes videos that are posted online, on YouTube. We are on social networks. That is how we can reach teens. We maintain our presence on social

145 CHPC, *Evidence*, 11 June 2024, 1810 (Dianne Lalonde).

146 CHPC, *Evidence*, 13 June 2024, 1700 (Shona Moreau).

147 CHPC, *Evidence*, 13 June 2024, 1705 (Dr. Signa Daum Shanks).

148 CHPC, *Evidence*, 11 June 2024, 1840 (Marc-Antoine Vachon).

> media, adapting our prevention message according to age, make it funny and a bit lighter rather than simply saying not to do this or that. …
>
> [The] prevention continuum starts in grade one. We have to hammer home the prevention message, along with the potential lifelong consequences, because there are lifelong consequences. I think that is how we can reach young people today.[149]

Mr. Vachon added that educating people about "the law of supply and demand" was also a necessary step: "We often see … a trivialization of [CSAM images] by both the families and the suspects, in the sense that they will claim that they did not touch a child. … We have to work to change the mentality of the accused and the families. We often see families protecting the arrested person by claiming that they have not abused anyone. Consuming that image, however, is feeding the person who produces it."[150]

Carol Todd said it was essential to "[empower] students, teachers and families with the knowledge and skills to navigate the digital world safely." She noted that her daughter Amanda "created a video five weeks before her passing" that "has been viewed 50 million times worldwide" and "is now used as a learning tool for others to start the discussion and for students to learn … why it's so important that we continue to talk about online safety, exploitation and sextortion."[151] She said that her organization talks "to kids as young as four or five years old … and there's a time to talk about online safety, social and emotional learning, respect and how to interact with others. That is the core, and you build upon it year after year." She also noted that "some teachers aren't getting it. They aren't seeing the importance."[152]

Ms. Todd also emphasized the importance of reaching out to parents: "Parents out there are unknowing. They're handing devices to their kids as early as seven and eight years old, and then they're complaining that this or that happened or whatever. … My role as an educator and a parent is to get that information out to those who need it. Yes, the tech industry and governments all need to be part of that, but this is multi-level."[153]

Ms. St. Germain agreed that "[education] is always a critical component of any policy or initiative that we have," adding that it is important to ensure "that young people are educated about sexual consent and understand the ramifications of sharing intimate images or creating [deepfake] material." She said, "we should have education for parents

149 CHPC, *Evidence*, 11 June 2024, 1845 (Marc-Antoine Vachon).

150 CHPC, *Evidence*, 11 June 2024, 1825 (Marc-Antoine Vachon).

151 CHPC, *Evidence*, 11 June 2024, 1715 (Carol Todd).

152 CHPC, *Evidence*, 11 June 2024, 1850 (Carol Todd).

153 Ibid.

and kids, taught through schools and available in a lot of different mediums and the places that kids go."[154]

Ms. Moreau agreed on the importance of education, noting that "we have to look at how we teach children to use new technologies"[155] and that children need to be made aware of the dangers: "They need to know that when they talk to a classmate, for example, that once that person is at home, they can use their image and make deepfake pornography. I think it's sometimes a little hard to picture yourself on a screen after a deepfake."[156] She agreed that "schools have a role to play, since it's the physical location where there's a lot of social interaction," but added that "platforms also have a role to play in educating the people who use them to distribute or even create material."[157]

Additionally, some witnesses pointed out that CSAM and NCDII do not take place in a vacuum and said that educational efforts should account for the broader context of gender inequity and gender-based violence in order to help people understand both the phenomenon and its impacts.

Ms. Lalonde said that while digital awareness was important, "[i]t's also getting to the root causes … we also need to talk about misogyny. We need to talk about gender equity. These are all very interconnected issues, especially when we're talking about these forms of violence that so disproportionately target women and girls."[158] She also noted that young boys are often the perpetrators of online sexual exploitation "because of social pressures they face relating to traditional masculinity and expectations around sexual experience."[159]

Ms. Rourke also emphasized the importance of understanding deepfake technology "within a societal context of gender-based violence and oppression."[160] She explained, "[t]he first thing you have to ask is why a nude image of a woman is so damaging":

> Why is there a reputational harm from that being shared? What kind of cultural response do we have to women's sexuality so that it's specifically women who are targeted with this—so that 99% of pornographic deepfakes are of women? There's a

154 CHPC, *Evidence*, 13 June 2024, 1635 (Monique St. Germain).

155 CHPC, *Evidence*, 13 June 2024, 1700 (Shona Moreau).

156 CHPC, *Evidence*, 13 June 2024, 1725 (Shona Moreau).

157 CHPC, *Evidence*, 13 June 2024, 1700 (Shona Moreau).

158 CHPC, *Evidence*, 11 June 2024, 1815 (Dianne Lalonde).

159 CHPC, *Evidence*, 11 June 2024, 1725 (Dianne Lalonde).

160 CHPC, *Evidence*, 13 June 2024, 1635 (Chloe Rourke).

> huge gender skew to that. I think you have to look at that fact in context with our treatment of women more broadly. Also, look at it specifically in the context of physical, as you said, real-world violence against women, which is often taking place in conjunction with online violence against women. Many of the revenge porn cases we've seen litigated … have been in the context of intimate partner violence. … I think those things aren't separable. I think you need to have education to combat both and see them as fundamentally linked.[161]

Ms. Rourke said, "[e]ducation and combatting that societal, cultural context is part of the solution. It's not going to fix the technology, but educating in schools to understand the harms so that teenage boys … know why it's so harmful is part of the solution."[162]

CONCLUSION

Over the course of the study, the Committee heard unequivocally that the spread of CSAM and NCDII, including deepfakes, is an urgent and growing problem that requires a comprehensive and multifaceted response, with governments, law enforcement, online platforms, civil society, teachers and parents all playing a role.

Witnesses were broadly supportive of Part 1 of Bill C-63, the government's online harms legislation, though several noted it was just a first step and would require amendments. The emphasis on platform accountability in combatting CSAM, NCDII and deepfakes was recognized as an effective approach to curbing the proliferation of illegal, sexually explicit material.

The rapid rise of AI-generated deepfake technology presents a serious concern, severely exacerbating the threat of CSAM and NCDII. A number of witnesses agreed that deepfakes should be explicitly added to the *Criminal Code* but that international cooperation, platform accountability and other measures were also urgently needed to confront the new technology and its abuses.

Witnesses also agreed on the need for education and awareness campaigns aimed at children, youth and the general public, not only around online safety but the broader context of gender-based violence as well.

The concluding words of this study should be left to Carol Todd, the mother of Amanda Todd, who died by suicide following extensive online harassment and cyber abuse in 2012:

161 CHPC, *Evidence*, 13 June 2024, 1725 (Chloe Rourke).

162 CHPC, *Evidence*, 13 June 2024, 1635 (Chloe Rourke).

> As an educator, I feel strongly that increasing education is crucial. The awareness and education needs to go to our children and our young adults and to our families.
>
> We need stronger regulations and laws. Bill C-63 is one of them. I know that in the province of B.C., more legislation has been passed and is done.
>
> We need to improve our online platforms and make them accountable. We need to increase parental controls and monitoring, and we need to encourage reporting.
>
> We also need to promote positive online behaviours. Social emotional learning and social responsibility are part of the awareness and the education that needs to come on.
>
> We need to be a voice. We need to stand up, and we also need to do more.[163]

RECOMMENDATIONS

The Committee recommends:

Recommendation 1

That the collection of, and access to, local and national intersectional data related to the non-consensual distribution of intimate images be supported, particularly by creating a database in collaboration with federal and provincial statistics services.

Recommendation 2

That an awareness campaign be launched with the objective of informing children and teens, in addition to equipping educators and parents, about

- **the consequences of viewing sexually explicit content depicting violent and abusive sexual behaviour, particularly for minors;**
- **the impact on victims of the non-consensual distribution of intimate images, including the creation and distribution of sexually explicit deepfakes; and**
- **tools to address sextortion.**

163 CHPC, *Evidence*, 11 June 2024, 1720 (Carol Todd).

Recommendation 3

That measures be put in place to improve victims' access to resources, particularly with regard to reporting.

Recommendation 4

That digital platforms implement processes for detecting and reporting illegal, sexually explicit content, such as child sexual abuse material and the non-consensual distribution of intimate images (including deepfakes), and that such content be removed immediately once it has been identified, under threat of penalty.

Recommendation 5

That section 161.1(2) of the *Criminal Code*, which defines "intimate image," be amended to include the concept of sexually explicit deepfakes.

Recommendation 6

That a study be undertaken on the involvement of private messaging platforms in the distribution of illegal, sexually explicit content, such as child sexual abuse material, and on possible legislative measures to regulate these platforms and protect users.

Recommendation 7

That the development of technologies to combat the distribution of illegal, sexually explicit content, such as child sexual abuse material and non-consensual intimate images, be supported.

Recommendation 8

Recognize that action to stop the use of illegal sexually explicit material must be part of the Government of Canada's broader agenda to promote gender equality and to end gender-based violence.

APPENDIX A:
LIST OF WITNESSES

The following table lists the witnesses who appeared before the committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the committee's webpage for this study.

Organizations and Individuals	Date	Meeting
Homewood Health, Inc.	2024/04/09	114
Claude Barraud, Psychotherapist		
IWK Health Centre	2024/04/09	114
Holly Murphy, Advanced Practice Leader of Trauma Informed Care		
Lila Pavey, Prevention and Health Promotion Specialist		
As an individual	2024/06/11	124
Vivek Krishnamurthy, Associate Professor of Law, University of Colorado Law School		
Emily Laidlaw, Associate Professor and Canada Research Chair in Cybersecurity Law, University of Calgary		
Amanda Todd Legacy Society	2024/06/11	124
Carol Todd, Founder and Mother		
Centre for Research and Education on Violence Against Women and Children	2024/06/11	124
Dianne Lalonde, Research and Knowledge Mobilization Specialist		
Connecting to Protect	2024/06/11	124
Jocelyn Monsma Selby, Chair, Clinical therapist, Researcher specialising in Forensic Sexology and Addiction		
Sûreté du Québec	2024/06/11	124
Marc-Antoine Vachon, Lieutenant		

Organizations and Individuals	Date	Meeting
As an individual	2024/06/13	125
Signa Daum Shanks, Associate Professor, University of Ottawa, Faculty of Law		
Shona Moreau, BCL/JD, Faculty of Law, McGill University		
Chloe Rourke, BCL/JD, Faculty of Law, McGill University		
Keita Szemok-Uto, Lawyer		
Heidi Tworek, Associate Professor, University of British Columbia		
Canadian Centre for Child Protection Inc.	2024/06/13	125
Monique St. Germain, General Counsel		

APPENDIX B:
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the committee related to this report. For more information, please consult the committee's webpage for this study.

Defend Dignity

Evangelical Fellowship of Canada

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 114, 124, 125, 130 and 133) is tabled.

Respectfully submitted,

Hon. Hedy Fry, P.C., M.P
Chair

Conservative Dissenting Report on Harms Caused to Children, Women, and Men by the Ease of Access to, and Online Viewing of, Illegal Sexually Explicit Material

The House of Commons Standing Committee on Canadian Heritage

On behalf of the Conservative members of the Standing Committee on Canadian Heritage, we submit this dissenting report on Harms Caused to Children, Women, and Men by the Ease of Access to, and Online Viewing of, Illegal Sexually Explicit Material. It is paramount that the current Liberal government properly address the online harms Canadians experience daily.

The study of online harms in committee was made possible through a Conservative motion that recognized a desperate need to understand the real harm experienced by many Canadians within virtual spaces and how it contributes to real world violence against women and girls and sex trafficking. This motion came prior to Bill C-63, the Online Harms Act, which continues to neglect the harms inflicted upon Canadians while adding undemocratic censorship.

As technology rapidly evolves, the government must urgently provide meaningful and real legislative protection against online harms.

The committee heard from various witnesses ranging from legal experts, law enforcement, advocates, and victims of online harms. Through witness testimony, it became overwhelmingly clear that legislation must be modernized to deal with online harms while taking on a victim-centric approach that protects those directly affected by online harms. While the committee's main report highlights important aspects of online harms, it fails to address the following points raised in the committee: 1) Women are overwhelmingly the primary targets of online harms; 2) Current government legislation fails to include deepfakes, but Bill C-412 provides the overdue criminal code amendments to address deepfakes; 3) Existing legislation must be amended to address the criminal nature of online harms; 4) A victim-centered approach is needed, and 5) More effort is needed to prevent uploading of Illegal Sexually Explicit Material.

1. Women are overwhelmingly the primary targets of online harms

There is a clear and alarming gendered dynamic to online harms. While online harm affects everyone, most incidents are targeted against women. One witness, Ms. Dianne Lalonde, highlighted the overwhelming harm occurring against women:

> NCIID (the non-consensual distribution of intimate images) does disproportionately target women. Out of the 295 Canadian cases of NCIID reported to police by adults in 2016, 92% were reported by women. Police-reported incidents, from 2015 to 2020, by

> youth 12 to 17, found girls, again, overrepresented as targets, at 86%, in comparison to boys at 11%.

Many witnesses at committee also expressed this concern, especially, in relation to the creation, distribution and viewing of deepfakes. Ms. Dianne Lalonde referenced a study illustrating the immensely disproportionate targeting of females online:

> A study of 95,000 deepfake videos in 2023 found that 98% were sexually explicit, and of those, 99% targeted women.

This fact, along with its frightening consequences was similarly echoed by Ms. Shona Moreau and Ms. Chloe Rourke:

> The non-consensual sharing of porn is already weaponized against women and is further exacerbated by deepfakes because anyone is able to create and distribute such content. Women will have limited options to protect themselves. It's already being used to target, harass and silence female journalists and politicians. If unchecked, deepfakes threaten to rewrite the terms of participation in the public sphere for women.

Women are overwhelmingly targets of online harms. This fact must be acknowledged and addressed in whatever legislative effort is put forward.

2. Current legislation fails to include deepfakes

The evolving capabilities of technology create increasingly accessible avenues for harm, such as the creation, distribution, and viewing of deepfakes. Deepfakes can easily be made to target any Canadian, regardless of social status or any other demographic difference. Ms. Shona Moreau and Ms. Chloe illustrated this in committee:

> Lifelike deepfakes can now be generated using just a single photo of a person. As a result, it's not just celebrities and public figures who are vulnerable. Everyone is vulnerable to this technology. And though there are other applications to deepfakes, by far the most common use is non-consensual porn.

Witnesses highlighted a glaring failure in current legislation to address the threat of deepfakes. Ms. Shona Moreau and Ms. Chloe Rourke stated this:

> I think the Criminal Code provisions that currently exist applying to actual real recordings of intimate images or so-called revenge porn is an incomplete remedy as it exists, not even including the issue of deepfake.

The Liberals' current attempt at legislating in this area, Bill C-63, fails to acknowledge and address the real danger of deepfakes and the tremendous harm they can do. Thus, the legislation is antiquated even before it comes into effect.

In contrast, Conservative Bill C-412 has a framework to update the Criminal Code with a legal definition capturing deepfakes and criminalize distribution. A number of witnesses expressed the importance of this approach including Ms. Dianne Lalonde who stated:

> We've certainly seen success in the U.K. in terms of their criminalization of distribution, so that does remain important.

To truly protect Canadians from online harms, deepfakes must be addressed in legislation.

3. Existing legislation must be amended to address the criminal nature of online harms

The harm caused by certain online behaviours is often severe and can even be fatal. Such incidents are criminal by nature.

Legislation must be modernized by amending it to address the criminal nature of online harms.

Many witnesses heard from at committee, urged the government to amend the Criminal Code to include online harms. When asked about including deepfakes to the Criminal Code, Ms. Dianne Lalonde stated: "Yes, I think so. I think, more than anything, it signals this as a form of violence."

Criminalizing online acts like the creation, distribution, and viewing of deepfakes would signal such actions as a form of violence.

4. A victim-centric approach is needed

When creating legislation, a victim-centered approach is needed to protect and support victims of online harms. Witnesses at the committee meetings made this abundantly clear by advocating for strengthening existing support for victims. One witness, Ms. Dianne Lalonde, reinforced this need by stating:

> In terms of ways to address this harm, I think much of the focus on legislation has been on regulation and removal of content, and that is absolutely essential. We also need to recognize the people this is impacting, the survivors and who survivors are going to. They are going to gender-based violence services in order to cope and heal from these harms. An added dimension when we're talking about addressing online harms is

> making sure we're supporting the gender-based violence agencies that are doing the work to support survivors who already have robust sex education programs.

Protecting Canadians from online harms requires focusing on protecting, supporting, and strengthening victims of online harms.

5) More effort is needed to prevent uploading of Illegal Sexually Explicit Material

The mandate of this study included consideration of preventative legal frameworks. Witnesses and submitted briefs pointed to the harm caused by the uploading and re-uploading of illegal content such as CSAM and NCIID. Once illegal sexually explicit material has been uploaded, it is virtually impossible to eliminate and can be reuploaded endlessly.

In a submitted brief, Defend Dignity noted that:

> Many of the survivors of sexual exploitation we work with have shared the nightmare of losing control over non-consensual intimate images of themselves. This is re-traumatizing and victimizing in a different way than other forms of abuse they endured. The platforms hosting the abuse are profiting from their pain, while users of the services view, comment, and sometimes further share the abusive content for their own pleasure. It's an impossible fight to get the content permanently removed from the internet, and they never know when or where it will resurface. There is also the dread of not knowing who will view the abusive content – will they be recognized by a stranger? Will their children see it?

They and other organizations recommended the passage of Conservative Bill C-270 which would focus on prevention by requiring on companies to obtain the age and meaningful consent of everyone depicted before creating or distributing pornographic content.

Summary:

There is a growing need to protect Canadians from the threat of online harms. The study of online harms at committee confirmed that women are the overwhelming target of online harms, the problem of deepfakes has failed to be addressed, current legislation must be amended, a victim-centric approach is needed, and more effort is needed to prevent uploading of Illegal Sexually Explicit Material. Current methods of addressing online harms are insufficient. The Liberal government's online harms legislation, Bill C-63, will not satisfy the need for protection and will only limit the freedoms of Canadians.

Conservatives contend that Canadians can be protected from online harms while still having their freedoms respected and preserved. Online harms must be included in the Criminal Code

to signal the violent nature of the acts and protect Canadians from all virtual harms including deepfakes.