Permanent Mission of Canada
to the United Nations
and the World Trade Organization

Mission permanente du Canada
auprès des Nations Unies
et de l'Organisation mondiale du commerce

GENEV- 10386

The Permanent Mission of Canada to the United Nations and the World Trade Organization at Geneva presents its compliments to the Special Rapporteur on violence against women and girls, its causes and consequences and Special Rapporteur on the right to privacy, pursuant to Human Rights Council resolutions 59/20 and 55/3, and has the honour to make reference to the letter dated 13 February 2026 (reference AL CAN 7/2025).

In this regard, the Permanent Mission of Canada has the honour to submit Canada's response.

The submission consists of one document.

The Permanent Mission of Canada to the United Nations and the World Trade Organization at Geneva avails itself of the opportunity to renew to the Office of the High Commissioner for Human Rights the assurances of its highest consideration.

Mission permanente du Canada auprès de l'ONU, de la [illegible] et de l'OMC
Permanent Mission of Canada to the UN, CD, and WTO
Geneva - Genève

[redacted]

Geneva, 29 April 2026.

Canada

Canada's response to Joint Communication from Special Procedures, OHCHR: April 2026

1. **Please provide any additional information and/or comment(s) you may have on the above-mentioned allegations.**

As noted in the communication, the Office of the Privacy Commissioner of Canada conducted an investigation into Aylo (formerly MindGeek) and issued findings in February 2024, concluding that the company's practices contravened the Personal Information Protection and Electronic Documents Act (PIPEDA). Specifically, the investigation findings noted the company's inability to demonstrate that it had obtained appropriate consent from individuals depicted in content or verified compliance with age-related requirements. The Government acknowledges these findings and notes that previous privacy-related legislative modernization efforts included measures to strengthen enforcement to better address privacy violations and protect Canadians' personal information. The Minister of Artificial Intelligence and Digital Innovation has publicly stated his intention to present a new bill to modernize Canada's federal private sector privacy law at the earliest opportunity.

2. **Please indicate the measures you have taken to ensure that women and children, including girls that have been the victims of image based sexual abuse, have the means to effectively report and to find effective redress, assistance and support.**

Canada condemns in the strongest terms all forms of discrimination against women of all ages and girls wherever it occurs. Technology-facilitated gender-based violence is a serious problem worldwide and a priority for Canada. The Government of Canada is committed to putting an end to gender-based violence in all of its forms. Canada is also a strong advocate of urgent action to protect children from violations and abuses of their rights.

The Government of Canada has implemented a multi-faceted approach to address image-based sexual abuse—including online child sexual exploitation, cyberbullying, non-consensual distribution of intimate images and other technology-facilitated gender-based violence—particularly targeting the protection of women and children. These measures include dedicated reporting mechanisms, legislative and regulatory reforms, proactive technology tools, and funding for support services.

As it pertains to minors, the Government of Canada launched the *National Strategy for the Protection of Children from Sexual Exploitation on the Internet* (National Strategy) in 2004. Public Safety Canada is the lead for the National Strategy and partners with the Royal Canadian Mounted Police, Justice Canada and the Canadian Centre for Child Protection, a not-for-profit organization dedicated to child safety. The National Strategy offers a comprehensive set of measures under four pillars: Prevention and Awareness, Protection, Prosecution, and Partnerships/Research. Federal efforts aim to prevent and raise awareness of online child sexual exploitation, reduce the stigma

associated with reporting, increase Canada's ability to pursue offenders, enhance knowledge and understanding of the crime type, and advance collaboration with partners and stakeholders.

As part of its commitment to create a safer online environment, in March 2026, the Minister of Canadian Identity and Culture and Minister responsible for Official Languages reconvened the expert advisory group on online safety to engage on new and emerging issues related to online harms. This followed a series of nine workshops, led by Canadian Heritage in 2022 with these experts on the important topic of online safety.

The Government of Canada will seek the group's expertise and advice on a limited and targeted set of issues that have emerged since the last consultation due to significant technological changes, including in the field of artificial intelligence (AI), chatbots and AI companions, as well as other evolving trends related to online services. The group's findings will subsequently go on to inform ongoing legislative work in various aspects of online safety.

Additional Measures:

Reporting and Removal Mechanisms

- **Cybertip.ca:** Operated by the Canadian Centre for Child Protection, Cybertip.ca is the national tipline for reporting suspected cases of online sexual exploitation of children, including the non-consensual sharing of intimate images of minors. Reports pertaining to potentially illegal content are then forwarded to the appropriate law enforcement jurisdiction, international hotline, or a notice is sent to the electronic service provider for removal of the material.
- **Project Arachnid:** the Canadian Centre for Child Protection manages this innovative, victim-centric set of tools to combat the growing proliferation of known child sexual abuse material (CSAM) on the internet. Launched in 2017, Project Arachnid unifies automated CSAM detection methods with a team of dedicated analysts around the world to quickly send removal notices to electronic service providers.
- **NeedHelpNow.ca:** A resource providing information and guidance for a youth or adult survivor who has reported their child sexual abuse material and/or intimate image directly to the hosting company or platform, but notices that the content remains online.

Support, Assistance, and Redress

- The Royal Canadian Mounted Police's National Child Exploitation Crime Centre is the national law enforcement arm of the *National Strategy for the Protection of Children from Sexual Exploitation on the Internet*. It is the central point of contact for investigations related to the Organization for Security and Economic Co-operation in Europe (OCSE) across the country and internationally when the victim or offender is Canadian.
- Public Safety Canada also provides funding to other Canadian police of jurisdiction's Internet Child Exploitation units to boost specialized investigative capabilities.

- The Canadian Centre for Cyber Protection offers a broad range of trauma-informed support services to those who have been victimized online by luring, sexual extortion, and non-consensual distribution of intimate images, or who have had child sexual abuse images shared online. These services include helping individuals and caregivers understand what steps to take after online sexual victimization, assisting with crisis situations, guiding them through reporting processes, creating safety plans, reducing the online availability of abusive material, and connecting them with counselling, peer support, victim services, and child-advocacy resources as needed.

Legislative Measures

The *Criminal Code* of Canada comprises many offences capturing online sexual exploitation, including luring a child, invitation to sexual touching, possessing or accessing child sexual abuse and exploitation material, making or distributing child sexual abuse and exploitation material, harassment, uttering threats, extortion, intimidation, and indecent communications.

In 2015, the *Protecting Canadians from Online Crime Act* came into effect and created a new criminal offence of non-consensual distribution of intimate images (section 162.1 of the *Criminal Code*). Section 162.1 prohibits distributing, publishing, transmitting, selling, making available or advertising an "intimate image" without the consent of the person depicted in that image. "Intimate image" is defined as a visual recording in which a person is nude, is "exposing his or her genital organs or anal region or her breasts" or is engaged in explicit sexual activity, in respect of which the person depicted had a reasonable expectation of privacy at the time of the recording, and retains this expectation at the time of the commission of the offence.

When prosecuted as an indictable offence, the maximal sentence is five years of imprisonment. The *Criminal Code* also allows the court to make an order prohibiting a convicted or discharged offender from using the Internet and other digital networks or limiting its use. The *Criminal Code* also provides that a court may order that the offender makes restitution to the victim for expenses linked to the removal of their intimate image from the Internet.

The *Criminal Code* authorizes courts to order the takedown or removal of non-consensual intimate images and child sexual abuse and exploitation material. It also authorizes courts to order the forfeiture of anything that was used in the commission of an intimate image offence or a child sexual abuse and exploitation material offence.

The *Criminal Code* also authorizes a court to impose a peace bond where a person fears, on reasonable grounds, that another person will distribute an intimate image without consent. A peace bond is a preventive tool that is used where a person has a reasonable fear that another person will commit a criminal offence (i.e. no offence needs to have already occurred). The court may impose any reasonable conditions to secure the good conduct of the defendant for up to 12

months. If the defendant fails or refuses to enter into the peace bond, they can be detained in prison for up to 12 months. If they breach the conditions of the peace bond, they may face up to four years of imprisonment on indictment or up to two years on summary conviction.

The *Protecting Canadians from Online Crime Act* (2015) also clarified that all offences containing an element of communication included telecommunications.

There were 1,728 police-reported incidents of non-consensual distribution of intimate images in Canada between 2015 and 2022. In this period, nearly all (97%) child victims of non-consensual distribution of intimate images offences were youth (i.e. between 12 and 17 years old). Non-consensual distribution of intimate images was reported as the most serious violation for almost all (98%) of these incidents. 41% of single incidents of non-consensual distribution of intimate images and 48% of multiple incidents of non-consensual distribution of intimate images were cleared (solved). Nine in ten (90%) persons accused of this offence were youth.

Section 163.1 of the *Criminal Code* defines child sexual abuse and exploitation material and makes its creation, distribution, possession, and access – among other conducts – criminal offences. Under the Criminal Code, child sexual abuse and exploitation material includes material produced through any electronic or mechanical means, thus covering material altered or generated using AI technologies. Sexual extortion, i.e., using threats, accusations, menaces, intimidation, or violence with the intent to obtain sexually explicit images is illegal under extortion provisions found in section 346 of the Criminal Code.

The federal government is considering enacting legislation to hold social media services accountable for harmful content – including child sexual abuse and exploitation material and intimate content shared without consent – found on their platforms.

The *Criminal Code* provisions are complemented by federal legislation. The federal *Act respecting the mandatory reporting of Internet child sexual abuse and exploitation material by persons who provide an Internet service* (2011) places obligations on those who provide an Internet service to the public. It requires them to report to the Canadian Centre for Child Protection if they are advised of an Internet address where child sexual abuse and exploitation material may be available to the public, or to law enforcement if they have reasonable grounds to believe that their Internet service is being or has been used to commit a child sexual abuse and exploitation material offence.
To strengthen protections for people in Canada against image based sexual abuse, Bill C-16, *the Protecting Victims Act*, was introduced on December 9, 2025. This Bill proposes to expand the definition of “intimate image” provided for in section 162.1 of the *Criminal Code* to include sexual deepfakes. Bill C-16 would also create a new offence that prohibits threatening to distribute, publish, transmit, sell, make available or advertise an intimate image, including a sexual deepfake, if the person knows the person depicted in that image would not consent to that conduct or was reckless as to that fact, and if the person intended to intimidate or to be taken seriously. It also proposes to increase the maximum penalty that applies to section 162.1 from five years to ten years imprisonment on indictment.

Bill C-16 also proposes a range of reforms to combat online sexual exploitation, including by:

- amending the criminal harassment offence to by removing the need to prove the victim's subjective fear, instead requiring proof that a reasonable person in the victim's circumstances would perceive a threat to their physical or psychological safety, reducing the need for survivors to relive their trauma in court;
- addressing extortion, by criminalizing threatening to distribute child sexual abuse and exploitation material, ensuring the child luring offence references extortion so that it applies to sexual extortion cases, and adding an aggravating factor to the extortion provision where that offence is committed in sexual extortion cases;
- expanding existing child sexual offences prohibiting invitation to sexual touching and sexual exploitation to protect children from individuals who may invite or incite them to expose their sexual organs for a sexual purpose; and
- amending an *Act respecting the mandatory reporting of Internet child sexual abuse and exploitation material by persons who provide an Internet service* to strengthen the ability of law enforcement agencies to investigate cases involving child sexual abuse and exploitation material and to improve enforcement of the Act, in particular by centralizing mandatory notifications to a law enforcement agency and extending the limitation period for prosecution under the Act from 21 days to 12 months.

3. **Please provide information on any interactions of your Excellency's Government with Aylo Holdings S.A.R.L., domiciled in Canada, in relation to regarding the potential human rights violations against women and girls in the context of the distribution of pornographic material.**

Nil.

4. **Please provide information on how your Excellency's Government intends to ensure that use of payment services on websites that allow the distribution of user-generated pornographic content without reliably verifying the age and consent of all individuals is prohibited, with the purposed of preventing the distribution and monetization of serious violations of human rights including sexual crimes.**

Existing *Criminal Code* offences address the conduct targeted by question 4. For example, making pornography without the depicted person's knowledge constitutes voyeurism (section 162); making pornography without a person's consent may constitute human trafficking (section 279.01 to 279.03); filming or distributing a recording of a sexual assault constitutes obscenity (section 163); and, making and distributing child sexual abuse and exploitation material are themselves criminal offences (subsections 163.1(2) and (3)). Also, distributing intimate images without the consent of the person(s) depicted in those images constitutes non-consensual distribution of intimate images (section 162.1), and the *Criminal Code* authorizes courts to order the takedown or

removal of non-consensual intimate images and child sexual abuse and exploitation material (sections 164 and 164.1).

All of these offences, most of which impose severe penalties, apply to both individuals and "organizations", defined to include corporations (section 2 of the *Criminal Code*), because "everyone" and "person" and similar expressions are defined to include an organization (section 2).

The *Criminal Code* does not, however, contain offences that seek to regulate particular industries, such as requiring platforms with user-generated pornographic content to verify the age and consent of individuals, and there is no specific regulatory statute targeting this conduct.

5. **Kindly state how your Excellency's Government intends to prevent the making and distribution and monetization of violent and degrading pornographic material online.**

Existing *Criminal Code* offences address the conduct targeted by question 5. For example, making pornography without the depicted person's knowledge constitutes voyeurism (section 162); making pornography without a person's consent may constitute human trafficking (section 279.01 to 279.03); filming or distributing a recording of a sexual assault constitutes obscenity (section 163); and, making and distributing child sexual abuse and exploitation material are themselves criminal offences (subsections 163.1(2) and (3)). Also, distributing intimate images without the consent of the person(s) depicted in those images constitutes non-consensual distribution of intimate images (section 162.1), and the *Criminal Code* authorizes courts to order the takedown or removal of non-consensual intimate images and child sexual abuse and exploitation material (sections 164 and 164.1).

Violent and degrading pornographic material may be captured by the definition of "obscene material" provided for in section 163 of the *Criminal Code*. Obscene material is defined as "any publication a dominant characteristic of which is the undue exploitation of sex, or of sex and any one or more of the following subjects, namely, crime, horror, cruelty and violence, shall be deemed to be obscene." The *Criminal Code* prohibits, among other conducts, making, distributing, and possessing for the purpose of publication or distribution of obscene material.

Bill C-16, the *Protecting Victims Act,* would also address this issue by making it criminal to distribute sexual deepfakes without consent and to distribute bestiality depictions, including deepfakes. Bestiality is defined by section 160(7) of the *Criminal Code* as "any contact, for a sexual purpose, with an animal".

Additionally, in March 2026, the Minister of Canadian Identity and Culture and Minister responsible for Official Languages, reconvened the expert advisory group on online safety to engage on new and emerging issues related to online harms. This followed a series of nine workshops, organized by Canadian Heritage in 2022, with these experts on the important topic of online safety.

The Government of Canada will seek the group's expertise and advice on a limited and targeted set of issues that have emerged since the last consultation due to significant technological changes, including in the field of artificial intelligence (AI), chatbots and AI companions, as well as other evolving trends related to online services. The group's findings will subsequently go on to inform ongoing legislative work in various aspects of online safety.