CANADIAN CENTRE *for* CHILD PROTECTION®

Helping families. Protecting children.

CHILDREN'S EXPERIENCES AND PERSPECTIVES ON SEXUAL VIOLENCE ON THE INTERNET

INFORMING POLICY FOR A MADE-IN-CANADA ONLINE SAFETY REGIME

Model in image and intended as illustrative.

CANADIAN CENTRE *for* CHILD PROTECTION®

Helping families. Protecting children.

Data sources for this report are as outlined in the "Method" section and further details about the survey methodology are in Appendix A. Data was collected between April 29 and May 20, 2025. All interpretation of the survey results was conducted internally by staff at the Canadian Centre for Child Protection Inc. E. & O.E. The survey results referencing specific companies represent the experience reported by the teen victims who participated in the survey; the experience of other teens with the same company may differ.

CONTENTS

SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS

Nearly 9 in 10 teen victims (86%) were harmed in private messaging environments.

Recommendation: Ensure online safety regimes impose appropriate duties of care and obligations onto private communication services and functions.

Harm occurred on many popular apps and platforms, with 2 in 5 teen victims (39%) sexually victimized on Snapchat®.

Recommendation: Online safety regimes must scope in and apply to a broad range of platforms, with graduated obligations based on a given service's anticipated or known risk factors.

Of teen victims who reported a nude or sexual image of them to an app or platform, 2 in 3 (67%) waited over a day for it to be removed. Teen victims also thought apps and platforms should prevent the non-consensual distribution of teens' nude and sexual images.

Recommendation: Online safety regimes must set clear expectations for online service providers to proactively detect, and quickly review and remove, reported nude or sexual images of minors.

At least 1 in 4 teen victims (25%) experienced online sexual violence involving an adult offender.

Recommendation: Online safety regimes must require online service providers to prevent potentially unsafe online interactions between adults and children. Updates to Canada's *Criminal Code* to address luring tactics should also be considered.

Over 1 in 2 teen victims (52%) had been sent an unwanted nude or sexual image, and 1 in 6 (17%) had someone make a "fake" nude or sexual image of them.

Recommendation: Amend the *Criminal Code* to address the creation and sharing of nude and sexual deepfakes, and consider whether existing *Criminal Code* offences adequately address cyberflashing.

Over 9 in 10 teen victims (93%) think Canada should legally force apps and platforms to prevent harm online. Most also thought safety measures would help.

Recommendation: Canada should introduce an online safety regime that requires apps and platforms be designed with safety in mind and provide children with enhanced protections.

ABOUT THE CANADIAN CENTRE FOR CHILD PROTECTION

The Canadian Centre for Child Protection (C3P) is a national charity dedicated to the personal safety of all children. Our goal is to reduce the sexual abuse and exploitation of children through programs, services, and resources for Canadian families, educators, child-serving organizations, law enforcement, and other parties. C3P also operates: Cybertip!ca®, Canada's tipline to report child sexual abuse and exploitation on the internet; Project Arachnid®, a victim-centric set of tools to combat the growing proliferation of child sexual abuse material on the internet; and NeedHelpNow.ca™, which supports those who are worried a nude of them under the age of 18 is being shared online, or are experiencing other forms of online sexual violence.

Through the above and other initiatives, C3P supports survivors whose child sexual abuse was recorded and distributed online. Through our work with survivors, crucial contextual information about the nature of child sexual abuse is collected and shared with stakeholders committed to the safety and protection of children.

INTRODUCTION

In Canada, children* are being sexually victimized online at an alarming rate.[1]

The daily stream of police and media reports available to the general public provides some insight into the nature of these harms: nation-wide police operations lead to mass arrests for online child sexual abuse and exploitation material ("CSAEM") related crimes,[2] thousands of boys and young men have been targets of financial sexual extortion tactics,[3] and artificial intelligence ("AI") apps and platforms that create realistic looking nudes are being weaponized against girls in Canadian schools.[4] In terms of scope, it is estimated that nearly one third of 13- to 18-year-olds in Canada have experienced some form of online sexual violence,[5] a figure that is generally consistent with estimates from other countries.[6,7]

Authorities and researchers have recognized online child sexual violence as a major public safety and health concern,[8,9,10,11] as experiencing online sexual violence as a child can have negative psychological, emotional, and social impacts that can endure into adulthood.[12,13,14,15] When a child's victimization involves nude or sexually abusive photos or videos of them, the fact that those images could be continually shared online can add additional layers of shame, self-blame, and concern,[16,17,18,19] and in some cases, may lead them to experience further victimization online and offline.[20,21] In these ways, online sexual violence against children violates their rights to privacy, safety, and freedom from exploitation.[22]

Model in image and intended as illustrative.

Online sexual violence against children is not an inevitable part of our increasingly digital lives. Through well-designed policies, governments can ensure online services and the broader technology industry are obligated to safeguard online users and prevent harms from occurring in the first place. This approach is different from a criminal law or policing response, which are reactive in nature and only address harms that meet a criminal threshold, leaving the broad spectrum of non-criminal harms – often referred to as "awful, but lawful" – unaddressed.

Encouragingly, several countries have already begun adopting online safety regimes.[23,24,25] Canada, though, has yet to successfully legislate a comprehensive national online safety framework.

* In this report, the words "child" and "children" refer to people under the age of 18.

In 2024, after nearly two years of consultations, the Canadian government introduced Bill C-63, which would have enacted a new statute called the *Online Harms Act.* This proposed legislation contained a number of features, including, but not limited to, duties of care for certain online services, updates to mandatory reporting laws related to the discovery of CSAEM, and amendments to the *Criminal Code* and the Canadian Human Rights Act. [26]


Model in image and intended as illustrative.

Chief among the concerns with Bill C-63 from the perspective of C3P, was the overly narrow scope of online services that would have been subjected to regulatory oversight as well as the lack of clarity over how online services would fulfil the proposed duties of care to children without a corresponding obligation to identify minors using their services.[27,28] Though Bill C-63 died on the order paper in early 2025 following the prorogation of Parliament, the Government of Canada and all major federal political parties have continued to express commitment to protecting children online.[29,30,31,32]

The Government of Canada now has an opportunity to create a strong online safety regime – one that addresses the gaps of previous attempts and builds on the lessons learned from other jurisdictions – that will ensure online services are accountable for the harms their services facilitate or cause, while requiring them to protect users, especially children from online sexual violence. To be most effective, an online safety regime must also be informed by the voices of those with lived experience. Toward that goal, this report presents the perspectives of nearly 1,300 teens in Canada who have been sexually victimized online. Through survey responses, they share valuable insights including the apps and platforms where they've been victimized, how platforms responded to their reports, and reasons why they haven't reported harms to platforms. The teen victims also weighed in on whether Canada should have online safety regulation and the perceived effectiveness of several policy measures.

METHOD

C3P developed a questionnaire and commissioned Leger, a market research and polling firm, to conduct an anonymous online survey. The survey was available in English and French. The 1,279 survey participants met the following criteria:

- Were 13 to 17 (inclusive) years of age at the time of the survey;
- Lived in Canada; and
- Experienced at least one form of online sexual victimization (discussed later under "Types of online sexual violence").

To ensure nationally representative results, the data was weighted on age, gender, and province/territory based on demographics from the 2021 Canadian census. The demographics are in Figure 1 and further details about the survey methodology are in Appendix A.

In this report, all noted group differences involve comparisons between groups of at least 100 participants and are statistically significant at $p < .05$. Some totals may exceed 100% due to rounding.

Figure 1. Demographics of teen victims who completed the survey

Gender	
Girl	52%
Boy	47%
Another gender	1%

Age	
13	15%
14	20%
15	28%
16	22%
17	15%

Sexual orientation	
Heterosexual	87%
Bisexual	4%
Lesbian	1%
Gay	1%
Pansexual	1%
Asexual	1%
Questioning	1%
Queer	<1%
Two-spirit	<1%
Self-describe	<1%
Prefer not to answer	2%
Don't know	2%

Race/ethnicity	
White	72%
Black	8%
South Asian	4%
Chinese	4%
First Nations	4%
Filipino	3%
Latin American	3%
Métis	2%
Arab	2%
Jewish	1%
Southeast Asian	1%
West Asian	<1%
Another race/ ethnicity	2%
Prefer not to answer	1%
Don't know	<1%

Region	
Ontario	34%
Quebec	19%
British Columbia	16%
Alberta	14%
Saskatchewan	4%
Manitoba	3%
New Brunswick	3%
Nova Scotia	3%
Newfoundland and Labrador	2%
Prince Edward Island	1%
Northwest Territories	1%
Nunavut	<1%

RESULTS

Experiences of online sexual violence

Types of online sexual violence

To be eligible for this survey, teens must have experienced at least one of seven types of online sexual violence defined in this survey.

Unwanted sexual talk

By far, the most common type of online sexual violence experienced by teen victims was unwanted sexual talk. This term was defined as having someone try to "get you to talk about sex, or say something sexual to you" in a way the teen didn't want (see Figure 2). Four in 5 (79%) teen victims had experienced unwanted sexual talk, with sexual and gender minority teens being especially likely to have experienced this (88% vs. 77% of sexual and gender majority teens;** Figure 3 shows group differences). Note that this is the only harm type that had large enough sample sizes to allow for stable statistical comparisons between sexual and gender minority versus majority teens; however, other research has established that sexual and gender minority youth experience higher rates of online child sexual abuse than do sexual and gender majority youth.[33,34]

Image-based sexual violence

The remaining kinds of online victimization discussed in the survey were different forms of image-based sexual violence. All of these refer to "nude or sexual images," which was defined in the survey as "photos or videos that are nude, partially nude, sexual, or sexually abusive." Some of these victimization types refer to "real nude or sexual images," meaning images that were taken of the teen when they were naked, engaging in consensual sexual activity, or being sexually abused. In contrast, "fake nude or sexual images" refers to images of the teen that were altered to appear as if they were naked, engaging in consensual sexual activity, or being sexually abused. These are also sometimes referred to as "deepfake nudes" or "sexual deepfakes," which can be created using basic photo editing tools or specialized "nudify" or "undress" apps and platforms that use AI technology.[35,36]

Model in image and intended as illustrative.

4 in 5 teen victims experienced unwanted sexual talk online

Model in image and intended as illustrative.

** Teens in the sexual and gender minority group either had both a sexual minority identity and a gender minority identity, or had one of these identities. Teens in the sexual and gender majority group did not have a sexual minority identity or a gender minority identity.

Unsolicited nude or sexual images

Over 1 in 2 teen victims (52%) had someone send them unwanted nude or sexual images online. Older teens were especially likely to have received these (55% of 15-17-year-olds vs. 47% of 13-14-year-olds). Often referred to as "unsolicited intimate images," "cyberflashing," and, when the images are of male genitalia, "dick pics," this form of online sexual violence has been criminalized in jurisdictions such as the U.K.[37] Canada's *Criminal Code* has certain offences that address the distribution of sexual images to children, but consideration should be given to whether these offences fully cover the range of harm arising from cyberflashing incidents. Of note, Canada's indecent exposure offence, which is sometimes applied to online incidents, only protects children under the age of 16.

Pressure to send nude or sexual images

Over 2 in 5 teen victims (44%) had someone online pressure them to send a nude or sexual image of themselves. Those more likely to have had this happen to them included older teens (47% of 15-to-17-year-olds vs. 39% of 13-to-14-year-olds) and girls (50% vs. 38% of boys).

Threatened distribution of nude or sexual images

Nearly 1 in 4 (23%) teen victims have had someone threaten to post, send, or show others nude or sexual images of them – either real or "fake" images. This figure likely represents a range of situations, including sextortion.

Model in image and intended as illustrative.

Sextortion (sexual extortion) is when someone threatens to share nude or sexual images of a victim with others, such as the victim's family and friends, in order to make the victim do something.[38,39] The images could be real sexual images of the victim (perhaps that the victim sent to the sextorter), "fake" sexual images that the sextorter created of the victim, or sexual images that are not of the victim but someone else might nonetheless believe are of the victim (such as photos of genitalia).

Up until recent years, sextortion tended to involve demands for more sexual images, for sexual acts, or to try and keep someone in a relationship.[40] Sextorters motivated by these acts are generally either known to the victim offline, such as an ex-partner or peer, or are someone the victim only knows online.[41,42]

In 2022, the sextortion landscape dramatically changed. Law enforcement[43,44,45,46] and tiplines[47,48] were reporting surges in **financially motivated sextortion.** Financial sextortion typically involves members of organized criminal groups who create social media accounts posing as young, attractive girls or women and send friend requests to potential victims, who are primarily young boys and men.[49] Often within their first conversation, a financial sextorter rapidly progresses from flirtatiously asking the potential victim to send or exchange nudes, to suddenly threatening to distribute the victim's nude images if the victim doesn't send them money or gift cards. Financial sextorters use incredibly aggressive tactics, like claiming they'll destroy a victim's life if the victim doesn't pay, or giving the victim a live countdown (e.g., "10... 9... 8...") to either pay or promise to pay.[50,51]

Sextortion can have devastating impacts on victims. Tragically, Canadian teens who have been victims of traditional and financial sextortion have taken their own lives.[52,53]

Distribution of nude or sexual images without permission

One in 5 teen victims (20%) had someone post, send, or show others their nude or sexual images online without their permission. This is the only type of victimization that was more common for boys than girls (24% vs. 17%) and may be covered by the *Criminal Code* offence of "non-consensual distribution of intimate images," which can often encompass other offences related to intimate partner violence, sextortion, or CSAEM.

Distribution of nude or sexual images without permission can take many forms, including:

- A sextorter follows through on their threats to send the teen's nudes to the teen's friends or family.
- A teen sends a nude of themselves to a dating partner over text, saying it's intended only for the partner. The dating partner forwards the nude to a group text of their friends.
- A teen takes a nude of themselves and saves it to their phone's camera roll. Someone hacks their phone and sends the nude to other people on social media.
- Someone uses an app to create a sexual deepfake of a teen, and texts it to a classmate.
- Someone secretly records a teen who is engaging in sexual activity and uploads the video to a pornography site.

In some situations, non-consensually shared nude or sexual photos or videos of a child may be considered **child sexual abuse and exploitation material ("CSAEM")**.

Creation of "fake" nude or sexual images without permission

Approximately 1 in 6 teen victims (17%) had someone make a "fake" nude or sexual image of them without their permission. Again, sexual deepfakes could be created using basic image editing tools on a smartphone or computer, or using newer AI "nudify" or "undress" apps or platforms.

Copies of real nude or sexual images without permission

Nearly 1 in 7 teen victims (15%) had someone make a copy of a real nude or sexual image of them by recording their live video or taking a screenshot of their photo, without their permission. This could include teens who have been **capped** – a term for when a person is naked or engaging in sexual activity on a video call or a livestream, and someone secretly records the video. Teens may have also had their nude or sexual images copied without their permission as part of a non-consensual distribution of intimate imagery incident or a sextortion incident.

Figure 2. Percentage of teen victims who experienced each type of online sexual violence

ScreenQ1-3: For full question text, see Appendix B.

	Yes	No	Don't know	Prefer not to answer
Tried to get you to talk about sex, or said sexual things to you?	79%	18%	2%	1%
Sent you a nude or sexual photo or video? For example, a photo of genitals, or a video of people having sex.	52%	46%	1%	1%
Pressured you to send them nude or sexual images of you (real or fake)?	44%	52%	2%	2%
Threatened to post, send, or show others nude or sexual images of you (real or fake)?	23%	73%	3%	1%
Posted, sent, or showed others nude or sexual images of you (real or fake), without your permission?	20%	70%	9%	1%
Made a fake nude or sexual image of you by editing or changing an image of you?	17%	73%	9%	1%
Made a copy of a real nude or sexual image of you by recording a live video or taking a screenshot?	15%	78%	6%	1%

Figure 3. Percentage of teen victims who experienced each type of online sexual violence – group comparisons

ScreenQ1-3: For full question text, see Appendix B.

	Overall	Age		Gender		Sexual and gender minority	
		13-14	15-17	Boy	Girl	No	Yes
Tried to get you to talk about sex, or said sexual things to you?	79%	76%	80%	73%	84%	77%	88%
Sent you a nude or sexual photo or video? For example, a photo of genitals, or a video of people having sex.	52%	47%	55%	53%	51%	52%	56%*
Pressured you to send them nude or sexual images of you (real or fake)?	44%	39%	47%	38%	50%	44%	52%*
Threatened to post, send, or show others nude or sexual images of you (real or fake)?	23%	22%	24%	23%	23%	23%	27%*
Posted, sent, or showed others nude or sexual images of you (real or fake), without your permission?	20%	20%*	21%	24%	17%	21%	17%*
Made a fake nude or sexual image of you by editing or changing an image of you?	17%	14%*	19%	18%	16%	17%	19%*
Made a copy of a real nude or sexual image of you by recording a live video or taking a screenshot?	15%	11%*	16%	16%	14%*	14%	16%*

*Note. *Subgroup size < 100*

Involvement of adult offenders

When considering all the online sexual victimization they'd experienced, 1 in 4 teen victims (25%) indicated that at least once, it had been an adult who victimized them (Figure 4); these teens may have also been victimized by other children. Another 1 in 5 (21%) did not know whether they'd ever been victimized by an adult online, and over half (53%) said they'd never been victimized by an adult online. This implies they believed they were victimized by another child, which police-reported data shows is common for several types of online sexual violence, such as non-consensual distribution of intimate images.[54] It is possible that some of these teens had been victimized by adult offenders who posed as children.

1 in 4 teen victims experienced online sexual violence involving an adult offender

Figure 4. Percentage of teen victims who've been sexually victimized by an adult online

Q4. When you've experienced the above, was it ever an adult who did this to you?

Yes	25%
No	53%
Don't know	21%
Prefer not to answer	1%

Where sexual victimization happens online

Apps and platforms

Snapchat was the most common platform where teens were sexually victimized (Figure 5), with 2 in 5 teen victims having experienced harm there (39%). Girls were especially likely to have been sexually victimized on Snapchat (46% vs. 32% of boys). It's also worth noting that the proportion of victimization on Snapchat alone nearly surpasses the combined total for the second and third most cited platforms, which were Instagram® (20%) and Facebook® (20%). Boys (23%) were more likely than girls (18%) to have been harmed on Facebook.

Consistent with prior research,[55,56] the list of apps and platforms in Figure 5 makes clear that teens are not only harmed in obscure corners of the internet: they are victimized on popular social media, gaming, and private messaging apps and platforms.

2 in 5 teen victims were sexually victimized on Snapchat

At least 2x more teens were sexually victimized on Snapchat than on any other platform

Figure 5. Percentage of teens victimized on each app and platform

Q5. On which apps or platforms did the online experiences you mentioned happen? Choose all that apply.

Snapchat®	39%	X™ (formerly Twitter)	3%
Instagram®	20%	Google Hangouts®, Meet®, or Chat®	3%
Facebook®	20%	Telegram®	3%
TikTok®	15%	Twitch®	3%
Discord®	14%	Reddit®	2%
Messenger™ (Facebook Messenger)	10%	Pinterest®	2%
WhatsApp®	9%	Chatroulette™	1%
Roblox®	8%	Kik®	1%
Call of Duty®	7%	Signal™	1%
Fortnite®	7%	Tumblr®	1%
YouTube®	6%	Wizz™	1%
iMessage® or FaceTime®	5%	Another app or platform	4%
Minecraft®	4%	Don't know	3%
Grand Theft Auto®	3%	Prefer not to answer	2%

Online environments

Some of the apps and platforms in Figure 5 are private environments, such as the private messaging apps Facebook Messenger™, WhatsApp®, and iMessage®. Most other apps and platforms offer not only private communication environments, such as direct messages, private livestreams, group chats, or private groups, but also public communication environments such as posts, feeds, forums, comments, and games that anyone can join or watch; Snapchat, Facebook, and Instagram are examples of these.

Overwhelmingly, teens had been sexually victimized in private communication spaces: nearly 9 in 10 teen victims (86%) experienced online sexual violence in private communication environments (Figure 6). Older teens were even more likely to have been victimized in these spaces (89% of 15- to 17-year-olds vs. 82% of 13- to 14-year-olds).

Nearly 9 in 10 teen victims were harmed in private messaging environments

Just under 1 in 5 teen victims (19%) were harmed in public communication spaces.

These findings mirror the information captured in thousands of reports processed by Cybertip.ca over the last several years: most online sexual victimization of children is initiated or facilitated in the context of private communications.[57]

Cybertip.ca is Canada's national tipline for reporting online sexual exploitation and abuse of children. Operated by C3P, it receives and processes reports from the public regarding illegal content like child sexual abuse images and videos, child trafficking, online luring, and non-consensual distribution of intimate images. Relevant information is then referred to law enforcement and child welfare agencies for investigation and action.

cybertip!ca®

Figure 6. Percentage of teens victimized in private and/or public functions/apps/platforms

Q6. Again thinking about the online experiences you mentioned, where in the apps or platforms did it happen? Select all that apply.

In private, such as direct messages or group chats	76%
In private **and** in public	11%
In public, such as on posts, forums, or comments	9%
Don't know	3%
Prefer not to answer	1%

In private (NET)	**86%**
In public (NET)	**19%**

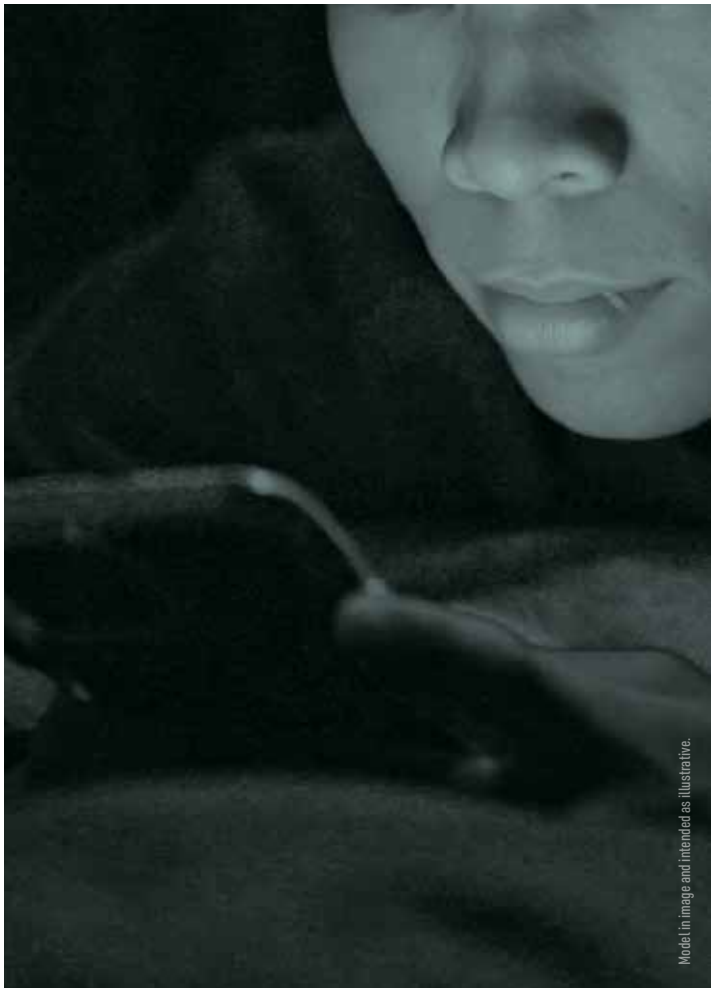
Responses to online sexual victimization

Teen victims also shared which steps they have taken, if any, following their experiences of online sexual violence. Encouragingly, most have sought at least one form of help or support at some point (Figure 7).

Over 1 in 2 teen victims (55%) have told someone they trust, such as a friend, parent, or teacher, with girls being more likely to do this than boys (59% vs. 51%). Some teen victims have reported the harm to police (8%)*** or to C3P's Cybertip.ca or NeedHelpNow.ca (4%). These latter two statistics reinforce that online sexual violence is underreported,[58] and consequently, police and tipline data only represent a small fraction of the true scale of online sexual violence experienced by Canadian teens today.

Teens have also responded to their victimization by taking action on the apps or platforms where harm occurred. Two in 5 teen victims (38%) – especially girls (43% vs. 34% of boys) – have unfollowed, blocked, removed, or muted the person(s) online (though note that not all platforms offer all of these tools). Only 1 in 5 teen victims (20%) have reported their victimization to the platform; the outcomes of those reports, as well as reasons why most of these teens have not reported to platforms, are detailed in the following sections.

Just over 1 in 5 teen victims (22%) didn't tell anyone about an experience of online sexual victimization or report it anywhere.



Model in image and intended as illustrative.

1 in 5 teen victims didn't tell anyone about their online sexual victimization or report it anywhere

*** Not all forms of online sexual victimization represented in our survey would constitute criminal acts in Canada.

Figure 7. Percentage of teen victims who took steps in response to their online sexual victimization

Q7. Thinking again about the online experiences you mentioned, did you do any of these things? Select all that apply.

I told someone I trust (for example a friend, parent or guardian, teacher)	55%
I unfollowed, blocked, removed, or muted the person(s) online	38%
I didn't tell anyone or report it anywhere	22%
I reported it to the apps or platforms where it happened	20%
I reported it to police	8%
I reported it to Cybertip.ca or NeedHelpNow.ca	4%
None of these	5%
Don't know	1%
Prefer not to answer	1%

Outcomes of reports to apps and platforms


Model in image and intended as illustrative.

Resolution

Although often limited and lacking cross-industry uniformity,[59,60,61,62] many apps and platforms offer ways for users to report certain types of issues experienced on their service.

As noted earlier, 20% (n=275) of the teen victims surveyed have reported their victimization to the apps or platforms where it occurred. Together, they had 514 experiences reporting to platforms (Figure 8). In half of these experiences (53%), the problems stopped after the teen victim reported it to the platform, which could represent effective platform intervention, such as permanently banning an offender, as well as situations wherein the victimization had already ended when the teen made the report. In over a third of reporting experiences (38%), reporting to the platform did not end all sexual victimization teens were experiencing on those platforms.

Figure 8. Apps' and platforms' resolution of teen victims' reports

Among 275 teen victims' 514 reporting experiences to apps or platforms

Q8. Did you report the problem(s) to [platforms selected in Q5]?

Q8b. [For each platform reported to as per Q8:] What happened after you reported the problem(s)?

The problem(s) stopped	53%
The problem(s) didn't stop	21%
Sometimes the problem(s) stopped	17%
Don't know	7%
Prefer not to answer	2%

Nude or sexual image removal

There were 135 teen victims who asked an app or platform to remove a nude or sexual image of them. Removing these images quickly is crucial to curb the further distribution of the image and prevent further victimization: the sooner an image is removed, the less opportunity there is for other users to view the images, make abusive comments about them, save copies, or share the images on other platforms. For these reasons, several jurisdictions have either adopted or proposed legislation that requires online services to remove nude or sexual images of children within 24 to 48 hours from the time they are made aware of their presence on their services.[63,64,65,66]

Of teen victims who reported a nude or sexual image of them to an app or platform, 2 in 3 waited over a day for it to be removed

Teen victims shared the longest amount of time they've had to wait for an app or platform to remove a nude or sexual image of them after reporting it to the online service (Figure 9). For 1 in 4 of these teen victims, their longest wait was up to one day (25%). Unfortunately, most others have had to wait much longer: 1 to 6 days for 2 in 5 teen victims (40%), between a week and a month for over 1 in 10 (12%), and more than a month for nearly 1 in 10 victims (8%). At the time of the survey, 1 in 20 (5%) of these teen victims were still waiting for images to be removed.

Figure 9. Longest wait time for an app or platform to remove teen victims' reported nude or sexual image

Among teen victims who've reported a nude or sexual image of themselves to a platform (n=135)

Q10. When you've made a report to an app or platform, was it ever to ask them to remove a nude or sexual image of you? If so, what's the longest you've had to wait for the app or platform to remove a nude or sexual image of you?

Less than one day	25%
More than one day (NET)	**67%**
One to six days	40%
One week to a month	12%
More than a month	8%
It hasn't been removed	5%

Model in image and intended as illustrative.

Not reporting to apps and platforms

There were 1,004 teen victims who had not reported their online sexual victimization to an app or platform where they'd experienced the harm. When asked why they hadn't reported, the most cited reason was that they didn't think the app or platform would help (43%; Figure 10); this was more common among girls than boys (48% vs. 37%). Other top reasons for not reporting were not knowing how (30%) or not wanting anyone to know they made a report (21%), perhaps out of fear of offender retaliation.[67] Even if reports are anonymous, an offender might be able to deduce that the victim made a report based on the timing and nature of the platform's response (e.g., banning the offending user for sharing nude images of children) – and an offender may have explicitly warned the victim of consequences if they tell anyone what happened.[68]

Some teen victims didn't make a report because they worried the platform would ban them (13%; which, for example, could be the case if they had violated a platform's rules in sharing nude images of themselves) or because the platform didn't have a place to report the harm (9%).

Figure 10. Reasons for not reporting online sexual victimization to the app or platform

Among teen victims who've never reported to a platform (n=1,004)

Q9: You told us you didn't report the online experiences to the app or platform. Which of these describe why you haven't reported to the app or platform? Select all that apply.

I didn't think the app or platform would help	43%
I didn't know how to report it	30%
I didn't want anyone to know I made the report	21%
I worried they'd ban me	13%
There wasn't anywhere to report it	9%
Something else	9%
Don't know	12%
Prefer not to answer	3%

Awareness of others' experiences of online sexual violence

In addition to having experienced online sexual violence themselves, over 2 in 3 teen victims (69%) personally knew someone who had experienced at least one of the forms of online sexual violence discussed in this survey (Figure 11). This awareness was more common among girls than boys (74% vs. 63%).

2 in 3 teen victims know someone else who has experienced online sexual violence

Figure 11. Percentage of teen victims who know other victims of online sexual violence

Q10b. And do you know someone personally (not including yourself) who has had any of these things happen to them online in a way they didn't want or without their permission?

Yes to at least one	69%
No, don't know, or prefer not to answer to all	31%

Opinions on policy solutions

Overwhelmingly, teens with lived experiences of online harms support regulation of the technology industry and think there are many measures apps and platforms could take to help prevent other teens from being sexually victimized online.

9 in 10 teen victims think Canada should legally force apps and platforms to prevent harm

Government regulation

Increasingly, online service providers are being legally required to meet safety standards designed to protect their users, especially children.[69,70,71] Canada is still without such measures, and teen victims of online sexual violence want this to change: over 9 in 10 teen victims (93%) agreed that Canada should have laws to force apps and platforms to prevent harm, with 3 in 4 (74%) expressing strong agreement (Figure 12). Of note, their support for online regulation in Canada appears to be stronger than adults' support.[72,73]

Figure 12. Percentage of teen victims who agree with government regulation

Q10c: How much do you agree or disagree with the following: In Canada, there should be laws that force apps and platforms to prevent harm.

Agree (NET)	**93%**
Strongly agree	74%
Somewhat agree	19%
Neither agree nor disagree	4%
Somewhat disagree	1%
Strongly disagree	1%
Don't know	1%
Prefer not to answer	0%

App and platform measures

Whether voluntarily or mandated by legislation, online apps and platforms can take steps to make their services safer. A large majority of teen victims felt there were many measures that would help prevent other teens from being sexually victimized online (Figure 13).

A number of these measures fall into the category of "safety by design," that is, proactive ways apps and platforms can anticipate harms, and design their services to minimize the chances of their platforms being used to facilitate the victimization of its users; these were rated as helpful by at least 85% of teen victims. The safety by design measure teen victims thought would be most helpful is to prevent teens from being contacted by someone they've blocked or reported (92%); girls were more likely to see this as helpful than boys (94% vs. 90%). Prior research has shown that blocking or reporting users is often ineffective at stopping harms: half of the children have been recontacted by problematic users they'd blocked or reported, either from a new account on the same platform or a new account on a different platform.[74] In the current study, teen victims also thought it would be helpful if apps and platforms were safely designed to: prevent nude or sexual images of teens from being shared without their permission (91%); prevent people from making accounts that pretend to be someone else (90%); and prevent strangers from connecting with or messaging teens (85%).

Teen victims saw promise in well-designed tools for reporting issues or abuse. Roughly 9 in 10 thought that if apps and platforms would do the following, it would be helpful in reducing online sexual violence against teens: have easy ways to report problems (92%; 94% of girls vs. 90% of boys); quickly help teens who report a problem (91%; 93% of girls vs. 88% of boys); and have a real person help teens who report a problem (87%).

Approximately 3 in 4 teen victims (74%) thought having ways for parents/guardians to monitor teens' online activities would help prevent the online sexual victimization of teens. This was the measure teen victims saw as least helpful. One possible explanation is that they do not want parental oversight of their accounts. It is also possible that those who think parental monitoring tools wouldn't be helpful are speaking from experience: in operating Cybertip.ca and NeedHelpNow.ca, we often hear of cases where, even when parents have used monitoring tools, children and teens were sexually victimized online. In practice, these tools typically do not address many of the known risks to children, including adult strangers' ability to connect with young users.[75,76]

Figure 13. Percentage of teen victims who think app and platform safety measures would help prevent online sexual victimization of teens

Q11. Still thinking about things that can happen to people online, like someone talking to them in a sexual way they don't want, or sharing nude or sexual images of them without their permission: How helpful or unhelpful do you think each idea would be at preventing these things from happening to teens? Making sure apps and platforms...

	Helpful (NET)	Very helpful	Some-what helpful	Neither helpful nor unhelpful	Some-what unhelpful	Very unhelpful	Don't know	Prefer not to answer
Stop teens from being contacted by people they've blocked or reported	**92%**	72%	20%	4%	2%	1%	1%	0%
Have easy ways to report problems to them	**92%**	67%	25%	4%	2%	1%	1%	0%
Prevent nude or sexual images of teens from being shared without their permission	**91%**	72%	19%	4%	2%	1%	1%	0%
Quickly help teens who report a problem to them	**91%**	69%	22%	5%	2%	1%	2%	0%
Prevent people from making accounts that pretend to be someone else	**90%**	69%	21%	6%	2%	1%	1%	0%
Have a real person help teens who report a problem to them	**87%**	59%	28%	6%	2%	1%	3%	0%
Prevent strangers from connecting with or messaging teens	**85%**	62%	22%	8%	3%	2%	2%	0%
Have ways for parents/ guardians to monitor teens' online activities	**74%**	44%	30%	13%	6%	4%	2%	1%

KEY FINDINGS AND RECOMMENDATIONS

This report details the experiences of Canadian teens who have been victims of online sexual violence. Both adults and their peers have subjected them to unwanted sexual talk and a range of image-based abuses, such as sending them unsolicited nude images or threatening to share their nude images with others. These forms of online harm are in many cases also manifestations of gender-based violence, reflecting patterns of power and control that disproportionately affected girls; an exception to this pattern is that, perhaps due in part to the rise of financial sextortion, boys were more likely to have had someone non-consensually share their nude or sexual images. Most concerningly, teens experienced these harms on the most popular social media, gaming, and private messaging apps and platforms in Canada.

Model in image and intended as illustrative.

The vast majority of teen victims did not report the harms they experienced to these apps and platforms, most often because they did not think the platforms would help, and sometimes because it wasn't clear how to make a report. Unfortunately, even when these teens did report their victimization to an online service, in many cases the problems did not stop and their nude or sexual images were not removed quickly.

These findings reinforce that apps and platforms can and must do more to prevent teens from being sexually victimized within the digital environments they create, and must also better respond when victimization does occur. In fact, most teen victims thought that in Canada, we should have laws that force apps and platforms to prevent harm; they also expressed strong support for a variety of potential policy solutions.

Accordingly, our findings point to policy recommendations that can help shape the structure of an eventual online safety regime in Canada. These recommendations are informed by and grounded in the perspectives and experiences of teens who have been sexually victimized online.

We encourage online service providers to voluntarily adopt the technical components of these recommendations; however, as careful observers of the repeated failure to prioritize child safety by the technology industry,[77] this guidance is intended for government and policy makers who have the ability to enact and enforce an online safety regime.

Nearly 9 in 10 teen victims (86%) were harmed in private messaging environments.

Recommendation: Ensure online safety regimes impose appropriate duties of care and obligations onto private communication services and functions.

If the guiding principles of an online safety regime are to safeguard children and prevent harm, then it must devote significant attention to the outsized role private communication services and functions play in the facilitation of online sexual victimization of teens in Canada.

Teen victims in this study overwhelmingly experienced online sexual violence in private digital environments, with nearly 9 in 10 (86%) saying they were harmed in the context of private messaging, such as direct messages or closed group chats. This finding also closely mirrors the trends observed in thousands of reports reviewed by our organization through the operation of Cybertip.ca.[78]

Consider that for some online services, their sole function is private communication (e.g., WhatsApp, Signal™, iMessage), whereas other services offer private communication functions alongside public communication functions (e.g., Snapchat, Instagram, Discord®). Online safety regimes must scope in both private communication services and functions. Some examples of harm reduction strategies include requiring private communication services and functions:

- Ensure their users can easily report abuse from other users;
- Establish high levels of safety and privacy settings by default, rather than privileging settings designed to maximize engagement;
- Make use of signal data (e.g., accounts that have been blocked or reported by many users) to keep bad actors off of their platforms;
- Provide users with safety prompts that indicate that an account communicating with them was, for example, recently created or has been the subject of many complaints from other users; and
- Provide settings that allow for geofencing a user's communication network to a specified geographic region.

Many more measures exist – for specifics, see our previous statement on this issue.[79]

Harm occurred on many popular apps and platforms, with 2 in 5 teen victims (39%) sexually victimized on Snapchat.

Recommendation: Online safety regimes must scope in and apply to a broad range of platforms, with graduated obligations based on a given service's anticipated or known risk factors.

Although online sexual violence occurred on popular social media services, these were not the only online spaces where harm happened. Gaming platforms, private messaging apps, and small, lesser-known social media services were also spaces where teens experienced sexual violence (see Figure 5).

Beyond this report, other research has shown that offenders commonly host and distribute CSAEM on fringe web forums and file hosting services.[80,81,82]

These findings emphasize the importance of establishing basic safety duties and responsibilities for all online services, particularly those that allow user-to-user interactions or user-generated content. From there, other factors such as risk levels, the nature of the service, the likelihood of having child users, and more can help dictate what further regulatory obligations are appropriate.

Lastly, given the frequency with which Snapchat has been cited by victimized teens in this study, we believe it's worth highlighting that the company has recently argued that it ought to be exempt from Australia's new law – the *Online Safety Amendment (Social Media Minimum Age) Act 2024*[83] – which established a minimum age of 16 for use of certain social media platforms. The company's position was that its primary purpose is private messaging and therefore should not qualify as a social media platform.[84] This example underscores the importance of having online safety regimes that are appropriately broad in their scope and apply graduated obligations based on risk.

Of teen victims who reported a nude or sexual image of them to an app or platform, 2 in 3 (67%) waited over a day for it to be removed. Teen victims also thought apps and platforms should prevent the non-consensual distribution of teens' nude and sexual images.

Recommendation: Online safety regimes must set clear expectations for online service providers to proactively detect, and quickly review and remove, reported nude or sexual images of children.


Models in image and intended as illustrative.

Most teen victims experienced at least one form of image-based sexual abuse, including having a nude or sexual image of them distributed online without their permission. When they took it upon themselves to ask platforms to remove the imagery, most had to wait anywhere from one day to months. Though we did not ask survey respondents what happened in the meantime, other research indicates that keeping this imagery online poses risks for further harm.[85,86,87]

To prevent further image distribution and victimization, an online safety regime in Canada should require that services remove nude and sexual images of children within 24 hours of learning it is on their systems – as was proposed in Bill C-63, the *Online Harms Act*.[88] An online safety regime should also establish enforcement actions to respond to services that fail to remove this imagery in 24 hours. This would be keeping with legislation in other jurisdictions, such as Australia.[89]

Teen victims also emphasized the importance of preventing the distribution of nude and sexual imagery. Nearly all thought it would be helpful if apps and platforms were designed to prevent nude or sexual images of teens from being shared without their permission. A Canadian online safety regime should require that online services adopt proactive detection tools, such as cryptographic and perceptual hash matching technologies, which can block the upload and further distribution of known CSAEM. Many online services currently make use of these technologies;[90] however, widespread adoption is needed along with standards to surround its use.

At least 1 in 4 teen victims (25%) experienced online sexual violence involving an adult offender.

> **Recommendation: Online safety regimes must require online service providers prevent potentially unsafe online interactions between adults and children. Updates to Canada's *Criminal Code* to address luring tactics should also be considered.**

In the absence of an online safety regime in Canada, many apps and platforms have no restrictions in place to prevent adult strangers from messaging, exchanging images with, and video calling children. As such, inappropriate unsupervised interactions between children and adults are commonplace across many digital services. These adults can also pose as children.

These adults can and do cause harm to children. Indeed, 1 in 4 teen victims (25%) said they'd been victimized by an adult online, with others unsure; it's also possible that others had been victimized by an adult who posed as a child or teen. Although less prevalent than peer victimization, which is also concerning and the other recommendations in this report would help address, we focus here on victimization by adult offenders as its prevention involves a unique policy approach.

An online safety regime should require online services to employ appropriate age gating mechanisms. Online services could, for example, be required to use effective age assurance technologies or verify identities when onboarding new users, to help prevent inappropriate interactions between adults and child users.

Mandated age assurance or even user verification obligations could also prevent the creation of fake personas and accounts;[91] a common tactic used by offenders to connect with and harm children online.[92] Indeed, nearly all teen victims thought that preventing people from making accounts that pretend to be someone else would help prevent online sexual violence.

To complement these requirements of online services, Parliament could also consider updates to the *Criminal Code*'s luring offence. For example, it could introduce a non-exhaustive list of factors for judges to consider in their analysis of the purpose behind the communications (similar to section 153(1.2) of the *Criminal Code*). One of the factors could be if the accused misrepresented their age, and especially if they posed as being under 18.

Another approach could be to create a new *Criminal Code* offence to deal with harmful age misrepresentations. For example, Australia has an offence which can include situations of "a person misrepresenting their age online as part of a plan to cause harm to another person under 16 years of age."[93]

Lastly, the same policies that would enable age gating of users also serve to support and even enable several other core online safety objectives. As an example, online safety regimes have imposed child-specific duties of care onto online service providers.[94,95,96] However, without a corresponding obligation to also establish the age of its users, it's unclear how an online service would fulfil these duties.

Over 1 in 2 teen victims (52%) had been sent an unwanted nude or sexual image, and 1 in 6 (17%) had someone make a "fake" nude or sexual image of them.

Recommendation: Amend the *Criminal Code* to address the creation and sharing of nude and sexual deepfakes, and consider whether existing *Criminal Code* offences adequately address cyberflashing.

Although some of the harms described in this study currently meet a criminal threshold in Canada, others do not.

The creation and distribution of deepfake nude imagery is a form of online sexual violence that is not expressly addressed in Canadian law. Many teen victims had someone make a "fake" nude or sexual image of them. Although we did not ask how the imagery was created, it's likely that at least some was made using widely available AI "nudify" or "undress" apps and platforms.[97] While the *Criminal Code* definition of CSAEM is broad enough to capture CSAEM created with AI tools, the non-consensual distribution of intimate images offence is not broad enough. Canadian law could prohibit the advertisement and availability of such tools, ensure this imagery is criminalized, and set expectations for the expeditious removal of this imagery. Measures to address AI-generated nude imagery have been adopted in the U.S.[98] and were recently announced by the Australian government.[99]

Another harm in need of consideration is cyberflashing, which impacted over half of the teen victims in this study. Some of these incidents could be considered criminal, but depending on the circumstances, it may not always be clear if or which existing *Criminal Code* offences might apply. The U.K.,[100] for instance, criminalized the act of intentionally sending images of genitals that are unsolicited and sent to cause distress to the recipient or for the purpose of sexual gratification where the sender is reckless to if the recipient will be distressed. Such a legislation could also include images that are real or AI-generated, images of the sender's genitals or another person's genitals, and incidents impacting victims of all ages.

Model in image and intended as illustrative.

Over 9 in 10 teen victims (93%) think Canada should legally force apps and platforms to prevent harm online. Most also thought safety measures would help.

Recommendation: An online safety regime must require that apps and platforms be designed with safety in mind and provide children with enhanced protections.

As those with lived experience, teen victims have unique and important insights into protecting children online. They were highly supportive of laws to force apps and platforms to prevent harm online, as well as several safety by design measures, which refer to proactive ways apps and platforms can make changes that would help minimize the victimization of users on their services, for example, changes to the layout, functions, prompts, and settings options. In addition to the measures discussed earlier, roughly 9 in 10 teen victims thought it would be helpful to prevent teens from being recontacted by someone they've blocked or reported (92%), or to prevent strangers from connecting with or messaging teens (85%).


Model in image and intended as illustrative.

Approximately 9 in 10 teen victims also thought that well-designed, teen-specific tools for reporting issues or abuse would help reduce online sexual violence against teens, including having easy ways to report problems (92%) that are responded to quickly (91%) and by real people (87%).

Many of these types of measures have been mandated by online safety legislation elsewhere. For example, in both Australia and the U.K., online services are required to have responsive and easy to use reporting tools.[101,102] The U.K. also adopted the U.K. Children's Code (officially known as the "Age Appropriate Design Code") in 2020,[103] which requires online services to be designed in the best interests of children. This Code consists of 15 standards that ensure built-in protections for children exist, including strong privacy settings by default, minimized data collection, transparent parental controls, and stopping inappropriate nudging techniques.

Finally, teen victims also weighed in on the helpfulness of parental monitoring to protect teens from online sexual violence. This measure was seen as helpful by 3 in 4 teen victims (74%), making it the lowest rated measure, but ultimately still seen as helpful by most. As such, parental monitoring, as well as parental controls more broadly, should be viewed as one of many measures online services ought to use to reduce risk and harm to children online. They should not, however, be viewed as a stand-alone solution, as industry data show that fewer than 1% of child accounts on Discord and Snapchat have parental controls enabled.[104] This may reflect overly complex control settings or even a view from parents that the controls made available to them are ineffective.

CONCLUSION

Online sexual violence against teens in Canada is pervasive, occurring largely on private communications on popular platforms used by millions of Canadians. The experiences shared by nearly 1,300 teen victims reveal systemic failures: platforms often do not prevent harm, and when victimization occurs, responses are slow and inadequate. These harms are not inevitable – they reflect design choices and regulatory gaps. Teen victims overwhelmingly support strong laws and safety by design measures to protect children online, emphasizing that voluntary industry action has proven insufficient.

A comprehensive online safety regime for Canada must impose enforceable duties of care, mandate rapid removal of abusive and harmful content, and prevent unsafe interactions between adults and children. It should also address emerging threats like AI-generated deepfake nudes through clear legal prohibitions. Protecting children online is not only a matter of safety, but also a matter of upholding their rights to privacy and freedom from exploitation. Canada has an opportunity to learn from these victims as well as the experiences of other countries with existing online safety regimes and improve on them.

Model in image and intended as illustrative

APPENDIX A: SURVEY METHODOLOGY

In March 2025, C3P created a questionnaire and commissioned Leger to administer it as a nationally representative online survey of 13- to 17-year-olds who live in Canada and had experienced at least one form of online sexual violence. Parents and guardians gave permission for their child to participate.

Leger sent study invitations to parents on their research panel, LEO. After parents and their children provided informed consent, the child completed seven screening questions to determine whether they had experienced any forms of online sexual violence. Children who had not experienced at least one form were screened out of the survey.

The screening questions instructed teens to focus on experiences that had happened without their permission or in ways they didn't want. We chose this focus because we wanted to assess harms that could be perpetrated by adults or children, and unwanted experiences that teens may be motivated to respond to. Consequently, our data do not reflect all forms of online sexual abuse and exploitation, such as experiences that teens may have expressed permission for but cannot legally consent to under Canadian law.

The final sample consisted of 1,279 13- to-17-year-olds who had experienced at least one form of online sexual violence. Data was collected between April 29 and May 20, 2025. Although no margin of error can be associated with a non-probability sample such as this, for comparison, a probability sample of n=1,279 respondents yields a margin of error no greater than ±2.7% (19 times out of 20). The data is weighted based on the 2021 Canadian census. Leger conducted all data analyses.

APPENDIX B: SCREENER QUESTIONS

Next, we have some questions about things that may have happened to you online. "Online" includes anything that happens when using a computer, phone, tablet, or gaming device.

Please remember:

- Your answers are completely anonymous. No one will know how you answered – not your parents, not the people running the survey, not anyone else.
- There are no right or wrong answers. The only "right" answers are the ones that are true for you.

You can skip any question or stop the survey at any time.

ScreenQ1. Has anyone ever done this to you online, in a way that you didn't want? Reminder: online includes anything that happens when using a computer, phone, tablet, or gaming device.

- Tried to get you to talk about sex, or said sexual things to you? For example, made sexual comments about your body to you.
- Sent you a nude or sexual photo or video? For example, a photo of genitals, or a video of people having sex.

ScreenQ2. These next few questions are about "nude or sexual images". By this we mean photos or videos of you that are nude, partially nude, sexual, or sexually abusive. [Programming note: This definition should appear as a hover definition for all instances of "nude or sexual images" in the survey]

Has anyone ever done this to you online, without your permission?

- Made a copy of a real nude or sexual image of you by recording a live video or taking a screenshot?
- Made a fake nude or sexual image of you by editing or changing an image of you?

ScreenQ3. Again, think about nude or sexual images. Has anyone ever done this to you online?

- Pressured you to send them nude or sexual images of you (real or fake)?
- Threatened to post, send, or show others nude or sexual images of you (real or fake)?
- Posted, sent, or showed others nude or sexual images of you (real or fake), without your permission?

REFERENCES

1 Savage, L. (2024). Online child sexual exploitation: A statistical profile of police-reported incidents in Canada, 2014 to 2022. *Statistics Canada.* https://www150.statcan.gc.ca/n1/pub/85-002-x/2024001/article/00003-eng.htm

2 Royal Canadian Mounted Police. (2025). *Protect STEEL leads to the arrest of 106 online child sex offenders.* https://rcmp.ca/en/news/2025/03/project-steel-leads-arrest-106-online-child-sex-offenders

3 Pedersen, K., & Wesley, A. (2023, November 2). Social media apps that facilitate sextortion blamed for not doing enough to prevent it. *CBC News.* https://www.cbc.ca/news/canada/sextortion-social-media-apps-victims-1.7014262

4 Canadian Press. (2024, February 3). AI brings deepfake pornography to the masses, as Canadian laws play catch-up. *CTV News.* https://www.ctvnews.ca/vancouver/article/ai-brings-deepfake-pornography-to-the-masses-as-canadian-laws-play-catch-up/

5 Nau, C., Reyes, E., Dietzel, C., Dodge, A., Dunn, S., & Mendes, K. (2025). Canadian youth and technology-facilitated sexual violence: Findings from a 2024 general population survey among Canadian teens. *DIY: Digital Safety.* https://doi.org/10.5683/SP3/HBJOCW

6 Chauviré-Geib, K., Gerke, J., Haag, A. C., Sachser, C., Finkelhor, D., Rassenhofer, M., & Fegert, J. M. (2025). The increase in online child sexual solicitation and abuse: Indicator 16.2.3 of the UN Sustainable Development Goals (SDG) documents a hidden and growing pandemic. Population-based surveys fail to capture the full picture. *Child Abuse & Neglect, 164,* 107452. https://doi.org/10.1016/j.chiabu.2025.107452

7 Walsh, K., Mathews, B., Parvin, K., Smith, R., Burton, M., Nicholas, M., Napier, S., Cubitt, T., Erskine, H., Thomas, H. J., Finkelhor, D., Higgins, D. J., Scott, J. G., Flynn, A., Noll, J., Malacova, E., Le, H., & Tran, N. (2025). Prevalence and characteristics of online child sexual victimization: Findings from the Australian Child Maltreatment Study. *Child Abuse & Neglect, 160,* 107186. https://doi.org/10.1016/j.chiabu.2024.107186

8 Government of Canada. (2023). Child sexual exploitation on the internet. *Public Safety Canada.* https://www.publicsafety.gc.ca/cnt/cntrng-crm/chld-sxl-xplttn-ntrnt/index-en.aspx

9 International Centre for Missing & Exploited Children. (2025). Global experts call for new approach to protect children from 'pandemic' of sexual exploitation and abuse. https://www.icmec.org/press/global-experts-call-for-new-approach-to-protect-children-from-pandemic-of-sexual-exploitation-and-abuse/

10 Fry, D. & Lambourne, Z. (2025). Public health and child sexual exploitation and abuse. *Childlight.* https://www.childlight.org/uploads/publications/Public-health-paper-survey-June-2025.pdf

11 World Health Organization. (2022). *What works to prevent online violence against children?* https://iris.who.int/server/api/core/bitstreams/0ce56bbf-4535-405e-9bd6-e143f64ae2ba/content

12 Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse & Neglect, 80,* 238–248.

13 Schmidt, F., Varese, F., & Bucci, S. (2023). Understanding the prolonged impact of online sexual abuse occurring in childhood. *Frontiers in Psychology, 14,* 1281996. https://doi.org/10.3389/fpsyg.2023.1281996

14 Colburn, D., Mitchell, K. J., Gewirtz-Meydan, A., Finkelhor, D., Turner, H. A., & O'Brien, J. E. (2025). Life impact following childhood Image-Based Sexual Abuse victimization among a sample of young adults. *Child Abuse & Neglect, 167,* 107584. https://doi.org/10.1016/j.chiabu.2025.107584

15 Mitchell, K. J., Colburn, D., Finkelhor, D., Gewirtz-Meydan, A., Turner, H. A., & Jones, L. M. (2025). Links between image-based sexual abuse and mental health in childhood among young adult social media users. *Child Abuse & Neglect, 164,* 107471. https://doi.org/10.1016/j.chiabu.2025.107471

16 Hanson, E. (2016). The impact of online sexual abuse on children and young people. In J. Brown (Ed.), *Online risk to children: Impact, protection and prevention* (1st ed., pp 97–122). Wiley Blackwell. https://doi.org/10.1002/9781118977545.CH6

[17] Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse & Neglect, 80,* 238–248.

[18] Canadian Centre for Child Protection. (2024). *Survivors' survey: Full report 2017.* https://protectchildren.ca/pdfs/C3P_SurvivorsSurveyFullReport2017.pdf

[19] Finkelhor, D., Turner, H., Colburn, D., & Mitchell, K. J. (2025). Persisting concerns about image exposure among survivors of image-based sexual exploitation and abuse in childhood. *Psychological Trauma: Theory, Research, Practice and Policy, 17*(Suppl 1), S88–S93. https://doi.org/10.1037/tra0001815

[20] Canadian Centre for Child Protection. (2024). *Experiences of child sexual abuse material survivors: How technology companies' inaction leads to fear, stalking, and harassment.* https://protectchildren.ca/pdfs/C3P_ExperiencesOfCSAMSurvivors_en.pdf

[21] Ringrose, J., Regehr, K., & Milne, B. (2021). *Understanding and combatting youth experiences of image-based sexual harassment and abuse.* https://www.ascl.org.uk/ASCL/media/ASCL/Our%20view/Campaigns/Understanding-and-combatting-youth-experiences-of-image-based-sexual-harassment-and-abuse-full-report.pdf

[22] Office of the High Commissioner for Human Rights. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment.* United Nations. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[23] Online Safety Act, 2021, no. 76. https://www.legislation.gov.au/C2021A00076/latest/text

[24] Online Safety Act 2023, c.50. https://www.legislation.gov.uk/ukpga/2023/50/enacted

[25] Regulation 2022/2065. Regulation (EU) No 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

[26] 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, 1st session, 44th Parliament. 2024. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading

[27] Canadian Centre for Child Protection. (2024). *Exclusion of private messaging features from proposed Online Harms Act leaves a substantial threat to children unaddressed.* https://www.protectchildren.ca/en/press-and-media/blog/2024/online-harms-bill-messaging

[28] Canadian Centre for Child Protection. (2024). *Legislated age assurance requirement needed to ensure regulated services fulfil their child specific duties under proposed Online Harms Act.* https://www.protectchildren.ca/en/press-and-media/blog/2024/online-harms-bill-age-verification

[29] Liberal Party of Canada. (2025). *Secure*. https://liberal.ca/cstrong/secure/

[30] Conservative Party of Canada. (2025). *Change: For an affordable life. For safe streets. For Canada First.* https://canada-first-for-a-change.s3.us-west-2.amazonaws.com/20250418_CPCPlatform_8-5x11_EN_R1-pages.pdf

[31] New Democratic Party. (2025). *Made for people. Built for Canada.* https://www.ndp.ca/campaign-commitments

[32] Bloc Québécois. (2025). *Choisir le Québec: Plateforme Politique 2025.* https://www.blocquebecois.org/wp-content/uploads/2025/03/blocqcplateforme-2025web.pdf

[33] Turner, H. A., Finkelhor, D., & Colburn, D. (2023). Predictors of online child sexual abuse in a U.S. national sample. *Journal of Interpersonal Violence, 38*(11-12), 7780-7803. https://doi.org/10.1177/08862605221149090

[34] Turner, H. A., Finkelhor, D., Mitchell, K., & Colburn, D. (2024). Prevalence of technology-facilitated abuse among sexual and gender minority youths. *JAMA Network Open, 7*(2), e2354485. https://doi.org/10.1001/jamanetworkopen.2023.54485

[35] Canadian Centre for Child Protection. (2025). *Online harms: AI and deepfakes.* https://cybertip.ca/en/online-harms/deepfakes/

[36] Thorn. (2025). *Deepfake nudes & young people: Navigating a new frontier in technology-facilitated nonconsensual sexual abuse and exploitation.* https://info.thorn.org/hubfs/Research/Thorn_DeepfakeNudes&YoungPeople_Mar2025.pdf

[37] *Online Safety Act 2021,* section 187. https://www.legislation.gov.uk/ukpga/2023/50

[38] Thorn (2025). *Sexual extortion & young people: Navigating threats in digital environments.* https://info.thorn.org/hubfs/Research/Thorn_SexualExtortionandYoungPeople_June2025.pdf

[39] Canadian Centre for Child Protection. (2025). *Online harms: Sextortion.* https://cybertip.ca/en/online-harms/sextortion/

[40] Thorn (2017). *Sextortion: Summary findings from a 2017 survey of 2,097 survivors.* https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf

[41] Thorn (2017). *Sextortion: Summary findings from a 2017 survey of 2,097 survivors.* https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf

[42] Finkelhor, D., Turner, H., & Colburn, D. (2022). Prevalence of online sexual offenses against children in the US. *JAMA Network Open, 5*(10), e2234471. https://doi.org/10.1001/jamanetworkopen.2022.34471

[43] City of Calgary. (2022). *Police issue warning of online extortion scam targeting young boys.* https://newsroom.calgary.ca/police-issue-warning-of-online-extortion-scam-targeting-young-boys/

[44] Gibson, C. (2022, May 17). Red Deer RCMP issue warning about increase in sextortion reports. *Global News.* https://globalnews.ca/news/8841770/red-deer-rcmp-sextortion-warning/

[45] Canadian Press. (2022, June 9). Ontario police warn public of online sextortion scams circulating. *CTV News.* https://www.ctvnews.ca/toronto/article/ontario-police-warn-public-of-online-sextortion-scams-circulating/

[46] Derksen, D., & Klippenstein, T. (2022, June 6). Pembina Valley RCMP raise awareness of sextortion scams. *Pembina Valley Online.* https://www.pembinavalleyonline.com/articles/pembina-valley-rcmp-raise-awareness-of-sextortion-scams

[47] Canadian Centre for Child Protection. (2022). *Boys aggressively targeted on Instagram and Snapchat, analysis of Cybertip.ca data shows.* https://cybertip.ca/en/campaigns-and-media/news-releases/2022/sextortion-data-analysis/

[48] Siemaszko, C. (2022, May 8). 'Sextortionists' are increasingly targeting young men for money. The outcome can be deadly. *NBC News.* https://www.nbcnews.com/tech/tech-news/sextortionists-are-increasingly-targeting-young-men-money-outcome-can-rcna27281

[49] Canadian Centre for Child Protection. (2022). *An analysis of financial sextortion victim posts published on r/Sextortion.* https://protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

[50] Raffile, P., Goldenberg, A., McCann, C., & Finkelstein, J. (2024). A digital pandemic: Uncovering the role of 'Yahoo Boys' in the surge of social media-Enabled financial sextortion targeting minors. *Network Contagion Research Institute.* https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf

[51] Thorn. (2024). *Trends in financial sextortion: An investigation of sextortion reports in NCMEC CyberTipline data.* https://protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

[52] CBC. (2013). *The sextortion of Amanda Todd.* https://www.cbc.ca/player/play/video/1.2429059

[53] McMillan, D., Pederson, K., & Tomlinson, A. (2025). Sextorters are targeting young boys online – and flaunting how rich the scam is making them. *CBC*. https://www.cbc.ca/news/marketplace/sextortion-teen-boys-canada-1.7648267

[54] Savage, L. (2024). Online child sexual exploitation: A statistical profile of police-reported incidents in Canada, 2014 to 2022. *Statistics Canada.* https://www150.statcan.gc.ca/n1/pub/85-002-x/2024001/article/00003-eng.htm

[55] Thorn (2025). *Sexual extortion & young people: Navigating threats in digital environments.* https://info.thorn.org/hubfs/Research/Thorn_SexualExtortionandYoungPeople_June2025.pdf

[56] Canadian Centre for Child Protection. (2022). *An analysis of financial sextortion victim posts published on r/Sextortion.* https://protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

[57] Canadian Centre for Child Protection. (2024). *Exclusion of private messaging features from proposed Online Harms Act leaves a substantial threat to children unaddressed.* https://www.protectchildren.ca/en/press-and-media/blog/2024/online-harms-bill-messaging

[58] Savage, L. (2024). Online child sexual exploitation: A statistical profile of police-reported incidents in Canada, 2014 to 2022. *Statistics Canada.* https://www150.statcan.gc.ca/n1/pub/85-002-x/2024001/article/00003-eng.htm

[59] Canadian Centre for Child Protection. (2020). *Reviewing child sexual abuse material reporting functions on popular platforms.* https://protectchildren.ca/en/resources-research/csam-reporting-platforms/

[60] Bejar, A., Cybersecurity for Democracy, fairplay, Molly Rose Foundation, & ParentSOS. (2025). *Teen accounts, broken promises: How Instagram is failing to protect minors.* https://fairplayforkids.org/wp-content/uploads/2025/09/Teen-Accounts-Broken-Promises-How-Instagram-is-failing-to-protect-minors.pdf

[61] Canadian Centre for Child Protection. (2022). *An analysis of financial sextortion victim posts published on r/Sextortion.* https://protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

[62] unicef. (2025). *Protecting children in online gaming: Mitigating risks from organized violence.* https://www.unicef.org/innocenti/media/11836/file/UNICEF-Innocenti-Protecting-Children-Online-Gaming-Working-Paper-2025.pdf

[63] eSafety Commissioner. (2025). *Child sexual abuse online.* https://www.esafety.gov.au/key-topics/illegal-restricted-content/child-sexual-abuse-online

[64] S.146 – 119th Congress (2025-2026): TAKE IT DOWN Act (2025, May 19). https://www.congress.gov/bill/119th-congress/senate-bill/146/text

[65] S.1829 – 119th Congress (2025-2026). STOP CSAM Act of 2025 (2025, May 21). https://www.congress.gov/bill/119th-congress/senate-bill/1829/text

[66] 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, 1st session, 44th Parliament. 2024. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading

[67] Safer by Thorn. (2024). *Youth tell the truth about safety tools: Advice on how to improve these tools from actual teens.* https://safer.io/resources/youth-tell-the-truth-about-safety-tools-advice-on-how-to-improve-these-tools-from-actual-teens/

[68] Friedman-Hauser, G., & Katz, C. (2025). "She has a history of making things up": Examining the disclosure and reporting of online sexual abuse among children with disabilities. *Child Abuse & Neglect, 163.* https://doi.org/10.1016/j.chiabu.2025.107398

[69] Regulation 2022/2065. Regulation (EU) No 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

[70] Online Safety Act 2023, c.50. https://www.legislation.gov.uk/ukpga/2023/50/enacted

[71] Online Safety Act, 2021, no. 76. https://www.legislation.gov.au/C2021A00076/latest/text

[72] Leger. (2024). *Online content regulation: Survey of Canadians.* https://leger360.com/wp-content/uploads/2024/04/Leger-x-CP-_-Online_Content_Regulation-1.pdf

[73] Lockhart, A. (2025). Survey of online harms in Canada 2025. *The Dias.* https://dais.ca/wp-content/uploads/2025/05/OnlineHarms2025.pdf

[74] Thorn. (2023). *Responding to online threats: Minors' perspectives on disclosing, reporting, and blocking in 2021.* https://info.thorn.org/hubfs/Research/Thorn_ROT_Monitoring_2021.pdf

[75] Revealing Reality. (2025). *A digital playground: The real guide to Roblox.* https://think.revealingreality.co.uk/roblox-real-guide

[76] Bejar, A., Cybersecurity for Democracy, fairplay, Molly Rose Foundation, & ParentSOS. (2025). *Teen accounts, broken promises: How Instagram is failing to protect minors.* https://fairplayforkids.org/wp-content/uploads/2025/09/Teen-Accounts-Broken-Promises-How-Instagram-is-failing-to-protect-minors.pdf

[77] Canadian Centre for Child Protection. (2025). *Track record of online harm: A timeline of failures by the technology industry to protect its users.* https://protectchildren.ca/en/press-and-media/tech-timeline/

[78] Canadian Centre for Child Protection. (2024). *Exclusion of private messaging features from proposed Online Harms Act leaves a substantial threat to children unaddressed.* https://www.protectchildren.ca/en/press-and-media/blog/2024/online-harms-bill-messaging

[79] Canadian Centre for Child Protection. (2024). *Exclusion of private messaging features from proposed Online Harms Act leaves a substantial threat to children unaddressed.* https://www.protectchildren.ca/en/press-and-media/blog/2024/online-harms-bill-messaging

[80] Canadian Centre for Child Protection. (2021). *Project Arachnid: Online availability of child sexual abuse material.* https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf

[81] Barker, K., Neufeld, K. H. S., Marcoux, J., & Podprugin, O. (2025). Uncovering and overcoming offender tactics for distributing child sexual abuse and exploitation material on file hosting services [Manuscript in preparation]. Canadian Centre for Child Protection.

[82] Salter, M., & Richardson, L. (2021). The Trichan takedown: Lessons in the governance and regulation of child sexual abuse material. *Policy & Internet, 13*(3), 385-399. https://doi.org/10.1002/poi3.256

[83] Parliament of Australia. (2024). Online Safety Amendment (Social Media Minimum Age) Act 2024. https://www.legislation.gov.au/C2024A00127/asmade/text

[84] Rintoul, C. (2025, October 28). Social media ban: Snapchat argues its platform is not 'toxic' and should be exempt from under-16s ban. *The Nightly.* https://thenightly.com.au/politics/social-media-ban-snapchat-argues-its-platform-is-not-toxic-and-should-be-exempt-from-under-16s-ban-c-20495005

[85] Canadian Centre for Child Protection. (2024). *Experiences of child sexual abuse material survivors: How technology companies' inaction leads to fear, stalking, and harassment.* https://protectchildren.ca/pdfs/C3P_ExperiencesOfCSAMSurvivors_en.pdf

[86] McGlynn, C., Johnson, K., Rackley, E., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2020). 'It's torture for the soul': The harms of image-based sexual abuse. *Social & Legal Studies, 30*(4), 541-562. https://doi.org/10.1177/0964663920947791

[87] Hellevik, P. M., Haugen, L. E. A., & Överlien, C. (2025). Outcomes of image-based sexual abuse among young people: A systematic review. *Frontiers in Psychology, 16,* 1599087. https://doi.org/10.3389/FPSYG.2025.1599087/BIBTEX

[88] 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, 1st session, 44th Parliament. 2024. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading

[89] eSafety Commissioner. (2024). *Image-based abuse scheme: Regulatory guidance.* https://www.esafety.gov.au/sites/default/files/2024-02/Image-Based-Abuse-Scheme-Regulatory-Guidance-Feb2024.pdf

[90] eSafety Commissioner.(2025). A baseline for online safety transparency: The first regular report on child sexual exploitation and abuse, and sexual extortion. https://www.esafety.gov.au/sites/default/files/2025-11/BOSE-full-report-CSEA-sexual-extortion-periodic-notices-Nov2025Update.pdf?v=1762905600021

[91] eSafety Commissioner. (2024). *Tech trends issue paper: Age assurance.* https://www.esafety.gov.au/sites/default/files/2024-07/Age-Assurance-Issues-Paper-July2024_0.pdf?v=1721088000021

[92] Canadian Centre for Child Protection. (2022). *An analysis of financial sextortion victim posts published on r/Sextortion.* https://protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

[93] Criminal Code Amendment (Protecting Minors Online) Act (No. 50) 2017 (Cth). Explanatory Note. https://www.ato.gov.au/law/view/document?LocID=%22NEM%2FEM201720%2FNAT%2FATO%2F00001%22&PiT=99991231235958

[94] Ofcom. (2025). *Quick guide to Protection of Children Codes.* https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/quick-guide-to-childrens-safety-codes

[95] European Commission. (2025). *Commission publishes guidelines on the protection of minors.* https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors

[96] eSafety Commissioner. (2025). *Learn about the Online Safety Act.* https://www.esafety.gov.au/newsroom/whats-on/online-safety-act

[97] Marr, B. (2025, July 28). AI apps are undressing women without consent and it's a problem. *Forbes*. https://www.forbes.com/sites/bernardmarr/2025/07/28/ai-apps-are-undressing-women-without-consent-and-its-a-problem/

[98] *TAKE IT DOWN Act*, S.146, 119th Cong. (2025), https://www.congress.gov/bill/119th-congress/senate-bill/146/all-actions

[99] Department of Infrastructure, Transport, Regional Development, Communication and the Arts. (2025). *Taking a stand against abusive technology.* [Press release]. https://minister.infrastructure.gov.au/wells/media-release/taking-stand-against-abusive-technology

[100] *Online Safety Act 2021*, section 187. https://www.legislation.gov.uk/ukpga/2023/50/section/187

[101] eSafety Commissioner. (2025). *Register of industry codes and industry standards for online safety.* https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards#register-of-industry-standards

[102] Ofcom. (2025). *Protection of Children Code of Practice for user-to-user services.* https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/protection-of-children-code-of-practice-for-user-to-user-services.pdf?v=403579

[103] Information Commissioner's Office. (n.d.) *Age appropriate design: A code of practice for online services.* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

[104] Tenbarge, K. (2024, March 29). Fewer than 1% of parents use social media tools to monitor their children's accounts, tech companies say. *NBC News.* https://www.nbcnews.com/tech/social-media/fewer-1-parents-use-social-media-tools-monitor-childrens-accounts-tech-rcna145592

CANADIAN CENTRE *for* CHILD PROTECTION®

Helping families. Protecting children.

protectchildren.ca

@cdnchildprotect.bsky.social

Canadian Centre for Child Protection

@cdnchildprotect

Model in image and intended as illustrative.