Online Safety Branch, Content Division
Department of Infrastructure, Transport, Regional Development and Communications
Parliament House, Canberra

# Submission to the Consultation on the Exposure Draft

# Online Safety Bill 2020

## 1. Introduction

Thank you for the opportunity to offer comment on the Draft Online Safety Bill 2020.

Collective Shout (www.collectiveshout.org) is a grassroots movement challenging the objectification of women and sexualisation of girls in media, advertising and popular culture. We target corporations, advertisers, marketers and media which exploit the bodies of women and girls to sell products and services, and campaign to change their behaviour.  More broadly we engage in issues relating to other forms of sexploitation, including the interconnected industries of pornography, prostitution and trafficking as well as the growing market in the sale of children for Live Distant Child Abuse.[1]

Our work puts us in touch with the unique and specific ways children are at risk from these practices, especially in regard to being targeted by predators, who attempt to groom them online, and from exposure to pornography.  We have been documenting these harms over the past decade, including in our 2016 submission on harms of pornography to children to the Senate Environment and Communication References Committee,[2] our 2019 Submission to Inquiry into Age Verification for Online Wagering and Online Pornography[3] and in many publications and commentaries since then.[4]

---

[1] Tankard Reist, M. (2017). Why are Australian Telcos and ISPs enabling a child abuse pandemic? *ABC Religion and Ethics*. https://www.abc.net.au/religion/why-are-australian-telcos-and-isps-enabling-a-child-sexual-abuse/10095644

[2] Collective Shout (2016). Harm being done to Australian children through access to pornography on the internet: Submission to the Senate Environment and Communications References Committee. https://d3n8a8pro7vhmx.cloudfront.net/collectiveshout/pages/1019/attachments/original/1457408234/CS_Submission_Harms_of_Pornography_Inquiry_March_2016.pdf?1457408234

[3] Collective Shout (2019). Submission to Inquiry into Age Verification for Online Wagering and Online Pornography. https://www.collectiveshout.org/submission_to_inquiry_into_age_verification_for_online_pornography

[4] For example, see Tankard Reist, M. (2016). Early sexualisation and pornography exposure: the detrimental impacts on children. *Australian Childhood Foundation Blog.* https://professionals.childhood.org.au/prosody/2016/07/melinda-tankard-reist/

We welcome the draft Online Safety Bill with its new measures dealing with cyber-bullying and cyber-abuse, and proposed industry regulation which, if successfully implemented, will make Australia a world leader in online safety legislation. We were pleased to see that many of our concerns were incorporated into this draft.

However, there are several important omissions that we would like to see addressed in this bill.

## 2. Industry codes need more specific content requirements

The expansion of powers of the eSafety Commissioner is a significant and necessary development, particularly as it applies to the enforcement of industry codes. Unlike advertising industry self-regulation, a system we have negatively critiqued for a decade,[5,6] these online safety codes will have real teeth, with significant penalties for violations and a complaints mechanism that will work in the interests of users and citizens.

We are also pleased to see a requirement for community consultation in the development of these codes and look forward to offering our expertise in due course.

We strongly suggest the addition of more specific recommendations for the content of these codes, examples of which can be found in our original submission to the Online Safety Legislation Review. These recommendations originate from the #wakeupinstagram campaign spearheaded by advocacy organisations in three countries: Collective Shout (Australia), National Center on Sexual Exploitation (USA), and Defend Dignity (Canada):

   a) Strengthened requirements that apps and services protect all minors from being direct messaged by adults.
   b) Algorithms, overseen by human moderators, should be included to proactively remove sexualising or sexually graphic comments on minors' images and posts.
   c) Privacy settings should be much more visible in order to increase awareness of safety tools.

---

[5] See Collective Shout's tag "Ad Standards Panel complaints dismissed" here:
https://www.collectiveshout.org/tags/ad_standards_board_complaints_dismissed
[6] Collective Shout (2019). Submission on the AANA Code of Ethics Review Discussion Paper.
https://www.collectiveshout.org/submission_to_aana_code_of_ethics_review . Collective Shout (2013).
Submission to the Health and Community Services Committee Inquiry into Sexually Explicit Outdoor Advertising.
https://www.collectiveshout.org/submission_to_the_qld_inquiry_into_sexually_explicit_outdoor_advertising
Collective Shout (2011). Submission to the House Standing Committee on Social Policy and Legal Affairs Inquiry into the regulation of billboard and outdoor advertising.
https://www.collectiveshout.org/submission_to_federal_inquiry_into_the_regulation_of_billboard_and_outdoor_advertising

d) When an account is made private, remove the ability for strangers to send unsolicited direct messages to that account. Remove the ability for that person's account to be visible in Likes or Comments on other posts.

e) Include links in safety sections to define sexual harassment, and how to get help.

f) Revise 'Community Standards' so that all sexualised, predatory and grooming-style comments (text, slang, short-hand, hashtags, emojis and graphics) qualify as violations.

g) Add 'sexualised/predatory/grooming comment directed at a minor' as a category for reporting violations of community guidelines and address these reports as a priority.

h) Prohibit adults from using 'live' posts to contact minors.

i) Update Instagram's system used to detect and remove sexualised, predatory comments.

j) Recognising that Instagram serves as a supply source of images of children for web-based paedophile forums, update all relevant policies, guidelines and help documents (including 'A Parent's Guide to Instagram') so that users are properly informed of the risks of sharing images of children to the platform.

k) Stop the 'explore' feature from promoting minors' pages and connecting predators with children.

l) Investigate parasite pages that are exclusively devoted to republishing photos of minors, deleting pages where children are sexualised, harassed, groomed or where any type of predatory comments/behaviour is displayed.

m) Prohibit the republishing of images of minors on Instagram pages that also feature porn-style images of adults.

Last year the Canadian Center for Child Protection (CCCP) reviewed tools for reporting child sexual abuse material on a range of popular online platforms including Facebook, Instagram, Twitter, YouTube and Snapchat. Key findings included that current tools are not easily accessible and serve as a disincentive to users to report child exploitation material.[7]

We support a mandated requirement for all platforms to improve tools for reporting child exploitation activity, as per CCCP's recommendations (reproduced here verbatim from the CCCP report, p25):

● Create reporting categories specific to child sexual abuse material. With the exception of Microsoft's Bing search engine, none of the platforms highlighted in this report provide reporting functions specific to child sexual abuse material [CSAM]. Providing users with CSAM-specific reporting options should enable the prioritization for assessment and removal. Limiting the time these illegal images and

---

[7]Canadian Center for Child Protection (2020). Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms. https://protectchildren.ca/pdfs/C3P_ReviewingCSAMMaterialReporting_Summary_en.pdf

videos are available helps reduce the re-victimization of survivors and minimize other's exposure.

- Include CSAM-specific reporting options in easy-to-locate reporting menus. Avoid creating alternative reporting channels for CSAM. This category should be included alongside other commonly reportable violations that are already accessible and easy to find. The process for reporting copyright infringement should not be more intuitive or easier to complete than reporting an image of a child being sexually abused.
- Ensure reporting functions are consistent across entire platform. Throughout this review several inconsistencies in the reporting tools were observed. The process and steps taken to report CSAM on a platform should be identical whether on desktop or mobile, reporting a post or a user, or if the content is contained within direct message or publicly visible.
- Allow reporting of content that is visible without creating or logging into an account. Many of the platforms examined in this report allow members of the public without an account or users not logged in to continue viewing media. If content is visible under these circumstances, submitting a report should not require account creation or login.
- Eliminate mandatory personal information fields in content reporting forms. All of the reporting forms reviewed in this report required users wishing to report content to provide, at minimum, their name and personal email address. One platform requires users [to] provide their full home mailing address, phone number, as well as a dated electronic signature. Such reporting structures discourage users from reporting content and may be a barrier to reporting CSAM given its illegal nature.

Regarding reporting requirements, we are pleased to see that companies will be required to provide transparency reporting on their online safety policies, activities, and outcomes. We would however like to see adoption of one of our original recommendations—to require companies to report on the qualitative nature of complaints and responses, rather than merely the quantity of complaints and takedowns. MacKinnon and Wingfield explained in 2019:

> *Transparency reporting requirements which only ask platforms about how much harmful content they've taken down risk creating a dangerous incentive. A platform faced with such a requirement might reason that – in order to show 'progress' or compliance – the easiest solution is to deliberately increase the volume and rate of content removal. Users need very clear terms of service explaining what is allowed and what is not allowed on the platform, and how decisions will be made with regard to removal of content.[8]*

[8] MacKinnon, Amy and Wingfield, Richard (February 26, 2019). Approaches to Content Regulation - #4: Transparency Reporting. *Global Partners Digital* https://www.gp-digital.org/approaches-to-content-regulation-4-transparency-reporting/

### 3. Sexual exploitation should be a distinct category of online harm for children

In our submission to the Online Safety Legislative Reform Inquiry, we recommended that within the category of 'seriously harmful material,' sexual grooming and exploitation of minors be addressed as a distinct category. Such behaviour is currently not being addressed under the category of cyberbullying. In fact, according to our research and observations over many years, it is likely that children and especially girls have come to accept sexual grooming and exploitation as a normal part of social media, rather than identifying it as cyberbullying or abuse:

> *What we've found shows that sexualisation and harassment of underage girls on Instagram is rampant. By giving adults unfettered access to children and facilitating the transmission of sexual comments, Instagram is complicit in putting underage girls at risk and normalising them as available for sexual gratification. This is a gross act of social irresponsibility and violates socially expected standards of corporate conduct. My colleagues and I are spending a lot of time reporting these comments. Too often Instagram says the sexually explicit comments don't violate their "community guidelines."[9]*

This has become such a major problem that Collective Shout, along with National Center on Sexual Exploitation (USA) and Defend Dignity (Canada), is directly addressing it in our global #wakeupinstagram campaign referred to earlier.

### 4. The impact of encryption on children's safety

As part of our ongoing campaign against Live Distant Child Abuse (LDCA), we have consistently recommended against end-to-end encryption (E2EE).[10] In 2020 we made a submission to the United Nations' consultation on the Committee on the Rights of the Child's *Draft General Comment on children's rights in relation to the digital environment*.[11] We voiced our objections to Facebook's plan to roll out E2EE across all its messaging services, a move which leading governments and child safety

---

[9] Alison, Coralie (2019). Why is Instagram letting men share sexual fantasies about 7 year old girls? *Collective Shout* https://www.collectiveshout.org/predators_on_girls_insta_accounts

[10] Collective Shout urged government to address the matter of telecommunications companies facilitating live distant child sexual abuse in our 2019 submission to the Inquiry into the Modern Slavery Act 2018 and related matters. *Parliament of New South Wales,* https://www.parliament.nsw.gov.au/lcdocs/submissions/66119/0039%20Collective%20Shout.pdf

[11] Collective Shout (2020). Submission to Draft General Comment No. 25 (202x): Children's rights in relation to the digital environment. https://d3n8a8pro7vhmx.cloudfront.net/collectiveshout/pages/7128/attachments/original/1606279465/CollectiveShout_20201112_UN_Sub.pdf?1606279465

organisations say will prevent detection of predatory activity and child abuse. We said the move to E2EE would violate Facebook's commitment to the *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse* and expressed our support for efforts to block it until adequate measures have been taken to ensure children are not placed at greater risk of harm. It is alarming to note that by introducing E2EE, Facebook may lose the ability to report 70% of the cases it currently sends to the National Center for Missing and Exploited Children because it will no longer have access to users' conversations.[12]

The Office of the eSafety Commissioner also expressed objection to E2EE in its submission and position statement on the matter:[13]

> *While encryption is a powerful tool for privacy, it also can assist in serious harms by hiding or exacerbating criminal activities, including online child sexual abuse. Encryption requires detailed consideration to minimise the potential for harm across communication channels, and to ensure there is a balance between security, privacy and safety.*

We agree with the position of the Australian Federal Government expressed in its submission to the same United Nations inquiry:[14]

> *Australia strongly affirms the importance of children's privacy, and also recognises the importance of keeping children safe online and protected from harm. While strong encryption plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security, such encryption is being increasingly exploited by terrorists, sexual predators and other criminals to conceal illicit activities that are harmful to children. End to end encryption can erode the ability of companies to detect and report harmful and illegal conduct and content on their platforms and significantly impedes law enforcement. agencies in their ability to investigate and prosecute serious crimes, including serious crimes against children.*

> *In light of this, Australia does not support the position set out in the draft General Comment that end to end encryption should be encouraged by States. Such a 'privacy protection' focus does not sufficiently take into account the abuse and crime that occurs online, and the vulnerability of children online in particular, as*

---

[12] Brookes J (2019). Update: Dutton tells Facebook to 'pick a side' on child exploitation, demands halt to encryption plans. Which-50. https://which-50.com/dutton-demands-facebook-halt-encryption-plans/
[13] eSafety Commissioner (2020). End-to-end encryption trends and challenges — position statement. Available at https://www.esafety.gov.au/about-us/tech-trends-and-challenges/end-end-encryption-position-statement
[14] Commonwealth of Australia (2020). Submission of the Australian Government to the Advanced Version of the Committee on the Rights of the Child's Draft General Comment on children's rights in relation to the digital environment.
https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

*targets for predators and grooming groups who may use end to end encryption
and other technology to carry out and conceal their illegal and harmful activities
(whether that be to incite violence, abuse of children, non-consensual sharing of
intimate images or otherwise). We would ask the Committee to carefully consider
the impacts of its draft recommendation in paragraph 72 in light of the role that
governments and technology companies play in protecting children online and
preventing the sharing of child sexual abuse material.*

This month, UK man David Wilson was jailed for 25 years after admitting to 96 sex offences against
boys aged 4 to 14. The 36-year-old targeted more than 5,000 boys, grooming and soliciting them for
child sexual exploitation material.

Rob Jones, Director of Threat Leadership for the National Crime Agency, warned:

*Facebook's plans (for E2EE) are a disaster for child safety and law enforcement and mean the
very many other David Wilsons out there will not be caught. Their plans will create a haven
for child sex offenders to congregate to target children.[15]*

We urge the Committee, along with state, federal and international parties, to condemn Facebook's
planned rollout of E2EE across all messaging services in the strongest possible terms.

## 5. Age verification has not been addressed

Unfortunately the Federal Government has yet to respond to the House of Representatives Standing
Committee on Social Policy and Legal Affairs report *Protecting the Age of Innocence*, which was
published a year ago (February 2020) following the Committee's inquiry into age verification for
online wagering and online pornography.[16] It would have been helpful to see the Government's
response before contributing further to this current consultation, especially given the Committee's
recommendation of a "roadmap for the implementation of a regime of mandatory Age Verification

---

[15] The Guardian (February 11, 2021). Facebook under fire over encryption plans as man is jailed for abusing 52
children:  Police say they would not have caught David Wilson, who admitted 96 offences, if Facebook end-to-
end encryption was in place. https://www.theguardian.com/uk-news/2021/feb/10/man-who-posed-as-girl-
online-jailed-for-abusing-51-children
[16] Commonwealth of Australia (2020). Protecting the age of innocence: Report of the inquiry into age
verification for online wagering and online pornography. House of Representative Standing Committee on
Social Policy and Legal Affairs. Canberra.
https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024436/toc_pdf/Protectingtheageofinn
ocence.pdf;fileType=application%2Fpdf

for online pornographic material." Without knowing if the Government agrees to this recommendation or not, it is impossible to say how it might inform and intersect with the draft Online Safety Bill.

We made the following recommendations to that inquiry:[17]

1. In light of data verifying the real-life harms of childhood exposure to pornography the Commonwealth Government should recognise the potential benefits of an Age Verification system along with other measures to limit porn exposure to children, including education programs and improved ISP filters.
2. An Age Verification scheme for access to online pornography, drawing from work done to develop the original United Kingdom model and with added measures that address perceived shortcomings in the model, for example, additions that extend application to social media platforms, should be implemented by the Commonwealth Government.
3. Introduce an Age Verification system that will restrict children's access to online pornography (and the global porn industry's unfettered access to children), acknowledging that our obligation to protect children, and the ensuing protections afforded to children by such a system, far outweigh the concerns of those with vested interests in the global porn industry.
4. Introduce an Age Verification system that will restrict children's access to online pornography (and the global porn industry's unfettered access to children) and so uphold Australia's international obligations to protect children from abuse, exploitation, and developmental harm, acknowledging that exposure to online pornography amounts to abuse, exploitation, and harm.

We suggest your Committee makes direct representations to the Government to urge it to release its response to this year-old inquiry as soon as possible.

---

[17] Collective Shout (2019). Submission to Inquiry into Age Verification for Online Wagering and Online Pornography.
https://www.collectiveshout.org/submission_to_inquiry_into_age_verification_for_online_pornography

## 6. Stronger measures to combat image-based abuse[18]

While the 24-hour takedown commitment is at least a start, we note that the US is considering a two-hour takedown notice period.[19] [20] We believe this to be a more appropriate response, given the devastating impact of image-based abuse. Any delay in take-down affords greater opportunity for wider sharing causing even more trauma to the victim. Social media platforms have the resources to do this.

The fact that it is so easy to upload image-based abuse content is a serious problem. The Federal Government could invest in tech solutions to address this, for example by identifying individuals uploading image-based abuse material and barring them from uploading further material. Australia could also implement the use of trauma-informed evidence collection and interviewing techniques for victims. We understand it is common for victims to experience shame through the process of reporting and evidence collection, as well as being asked to hand over their images to proceed with charges.

Dedicated and specially trained police departments would be a positive step forward in obtaining justice for victims and preventing further offending.

Civil liability is an important way to get convictions and achieve redress for victims. When victims have recourse through civil courts, the standard of proof will be lower, allowing a less invasive and traumatic process for the victim. Being able to identify uploaders will involve user ID verification, age and consent verification, and personal civil liability for users and porn platforms.

We also recommend the establishment of a 24-hour hotline for victims to obtain support.

---

[18] We acknowledge advice provided by Laura Bloomer, CEO of Backed Technologies, providing data and legal knowledge to provide support to victims of image-based abuse/leaked content and create more accountability and convictions for offenders.

[19] Merkley, J. (2020). A BILL To prevent the uploading of pornographic images to online platforms without the consent of the individuals in the images. https://cdn.arstechnica.net/wp-content/uploads/2020/12/256391_SasseMerkleyDEC2020.pdf

[20] Merkley, J. (2020). Merkley, Sasse Unveil Urgently Needed Legislation to Crack Down On Online Sexual Exploitation. https://www.merkley.senate.gov/news/press-releases/merkley-sasse-unveil-urgently-needed-legislation-to-crack-down-on-online-sexual-exploitation

## 7. Concerns regarding Australia's Classification regulation

Noting the reliance on the Classification Board presumed by this Bill, we would like to reiterate our concerns regarding the classification system. We made multiple recommendations to the Review of Australian Classification Regulation in 2020 including the following:[21]

- Replace the current system with an evidence-based and age-based classification system.
- Broaden the provisions relating to 'sex' to reflect new research insights into sexual objectification.
- Any regulatory body (the existing or a new body) should be required to consult the international research along with child and youth development experts to ascertain the possible impact of content with sexualised content or messaging on this audience.
- If self-classification is to be introduced, it must be strongly regulated by the government using approved classification tools, overseen by a single regulator with powers of enforcement.
- Pornography should no longer be treated by default as 'adult content', but as commercialised sexual exploitation.
- Reliance on parents to control what their children access is unrealistic.
- An urgent investigation needs to be conducted into the Classification Board assigning M or MA15+ ratings to anime and manga genres featuring Child Sexual Abuse Material contrary to Australian law.

We note that the Committee review of the Australian Classification Regulation system, which concluded in February 2020 has also yet to report, which again limits the ability of stakeholders like ourselves to provide fully informed feedback to this consultation process.

We hope our input is useful to the Committee and thank members again for the opportunity to contribute to this consultation.

February 12, 2021

---

[21] Collective Shout (2020). Submission to the Review of Australian Classification Regulation. https://d3n8a8pro7vhmx.cloudfront.net/collectiveshout/pages/3311/attachments/original/1583331025/Collective_Shout_submission_review_classifications_system.pdf?1583331025