February 18, 2021

House of Commons
Standing Committee on Access to Information,
Privacy and Ethics

Re: Study on Protection of Privacy and Reputation on Platforms such as Pornhub.

Thank you for giving the Canadian Centre for Child Protection the opportunity to participate in the above-noted study.

I. About the Canadian Centre for Child Protection ("C3P") and Cybertip.ca

C3P is a registered Canadian charity dedicated to the personal safety of all children. Our focus is on providing national programs and services aimed at reducing and preventing child sexual abuse ("CSA") and the online victimization of children. All programs and services are provided in both official languages.

For the past 18 years, C3P has been operating Cybertip.ca, Canada's national tipline for the public reporting of online child sexual exploitation. Cybertip.ca was officially launched in 2002 as a pilot project in the Province of Manitoba, and in May 2004, Cybertip.ca became a central component of the Government of Canada's *National Strategy for the Protection of Children from Sexual Exploitation on the Internet*. In addition, as the legal entity that operates Cybertip.ca, C3P is designated to receive reports from Manitobans under the *Child Pornography Reporting Regulation (Manitoba)*[1] and from internet service providers under the federal *Internet Child Pornography Reporting Regulations*[2].

Cybertip.ca receives and processes tips from the public about potentially illegal material online, such as child sexual abuse material[3] (CSAM), child trafficking, internet luring, and other areas of child exploitation. The tipline then refers any potentially actionable reports to the appropriate police unit and/or child welfare agency. Specifically as it relates to reports of possible "child pornography", Cybertip.ca analysts review the actual image, video, written content or audio to determine what action is required. This review involves accessing the reported material to determine whether it meets the *Criminal Code* definition of "child pornography" or whether there is harm to a child that might not meet the *Criminal Code* by assessing both the severity of the abuse depicted in the reported material and the approximate age of the child through sexual maturation characteristic analysis. As part of responding to public reports and classifying images/video located on the internet, Cybertip.ca analysts may also review the context surrounding the reported image/video, which may include file names and text communications posted on forums used by consumers of child sexual abuse material.

To illustrate the ease with which CSAM can spread online, a report published by Cybertip.ca in 2009 indicated that "over a 48 hour period, Cybertip.ca observed one website cycle through 212 unique IP

[1] The *Child Pornography Reporting Regulation*, Reg. 79/2009 is made pursuant to *The Child and Family Services Act (Manitoba)*, C.C.S.M. c. C80 and pertains to the reporting obligation set out in section 18(1.0.1) of *The Child and Family Services Act (Manitoba)*.
[2] *Internet Child Pornography Reporting Regulations*, SOR/2011-292. Pursuant to section 2 of *An Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service*, S.C. 2011, c. 4.
[3] In the *Criminal Code*, child sexual abuse material is called "child pornography".

addresses, located in 16 different countries." [4] That was in 2009. The techniques used by offenders today are different, but the sophistication is even greater now.

II. International Survivors' Survey

In 2016, our organization worked with an international group of experts to develop and launch a survey 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. [5]

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. Survivors told us the recording of the abuse and its continued online availability created an additional layer of trauma which coloured every aspect of their lives. Simply knowing such recordings exist, and that individuals around the world are able to view and take pleasure from them, evokes a variety of emotions including fear, shame, and a pervading sense of powerlessness. As so eloquently expressed by one such survivor:

> *"I still believe these images can ruin my life. I will still feel ashamed of myself for a long time that so many people can look at them, even though the abuse is over. I can protect myself from being raped again, but there's nothing I can do against these photos and videos being sold and stored."*[6]

A prevalent theme observed in responses to the survey was the fear of being recognized by someone who had seen images of the abuse – nearly 70% of respondents expressed this fear (n=103), and 30 respondents reported being identified by someone who has seen images/videos of their abuse.

The knowledge that their sexual abuse images/videos may be or are publicly available has an enormously negative impact on survivors. The impact of ongoing circulation significantly reduces the ability of survivors to cope with day-to-day stressors, maintain healthy relationships, and reach their full potential in educational and occupational pursuits. By taking concrete steps to curb the public availability of child sexual abuse images, the ongoing harm to survivors can be reduced.[7]

III. Project Arachnid – a global tool to tackle online CSAM

To assist in tackling the public availability of child sexual abuse material that continues to proliferate online, C3P launched Project Arachnid in January 2017. Project Arachnid is a platform designed to reduce the availability of child sexual abuse material ("CSAM") [8] globally and help break the cycle of abuse experienced by survivors. This innovative tool helps combat the growing proliferation of CSAM on the internet by detecting where known CSAM is being made publicly available and issuing notices to the

[4] Canadian Centre for Child Protection Inc., "Child Sexual Abuse Image: An Analysis of Websites by Cybertip.ca" (November 29) at page 63. Available online: <https://www.cybertip.ca/pdfs/CTIP_ChildSexualAbuse_Report_en.pdf>.
[5] An executive summary, and the full results, of the survey can be found at www.protectchildren.ca/surveyresults
[6] Canadian Centre for Child Protection Inc., (2017), *Survivors Survey*, *Full Report.* Page 149.
[7] Canadian Centre for Child Protection Inc., (2017), Survivors Survey, Full Report, Page 90.
[8] This material is often referred to as "child pornography" in legislation.

entity hosting the material to request its removal.[9] Processing tens of thousands of images per second, it detects content at a pace that far exceeds that of traditional methods, and expedites the process of removal by alerting companies to the presence of this harmful material on their platforms. As of February 1, 2021, over 6.6 million notices have been sent to providers requesting removal of CSAM. Approximately 85% of the notices issued to date relate to victims who are not known to have been identified by police.

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.

IV. Scope of the Problem

There have been countless research projects and studies attempting to quantify the volume of child sexual abuse images on the internet. As a result, there is more than enough evidence to confirm an abundance of images and videos of children being sexually abused is available worldwide.

Over the past 18 years, our organization has been on the front lines of this issue, and has witnessed the exponential growth of an online community that takes pleasure in the abuse and rape of children. Consider the following:

- Over the last few years, Cybertip.ca has moved from managing3,000 or more reports/month from the public to processing approximately 100,000 reports/month as a result of Project Arachnid and the automated detection of suspected child sexual abuse images. In 2018, Cybertip.ca assessed double the amount of imagery it had in the previous 15 years combined.
- In early 2018, a joint report released by INTERPOL and ECPAT International[10] stated as of August 2017, the Internet Child Sexual Exploitation Database (ICSE) Database[11] contained over one million unique individual images and videos and that, "it is widely acknowledged that many millions of child sexual abuse images are currently in online circulation."[12]

As another indicator that this problem has grown exponentially, one need only look to Statistics Canada's reports on police-reported crime statistics in Canada which clearly demonstrate an alarming increase in police-reported incidents involving child pornography offences. According to Statistics Canada, the rate of police-reported child pornography offences in Canada increased by 46% in 2019 over 2018,[13] and there has been a 449% increase in police reports of child pornography offences from 2009 to 2019.[14]

[9] Approximately 85% of the notices issued to date relate to victims who are not known to have been identified by police.
[10] EPCAT International and INTERPOL, (2018), *Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material*. Interpol, 2018.
[11] Launched in 2009, ICSE is a tool for law enforcement to investigate child sexual abuse material in the form of images, videos and hashes.
[12] EPCAT International and INTERPOL, (2018), *Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material*. Interpol, 2018. page 20, quoting: Carr, J., and Hilton, Z. (2011), "Combating child abuse images on the internet – international perspectives". In J. Davidson and P. Gottschalk, (Eds.), "Internet Child Abuse: Current Research and Policy", 52-78, Abingdon: Routledge.
[13] Juristat, *Police-reported crime statistics in Canada, 2019* (Catalogue no. 85-002-X) Table 1 (Statistics Canada, 20 October 2020).
[14] Juristat, *Police-reported crime statistics in Canada, 2019* (Catalogue no. 85-002-X) Table 1 (Statistics Canada, 20 October 2020).

Consider also a 2018 joint report from INTERPOL and ECPAT International which describes the immense challenges with quantifying the amount of child sexual abuse material available online and points to the fact that new content is created daily as one of the major hurdles.[15] Our agency is well aware of this challenge - in addition to detecting millions of images of known CSAM, Project Arachnid is currently also detecting over 100,000 unique images per month that do not match to known CSAM but are posted on sites with known CSAM and thus require analyst assessment. This number has been increasing each month, and our organization has directly engaged hotlines around the world to assist in the assessment and classification of these additional images. In addition, members of the offending community will often modify or combine existing CSAM to create new CSAM. Such modified content poses significant challenges for detection and assessment as it may not be readily recognized by automated systems relying on existing hash technology.

V. How children are being failed within the current legal framework

In November 2019, our experiences within Project Arachnid prompted us to write *How we are Failing Children: Changing the Paradigm*. (the "Framework"),[16] an urgent call to action for governments, industry, and hotlines around the world. The Framework used information learned from operating Project Arachnid to explain how the absence of a legal or regulatory framework governing the removal of child sexual abuse material directly harms children.

We were prompted to write the Framework as our experience in operating Project Arachnid had caused us to become deeply concerned by the varying levels of commitment demonstrated by technology companies to address this problem and safeguard children. There was, and still is, a range of responses to notices issued by Project Arachnid whereby some react quickly to remove CSAM and are proactive in their detection efforts, using the latest tools and database, while others enter into protracted debates about the legality of a particular image or even refuse to remove clearly illegal material. We have also encountered cases in which small companies are exploiting loopholes and jurisdictional differences to evade authorities and obscure their identity and location, thus not only routinely avoiding their obligations to remove child sexual abuse images, but in some instances providing the platform that facilitates and promotes the exchange of such material. Notably, these quasi-legal or potentially criminal operators receive internet, technical, and professional support from larger internet transit providers who are generally not in a position to know this is occurring through their services. The problem is complex and multi-layered, and cannot be solved through criminal law alone.

The Framework advocates for a paradigm shift whereby removal efforts focus on the best interests of the child, and the rights of children to dignity, privacy, and protection from harm. That has not been the case to date, and in fact, the voices of victims and survivors have been notably absent in public discourse surrounding internet regulation and privacy. As pointed out in the Framework, 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. The child's rights to privacy, identity, to be protected

[15] INTERPOL and ECPAT International, *Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material*, 2018 at page 20. Available online: <https://www.interpol.int/Media/Files/Crime-areas/Crimes-against-children/Technical-report-Towards-a-Global-Indicator-on-Unidentified-Victims-in-Child-Sexual-Exploitation-Material-February-2018>.

[16] Visit https://protectchildren.ca/en/resources-research/child-rights-framework/ for a copy of the Framework.

from harm, as well as to full psychological recovery and social reintegration – rights guaranteed to children through the United Nations *Convention on the Rights of the Child* - are all violated when CSAM remain accessible on the internet. It is incumbent upon governments to play a leadership role in setting up a legal and regulatory framework. The current model that puts criminal law responses at the forefront, and relies upon the voluntary actions of a largely unregulated industry, with no transparency and no accountability, has failed children.

Within 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.[17] It is grounded in the rights of children to dignity, privacy, and protection from harm, and proposes that 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 clear 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, in particular their rights to privacy and dignity, will be continually violated as long as images/videos of them of a sexual nature are available on the internet. It is essential that all such content be removed as expeditiously as possible.

The rights of children to dignity, privacy, and protection from harm will only be realized if governments take decisive action to regulate the digital environment in so far as it applies to children.

[17] 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.

VI. MindGeek (and other Adult Pornography Sites)

MindGeek is a tech company that owns one of the largest networks of web-based adult pornography sites. This network includes PornHub – its most popular asset – but also includes other popular adult sites as RedTube, YouPorn, Tube8, Brazzers, XTube, PornMD, Thumbzilla, RealityKings, My Dirty Hobby, Digital Playground, GayTube, ModelHub, Brazzers.

While MindGeek is a large player in the adult industry, similar services across the industry have parallel issues because of the lack of a regulatory framework that specifies the way in which companies must treat illegal content, the lack of age verification for uploaders as well as the individuals pictured in the media, and the lack of verification of consent regarding the participants depicted in the content.

VII. Reports made to Cybertip.ca and Project Arachnid related to Pornhub and other MindGeek Platforms

The following data pertains to all of the reports processed by Cybertip.ca related to MindGeek domains in the last five years. These include incidents involving CSAM on their platforms as well as incidents of sexual exploitation or abuse with a connection to a MindGeek domain. Therefore, some reports were sent directly to law enforcement while in other cases, a notice was issued to a service provider for the removal content:

Year	Total	Total Actioned*	Reports Where Notice Sent to Service Provider	Reports Sent to Law Enforcement
2015	282	12	0	12
2016	422	27	0	27
2017	285	18	2	16
2018	496	7	3	4
2019	379	61	44	17
2020	788	348	334	14

*Total Actioned is the combined total of the reports where a notice was issued to a service provider and the reports sent to law enforcement. Reports may be about many issues, including online luring and CSAM, and multiple reports about the same image or video of CSAM may also arise. Our oral submission will focus on CSAM that had been reported to us or detected via Arachnid.

In some of the material in circulation on adult pornography websites, whether they are CSAM or material that is harmful/abusive of children, the child is often fully visible and identifiable.[18] This visibility not only heightens the degree of the privacy violation, but also presents an obvious risk to the child's personal safety and psychological security, now and in the future. It means any person who knows the victim could possibly recognize them, and for someone who does not know the victim, they might be able to identify them in the future. Of even more concern, in some instances, the actual name of the child is posted along with the abusive imagery or the name of the child becomes known to the offending community through other means. Due to the ongoing availability of the CSAM, many of these children have had to change

[18] This is in stark contrast to the offender who is either not visible in an identifiable way (e.g., face is blacked or blurred out, or cut off) or is not visible at all in the image/video, which in some instances can make it appear as though the image/video was created by the victim alone.

their name to avoid being identified and harmed by those who view them as sexual objects or commodities.[19]

> *I can never feel safe so long as my images are out there. Every time they're downloaded I am exploited again, my privacy is breached and I feel in danger again. I fear that any of them may try to find me and do something to me.*
>
> - Victim Impact Statement of a victim of CSAM that is actively traded online[20]

VIII. Categories of illegal content on adult sites such as PornHub

Based on the experience of C3P, the manner in which illegal content finds its way onto adult pornography platforms varies depending on the nature of the content itself.

There are three broad categories of **illegal** content:

(1) Child Sexual Abuse Material: pre-pubescent (Under 12 years)
(2) Child Sexual Abuse Material: post-pubescent (Between 12 and 17 years)
(3) Non-consensual distribution of intimate images (typically, 18+ years, but can also involve images of youth that were consensually shared initially but later distributed non-consensually)

Typically, images of prepubescent images of infants and young children are both recorded by an abuser and uploaded to the internet without the knowledge of the children depicted in the images.

With teenagers and adults, illegal or non-consensual content generally finds its way online under these scenarios:

- Images recorded by another person in the course of a sexual assault or exploitative action (e.g., voyeuristic recording) and then distributed online.
- Intimate images were voluntary created by the victim and shared with a partner in confidence who unlawfully distributed the media.
- Intimate images were voluntary created by the victim, but the images were stolen; or the victim voluntarily exposed themselves over webcam and the other person screen-captured the activity (e.g. FaceTime®, Zoom®, Skype®, etc.); and then someone unlawfully distributed the images created online.

Examples of File Names Seen by C3P on MindGeek Sites

In addition, the file names associated with content reported to Cybertip and that appeared to have been posted on MindGeek sites at the time of reporting are clearly descriptive/suggestive of illegal activity. This does not mean the file itself actually depicted what the title suggested it depicted (users do sometimes

[19] Under the United Nations Convention on the Rights of the Child, a child has the right to preserve his or her identity and name. Yet once an offender has tied a child's real name to a child sexual abuse image or harmful/abusive image, not only is that child's safety and security at risk, the child's right to retain their identity and name is potentially violated.
[20] Filed in multiple Canadian sentencing hearings. Citations available upon request.

misname a file to get more "clicks". In preparation for the presentation before this Committee, the Canadian Centre went back through its records and found the following examples of file names that were associated with videos posted to a MindGeek site.

- *[Personal Name redacted] Masturbates on Camera in Front of a 7 Year old Girl (detected in 2020)*
- *Very Young Girl Masturbating Porn Videos (detected in 2016)*
- *Dad Fucking his Young Son (detected in 2018)*
- *Jailbait Porn Videos (detected in 2015)*
- *SPYCAM -(©¿©)- PRIVATE CHANGING SHOWER CUBICLES AT PUBLIC BEACH (detected in 2016)*

Large Volume of Adolescent Content on Adult Pornography Sites

C3P is aware of a significant volume of CSAM that includes pubescent/post-pubescent victims that is available on adult sites. Particularly in the case of CSAM of post-pubescent content, confirmation of the identity and age of a minor in an image/video provides the opportunity to issue notices requesting its removal. Project Arachnid regularly detects child sexual abuse material involving identified pubescent and post-pubescent children on adult pornography sites, which is unlawful and must be removed.

IX. Content moderation practices for user-generated content

Generally speaking here are three methods technology companies can adopt to prevent or limit the amount of illegal or harmful content on their websites: proactive scanning via automation, human moderation and legitimate user-verification policies.

1) Proactive media scanning: One of the primary methods major tech companies can use to prevent the dissemination of child pornography of their system is to automatically compare the digital fingerprints of newly uploaded content against the fingerprints of known images of previously-confirmed child pornography. These fingerprints are generally available through a number of sources. One of the largest repositories of these digital fingerprints is managed the U.S. National Centre for Missing and Exploited Children (NCMEC). This approach, uses various types of technology, but one of the most effective ones is known as PhotoDNA (created by Microsoft). PhotoDNA allows systems to automatically detect exact or derivatives of known illegal images. The process of proactive scanning technologies, however, cannot detect images that are previously unknown (i.e. newly created content).

A note on claims of using "artificial intelligence" to detect illegal images: Based on C3P's extensive experience in the classification of child sexual abuse imagery and working with the technology industry, there is no known reliable method for detecting or classifying images for child pornography using artificial intelligence. In our experience, claims about the reliability of AI are generally suspect.

Distinguishing between a 17 and 18 year old person, for example, requires human moderation and often requires further inspection, including follow-up with the uploader. As well, certain images taken out of their original context and re-purposed in a sexualized context can at times meet the legal definition of Child Pornography (e.g. stolen picture from a online family photo album, with added captions and shared on pedophile web forums).

Lastly artificial intelligence cannot establish whether or not an intimate image of an adult was created voluntarily or willingly distributed.

Platforms may point out that their service has a good track record – relative to other platforms – for keeping their service clear of any illegal material based on their mandatory reporting figures. However, it is critical to understand that mandatory reporting figures are largely correlated to the amount of resources invested in the detection of illegal content.

An illustrative example: In 2019, Facebook reported approximately 13 million abusive images to NCMEC under mandatory reporting laws in the U.S. However, Facebook has invested significant resources in recent years to bolster its moderation practices. Another tech platform that does very little to attempt to detect illegal imagery and is satisfied with remaining in the dark on the nature the content on its platform would report significantly lower figures than Facebook. That doesn't mean that platform has less problematic content than Facebook.

2) Human moderation: Since automated systems cannot detect newly created (or previously unknown images) or understand the context in which an image was taken, platforms that accept user-generated content – such as PornHub – require teams of human trained human moderators who can intercept and assess suspect content before it is uploaded and spreads across the platform, if they hope to appropriately moderate their platforms.

   C3P's experience has been that tech companies rarely disclose details about the scale of their human moderation activities, nor the nature of the training they receive.

3) User-verification process: Any platform that allows user-generated content and does not verify users uploading content to their service inevitably leads to the distribution of harmful and illegal content. The last decade of social media has clearly demonstrated how ill-intentioned individuals can exploit poorly moderated platforms.

Some websites claim they "verify" user accounts. However, generally speaking, it is not clear what is meant by "verified user" and what the verification process entails. Furthermore, the act of verifying a user, does nothing to ensure that the individuals appearing in the video or images are (a) of legal age, (b) consenting participants in both the activity and the recording of the activity, (c) consenting to the distribution of the media depicting the activity.

Conclusion

While this committee's focus to date has been largely been on the activities of PornHub, it must be made clear that several mainstream companies operating websites, social media, email, and messaging services that most parliamentarians interact with daily could just as easily have been put under the microscope.

With – literally-- billions of daily users across these platforms, moderating content at this scale is a colossal and expensive undertaking. Our two-decade long social experiment with a largely unregulated internet has shown that whatever companies claim they are doing to keep CSAM off of their servers – it is not enough.

We must not lose sight of the core problem that led to this moment. We have allowed digital spaces – where children and adults intersect - to operate with no oversight. We have allowed companies to unilaterally determine the scale and scope of their moderation practices. These failures have left victims and survivors at the mercy of these companies to decide if they take action or not.

We do not accept this standard in other forms of media in his country — including television, radio and print. We should not accept it, as our inaction collectively has, in the digital space.
As we are seeing in Europe, in the U.K., in the U.S. and at home, in Canada: those with the power to effect change are coming to their senses and beginning to enact meaningful change. This is critical because this is a global issue, and it needs a global, coordinated response, with strong, unambiguous laws that require tech companies to:

- implement and use available tools to combat the flagrant and relentless reuploading of illegal content;
- hire, train and effectively supervisestaff to carry out moderation and content removal tasks at scale.
- keep detailed records of user reports and responses that can be audited by authorities;
- be accountable, from a legal perspective, for moderation and removal decisions and the harm that flows to individuals, when companies fail in this capacity;
- build in, by design, features that prioritize the best interests and privacy rights of children.

Our sincere hope is that Canada will assume a leadership role in addressing the harm that has resulted from a lack of regulatory and legal oversight in this space. It is clear that relying on the goodwill and voluntary actions of tech companies is not working. The time has come to impose some guardrails in this space. Children deserve no less.