# Submission regardingDraft General Comment No. 25(202x)Children’s rights in relation to the digital environment

The Canadian Centre for Child Protection Inc. (“**C3P**”) is pleased to have the opportunity to provide input into the Draft General Comment. C3P supports the Draft General Comment as a whole. In this submission, we wish to offer specific information on the impacts of the digital environment on victims and survivors of online child sexual abuse and child sexual abuse material to ensure their experiences are taken into account in the final version of the General Comment.

# About C3P

C3P is a registered Canadian charity dedicated to the personal safety of all children. Our focus is on providing programs and services aimed at reducing and preventing child sexual abuse (“**CSA**”) and the online victimization of children. C3P operates Cybertip.ca, Canada’s national tipline for the public reporting of online child sexual exploitation, which is a central component of the Government of Canada’s *National Strategy for the Protection of Children from Sexual Exploitation on the Internet*. Cybertip.ca receives and processes tips from the public about online crimes against children and refers any potentially actionable reports to the appropriate police unit and/or child protection agency.

## International Survivors’ Survey

In 2016, our organization, along with NCMEC and other experts from around the globe, launched the International Survivors’ Survey (Survivors’ Survey)[[1]](#footnote-1) for adult survivors whose childhood sexual abuse was recorded and, in most cases, distributed online. Over the course of a year and a half, 150 survivors from various countries completed the survey and contributed invaluable insight into the unique historical and current challenges faced by survivors. As the first generation of victims whose abuse has been/may have been posted or circulated online, these survivors provided critical information to identify gaps in the systems that respond to and support victims of this crime. The primary findings from this research that are pertinent for the General Comment were:

• Nearly 70% of respondents indicated they constantly worry about being recognized by someone who has seen images/videos of their abuse (n=103), and 30 respondents reported being identified by someone who has seen images/videos of their abuse.

• When asked how the existence of the images/videos impacted them differently from the child sexual abuse itself, survivors frequently spoke of the permanence of the images/videos and that if the material was distributed, their circulation will never end, which underscored the powerlessness they felt about the imagery/videos.

## Project Arachnid – a global tool to tackle online CSAM

Following the release of the survey results, C3P launched **Project Arachnid** to reduce the availability of child sexual abuse material (“CSAM”) [[2]](#footnote-2) globally and help break the cycle of abuse experienced by survivors. This innovative tool helps combat the growing proliferation of child sexual abuse material (CSAM) on the internet by detecting where known CSAM is being made publicly available and issuing notices to the entity hosting the material to request its removal.[[3]](#footnote-3) Processing tens of thousands of images per second, Project Arachnid detects content at a pace that far exceeds that of traditional methods of identifying and addressing this harmful material. As of October 1, 2020, over 6.2 million notices have been sent to providers requesting removal of content. Project Arachnid is currently detecting over 100,000 unique images per month that require analyst assessment, and this number has been increasing each month.

One of the most important outcomes of Project Arachnid is the psychological relief offered to survivors of CSAM who have had no control over the distribution and ongoing sharing of their recorded sexual abuse. Every time their image or video is viewed survivors are re-victimized. By curbing the public availability of this content, Project Arachnid helps break the cycle of abuse for survivors, and address the very real fear someone they know may come across an image of their abuse on the internet.

## How children are being failed within the current regulatory vacuum

In November 2019, our experiences within Project Arachnid prompted us to write *How we are Failing Children: Changing the Paradigm*. (the “**Framework**”),[[4]](#footnote-4) an urgent call to action for governments, industry, and hotlines around the world. In the framework, a set of principles is proposed that prioritizes the best interests and protection of children, clarifies roles and responsibilities with governments, trusted/verified hotlines and industry, and ensures a coordinated, standardized, and effective response across jurisdictions as it relates to the removal of CSAM and harmful/abusive material.[[5]](#footnote-5) The framework is grounded in the rights of children to dignity, privacy, and protection from harm. There are two major aspects around the removal of CSAM, and harmful/abusive images that urgently needs to change:

1. To date, the removal of child sexual abuse imagery has been limited to content that reaches a criminal law threshold (images that would qualify as worst of the worst, and be seen as illegal in most countries). It has become abundantly clear from our work in Project Arachnid that we are not going far enough to protect children from abuse and harm when we confine content removal to a criminal threshold. Countless harmful/abusive images of children remain online (such as physical abuse material, or material that sexualizes children without being illegal in all cases). **Removal strategies must be based on what is in the best interests of children and what is needed to safeguard them from harm.**
2. What is removed, and the speed at which it is removed, is highly inconsistent and varies widely by provider. Some providers are resistant to removal, and will engage in debates about whether an image is of a child or a young adult, and use the slightest hint of sexual maturation to delay removal. Moreover, while approximately 400 companies currently receive notices issued by Project Arachnid, actual removal ranges from one day or less (with the top 10% of companies) to two weeks (for the bottom 10% of companies). **The undeniable truth is the rights of a victimized child will be continually violated as long as images/videos of them being sexually harmed and abused are available on the internet. It is essential that all such content be removed as expeditiously as possible.**

# Focus of Submission

**Overall, the Draft General Comment covers many of the issues that ought to be included. In the comments below, we have confined our comments to those sections of the Draft General Comment that may not adequately reflect the experiences of victims of CSAM and online CSA:**

## The best interest of the child (art. 3, para. 1) (Section 14)

The internet is largely unregulated, which means that to date, the safety of children online has been left in the hands of industry. While it is true that some of the more prominent industry members have taken some voluntary steps to safeguard the interests of children, something as important as ensuring a child’s best interests are met cannot be left to voluntary action. **The rights of children to dignity, privacy, and protection from harm will only be realized if States take decisive action to regulate the digital environment in so far as it applies to children.** *We refer you to page 18-29 of our Framework for concrete examples of how the current model of regulation is failing children (see footnote 4 for the link).*

## The right to be heard (art. 12) (Section 18 & 19)

For the past few years, we have been working with many survivors who are now adults but whose CSAM continues to circulate online. These survivors have given use a lens into the silencing effect that accompanies having your CSAM circulating online. For example, some survivors have actually had to change their name because their abuser posted it alongside their imagery. Some survivors avoid online spaces all together for fear of being identified, recognized or stalked. We strive to ensure that the voices of these survivors are amplified for policy makers, the courts, and the public in a way that is safe for them and protects their identity.[[6]](#footnote-6) These survivors have first-hand experience with the harm that can result when online decision making and user safeguards are left in the hands of businesses and must be consulted in addition to consulting those who are still children.

## The business sector (Section 36 – 39)

To date, businesses have been able to set the rules for access to their platforms. They have been free to decide who obtains access to their platforms, what those with access are allowed to do/post on the platform, the age at which children can access the service, what children can and cannot do on the platform, and what content can be communicated to children using the platform. All of this has occurred without concrete rules or guidance from any government, which has created a digital landscape that is not safe for children and is prone to abuse by those who seek to harm them. The current speed at which technology is evolving and new apps are being created presents an ongoing challenge to preventing and addressing online child sexual exploitation. Legislation in Canada – and in all other countries – cannot realistically keep up with that pace. The result is a technology sector that has some members who do a lot to stop the proliferation of CSAM and online grooming on their platforms, and others who do virtually nothing.[[7]](#footnote-7) Governments must step in and create binding, enforceable laws that require all businesses to operate in a way that safeguards and promotes the best interests of children.

## Remedies (Sections 44 – 50)

Through C3P’s work with survivors of CSAM, it is apparent that supports such as restitution (section 47), a responsive legal system and legal assistance (section 45), therapy (section 46), and the ability to bring forward a class action or public interest litigation (section 45) are not universal, and even when they appear to exist on paper, they are either inaccessible or insufficient in practice.[[8]](#footnote-8)

An important remedy to implement is the “*removal of unlawful content*” (section 47). For survivors of CSAM and other harmful material posted online, the removal of such material is integral to their psychological recovery and reintegration. The existence of such material and the knowledge of its continued presence online causes extreme anxiety and distress for many survivors (see Survivors’ Survey, footnote 1 above). Current practices and procedures for the removal of CSAM and other harmful material has not been consistent or transparent, with critical decisions about removal being largely left in the hands of businesses. This has resulted in several issues, namely:

* **Removal has been restricted to that which is clearly and unequivocally illegal, without regards to other material that is still harmful to children.** Criminal definitions do not account for the wide range of harmful/abusive images that are available, and are too restrictive when making decisions about image removal. This means a significant proportion of harmful/abusive images remain online.
* **Inconsistent and subjective assessment processes by digital companies**. For some businesses any signs of physical maturity will result in an image not being removed in spite of having received the removal request from a trusted/verified hotline.
* **Physical abuse images/videos are often not addressed.** The physical abuse is extreme and sometimes includes elements of bondage or even physical torture.
* **Arbitrary application of terms of service by businesses.** Companies interpret and apply these rules without any real avenues for review or appeal by members of the public. Operating independent of any meaningful oversight has inevitably resulted in arbitrary decisions associated with removal of harmful material from the internet.

States should implement a regulatory framework that requires companies to remove material that is harmful to children. While voluntary guidelines are a start, they are not a long term solution. What is required is legislation from States that regulates the way in which businesses operate in relation to safety and security safeguards for children.

The implementation of a regulatory framework is also supported by the public. For instance, following the publication on November 9, 2019, of the *New York Times* article, “*Child Abusers Run Rampant as Tech Companies Look the Other Way*,”[[9]](#footnote-9) C3P launched a short survey for the general public to weigh in with their view on the responsibility businesses bear in the removal of CSAM and harmful/abusive images of children on the internet. Over 10,000 people completed the survey, and results showed that 90% felt governments should pass laws that require technology companies to meet safety standards that include penalties for non-compliance.[[10]](#footnote-10)

## Access to information (arts. 13 and 17) (Section 57)

Guidelines, standards and codes are all approaches that have been part of the narrative on the issue of CSAM for over two decades. Yet the proliferation of CSAM and other content harmful to children has exploded. We believe the time has come for regulation. In the meantime, transparency in content moderation and enforcement of community standards is desperately needed.

## Right to Privacy (art 16) (Sections 69, 72, and 78)

**Threats to children’s privacy (section 69).** Distribution of CSAM is not included in the list of criminal offences at the end of section 69, and that is a significant oversight. CSAM is one of the fastest growing crimes in the world and poses a pressing danger not only to the children in the CSAM, but to children everywhere. Moreover, in much of the CSAM found online, the child’s face is fully visible.[[11]](#footnote-11) Also, some offenders post the child’s name, location, age, and/or other identifying information about the child with the CSAM, while some chatrooms and online forums post information about the children in the CSAM, such as the child’s current location, and even sometimes reposting content obtained from the child, a parent, or a family member’s social media profile.

**End to End Encryption (section 72).** C3P agrees that children should be protected from surveillance from third parties. However, it is an inescapable fact that end-to-end encryption (E2EE) will make it far easier for those who offend against children to escape detection. Adoption of E2EE must not occur without first assessing and mitigating against the risk to children, particularly those who are victims of CSAM or online grooming and predatory behaviour.

**Safety by design (Section 78).** The examples of illegal and harmful behaviour in section 78 must also include CSAM, harmful/abusive material and the online grooming/luring of children.

## Violence against children (Part VII) (Sections 82 – 88)

**Forms of violence (Section 85).** Worldwide, CSA offences are on the rise and in particular CSA offences facilitated by technology. The number of victims of these crimes is growing exponentially. Article 19 of the UNCRC expressly requires that State Parties **shall** take all appropriate measures to protect the child from **all** forms of violence. Similarly, Article 34 of the UNCRC expressly mandates that State parties **shall** prevent the inducement or coercion of a child in **any unlawful sexual activity**. The clear directives in the UNCRC are weakened by the language used in the last statement of section 85 which says that States “should” pursue preventative, safeguarding and restorative justice approaches”. Moreover, referencing “restorative justice” in this context is confusing without more context, and risks detracting from the overall combined thrust of Articles 19, 34 and 39 which is to promote the physical and psychological recovery and social reintegration of a child victim.

**Regulatory framework (section 87).** It is clear that society cannot police its way out of online child victimization. It is essential that businesses start heavily investing in proactive measures to protect children on their platforms. Social media companies & online platforms are the entities that have the data and infrastructure needed to engage in effective prevention activities, and must be mandated to do so. Some examples of what could be done include:

* Requiring business to have easy to use and locate reporting mechanisms that are specific to CSAM and online CSE, and prioritize the processing of reports of this nature
* Requiring business to consistently use tools to detect known CSAM and online grooming, and remove content/intervene as necessary to disrupt abuse in progreess.
* Enacting a legal framework that mandates providers to detect, intervene and disrupt online discussions clearly aimed at child victimization or CSAM (e.g., chatrooms, feeds or usernames titled “Daddy-daughter incest”).

**Missing. While Part VII of the Draft General comment references Article 39, it does not appear that any of the provisions address Article 39. This oversight should be rectified in the final version. Article 39 of the UNCRC is particularly relevant for those who have had CSAM of their abuse distributed online, as these individuals are revictimized each time such CSAM is shared.**

## ****Protection from economic, sexual, and other forms of exploitation (arts. 32, 34, 35 and 36) (Section 123).****

While many countries have in place legislation that tackles trafficking of children for sexual purposes or forced child labour, and child abuse, such legislation does not always account for the ways in which these crimes are committed online (e.g., the use of live streaming to sexually exploit children for money, the rise of the amateur porn industry in which adolescent content may go undetected, and the increase in platforms/apps that reward content creators with tokens or digital currency, and have been associated with child victimization). States must enact legislation to address these new ways in which children are being exploited. In addition, section 12 ought to include crimes such as the trafficking of children for sexual purposes or forced child labour, CSAM, and harmful/abusive material, in addition to the examples already provided – fraud and identity theft.

# Conclusion

The General Comment on children’s rights in relation to the digital environment is a welcome addition to the General Comments that related to the UNCRC. States who wish to do more to protect children, and address the shortcomings of the present, unregulated, digital environment need to understand that it is no longer an option to accept the status quo. We know too much about the ways in which children are being exploited and victimized online to continue along the current path. Adopting criteria for the digital environment that is focused on what is in the best interest of child is essential and long overdue.

1. An executive summary, and the full results, of the survey can be found at [www.protectchildren.ca/surveyresults](http://www.protectchildren.ca/surveyresults) [↑](#footnote-ref-1)
2. This material is often referred to as “child pornography” in legislation. [↑](#footnote-ref-2)
3. Approximately 85% of the notices issued to date relate to victims who are not known to have been identified by police. [↑](#footnote-ref-3)
4. Visit <https://protectchildren.ca/en/resources-research/child-rights-framework/> for a copy of the Framework. [↑](#footnote-ref-4)
5. Harmful/abusive material includes material that depicts or describes a person who is, or who appears or is implied to be, a child as a victim of torture, cruelty or physical abuse (whether or not the torture, cruelty or abuse is sexual; or material that is harmful to children but does not meet the legal definition of CSAM. [↑](#footnote-ref-5)
6. For examples of how we do this, see <https://www.protectchildren.ca/en/programs-and-initiatives/phoenix11/> for the work we have done with the Phoenix 11, a group of 11 survivors whose child sexual abuse was recorded, and in the majority of cases, distributed online. The Phoenix 11 uses the collective power of their voices to affect change for themselves and the others who continue to suffer in silence. [↑](#footnote-ref-6)
7. See *the Canadian Centre’s report on How We are Failing Children: Changing the Paradigm*. Available online at <https://protectchildren.ca/pdfs/C3P_ChildRightsFramework_en.pdf>. Sources of information used to create the Framework included consultations with survivors, professionals working with survivors of CSA and CSAM, data gathered through Cybertip.ca, and information gleaned from survivors of CSAM. [↑](#footnote-ref-7)
8. For example, Canada’s Criminal Code has a provision that allows for restitution, but it has only been used in a handful of cases for the benefit of a victim of CSAM. Moreover, in Canada, access to state-funded therapy following the commission of a crime is the purview of provincial governments, and these programs are seriously limited in scope and duration and are rarely sufficient to meet the needs of survivors of CSAM, who are continual victims as a result of their content being repeatedly shared. [↑](#footnote-ref-8)
9. This article provides information about the ways offenders exploit the non-regulated internet to facilitate their crimes, and can be found at: [*https://www.nytimes.com › interactive › 2019/11/09 › internet-child-sex-abuse*](https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html) [↑](#footnote-ref-9)
10. 83% felt a technology company who does not remove CSAM on its service companies should be criminally charged. Another 15% felt companies should be fined for failure to remove. 95% felt that technology companies who are notified that stolen images of children are being reposted/shared in a sexual context on their services and platforms should be required by law to remove the stolen images (An example of a stolen image is when someone snags a photo of a nude or semi-nude child from a person’s unsecured social media account. It is not uncommon for these type of images (e.g., an image of a toddler in a mini pool in a backyard) to then appear on public forums and chatrooms harmful to children where the image is used in a sexualized context by those with a sexual interest in children.) [↑](#footnote-ref-10)
11. Canadian Centre for Child Protection Inc., “Child Sexual Abuse Images on the Internet: A Cybertip.ca Analysis” (2016). Available online: <https://www.cybertip.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf>. [↑](#footnote-ref-11)