Draft General Comment No. 25 (202x) Children's rights in relation to the digital environment

Contents

I. Introduction

We commend the Committee on its examination of this issue and welcome the opportunity to contribute.

Collective Shout is a grassroots movement challenging the objectification of women and sexualisation of girls in media, advertising, and popular culture. The unique vulnerabilities of children to online child sexual exploitation (CSE), grooming, harmful pornography exposure, and their exploitation in Live Distant Child Abuse (LDCA), is also of special concern, therefore our recommendations focus on these matters.

21. and 52. Children's evolving capacities

Recommendation:

We commend to you the submission made by our colleagues at the Australian Council on Children and the Media (ACCM), the peak Australian NGO providing information and advocacy on children's engagement with the media, which addresses children's evolving capacities, balancing protection and emerging autonomy.

28. Mandated government body

Australia's Office of the eSafety Commissioner (eSafety) was established in 2015 with a mandate to coordinate and lead online safety efforts across government, industry and non-profits. Resources and services are underpinned by evidence-based research into internet use, online safety, e-security and related issues. This is a model for other States seeking to improve citizens' and particularly children's online safety and benefits.

Recommendation:

States investigate the model of a mandated government body such as eSafety.

36-39. Business sector obligations

In November 2019, Collective Shout, the National Center on Sexual Exploitation (USA) and Defend Dignity (Canada) launched the #WakeUpInstagram and #InstaPimpsGirls campaign to stop sex trafficking, CSE, grooming and fetishisation of underage girls, calling on social media platforms to prioritise the safety of children over their accessibility to adults. Our investigation documented

hundreds of cases of predatory behaviour toward underage girls on Instagram which was facilitating the transmission of sexual comments—including requests for sexual images—from men to girls. We captured naked men masturbating to underage girls—one just 9 years old—during the girls' live posts.

With our partner agencies, we have called for the following action, and recommend them to States as policies for all social media platforms:

1) Do not allow strangers to direct message minors.

2) Proactively remove sexualising or sexually graphic comments on minor's photos.

3) Improve reporting categories to capture grooming/sexualising/exploitation of a minor.

Since July 2019 we have reported hundreds of accounts directly to Instagram for CSE activity. We also documented the widespread failure of moderators to remove exploitative content and block users engaged in CSE—even where users solicited or advertised sale or trade of CSE material (CSEM). Most often our reports were only actioned when we referred them to the Office of the eSafety Commissioner or to our Facebook executive contacts.

In September 2020, Instagram responded directly to our campaign by adding a new in-app reporting tool to flag users who share and host content which exploits children and expedite review and takedown. Earlier, Instagram had added a tool for reporting individual posts which sexualised children; while this allowed moderators to prioritise their review, the context in which the posts were shared was often missed. The new tool is intended to close that gap. However, our experience so far is that there has been no improvement in the takedown rate of this content since.

In October 2020 Instagram added a new privacy feature in the USA to block strangers from direct messaging account holders, giving minors increased protection from predators. It is expected to be made more widely available in future. However, it only works where minors are not connected to predatory adults via a follow i.e. where the child follows the adult's account. We documented minors including a nine-year-old who follow predatory men or men who post pornographic content. Such children remain vulnerable to being targeted by direct-message-facilitated CSE despite the new tool.

Associate Professor of Criminology at the University of NSW, Dr Michael Salter, argues social networks should keep minors in a "walled garden" similar to the new YouTube Kids. He says the fundamental flaw in platform design was that adults could directly contact children who were strangers to them. "For as long as those design features are enabled in platforms, we will always have predatory adults who are targeting children," Dr Salter said. "We need to reject industry claims that they cannot keep kids safe on the platforms. We need to reject the industry claim that it is 'up to parents' to police children's behaviour." The eSafety Commissioner Julie Inman Grant shares these concerns (Fitzsimmons 2019).

Some digital platform providers will be recalcitrant in the absence of regulatory measures including meaningful penalties for non-compliance and powers of enforcement. Additional sanctions are warranted where Big Tech corporates defy community expectations and ignore the real harm caused by child sexual exploitation.

We support initiatives to compel compliance. Minister for Home Affairs, Peter Dutton (2019), in an address delivered at the Global Summit to Tackle Online Child Exploitation in Ethiopia stated:

> *We prefer to collaborate on a voluntary basis and appreciate industry partners who are willing to come to the table without legal incentive. However where providers are unwilling to comply, the legislation ensures that we will not be deprived of the ability to enforce our*

laws... We believe the fundamental right of a child to be safeguarded from sexual harms trumps a paedophile's "right to privacy."

Commendably, some tech companies have made significant efforts to identify, report and rid illicit content from their platforms, including by working with law enforcement agencies, but more still have to pledge to support online safety. And there's an inherent contradiction between this behaviour and intentions of some companies to adopt end-to-end encryption.

Sanctions for companies which do not care about community wellbeing and refuse to abide by agreed Corporate Social Responsibility and ethical standards are necessary.

We recommend that the Committee urge States to ensure these policies are developed by digital platforms and ISPs:

- **Apps and services must protect all minors from being direct messaged by adults.**
- **Privacy settings should be more visible to increase awareness of safety tools.**
- **Digital services should automatically provide children with maximum data protection whenever they download a new app, game or visit a website, as proposed in the UK.**
- **Privacy settings should be set at maximum by default.**
- **Nudge techniques should not be used to encourage children to weaken their settings.**
- **Location settings should be switched off by default.**
- **Data collection and sharing should be minimised and profiling which can allow children to be served up targeted content should be switched off by default.**
- **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.**
- **Include links in safety sections to define sexual harassment, and how to get help.**
- **Revise 'Community Standards' so that all sexualised, predatory and grooming-style comments (text, slang, short-hand, hashtags, emojis and graphics) qualify as violations.**
- **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.**
- **Prohibit adults from using 'live' posts to contact minors.**
- **Update systems used to detect and remove sexualised, predatory comments.**
- **Recognising that social media 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 platforms.**
- **Stop algorithms such as the 'explore' feature from promoting minors' pages and connecting predators with children.**
- **Investigate parasite pages which are exclusively devoted to republishing photos of minors; delete pages where children are sexualised, harassed, groomed or where any type of predatory comments/behaviour is displayed.**

- **Prohibit the republishing of images of minors on pages that also feature porn-style images of adults.**
- **Prohibit the promotion of paid content which includes images and videos of minors available on private websites or other content sharing platforms including Patreon, Boosty and OnlyFans.**

38. Regulatory frameworks, industry codes and terms of service

We caution against reliance on industry self-regulation, having publicly exposed and documented several major failings in the Australian context:

- The failure of industry self-regulation in advertising has served the vested interests of business ahead of the wellbeing of the community (Collective Shout 2011-2020; Kennedy 2019)). Despite parliamentary inquiries hearing evidence of the need for systemic reform—including the need for a co-regulatory system—self-regulation has failed to halt or even hinder the proliferation of hyper-sexualised imagery and messaging (Kennedy 2020).
- The failings of Classification systems allowed illegal animated CSEM depicting child rape, abuse and exploitation to be classified as suitable for audiences as young as 15—in some cases even younger (Lisziewski 2020).
- Attempts to require online pornography platforms to require proof of age to help protect minors from exposure have failed due to organised opposition by industry (Alison 2020).
- ISPs and Telcos failed to protect children by facilitating Live Distant Child Abuse (Tankard Reist 2017).
- Replica, life-like children, infant and baby sex abuse dolls are being sold through e-commerce platforms Alibaba, eBay, Etsy, and Amazon (Collective Shout 2020; Roper 2020).

Recommendations:

- **The UN investigate sanctions against global corporations which profit from hosting/facilitating direct and indirect sexual exploitation of children including the sex industry (for example Pornhub), e-commerce platforms and ISPs/Telcos.**
- **The UN explore best practice legislation to rein in corporates which profit from child exploitation and develop legislative measures for States to ensure consistency in a global interconnected environment.**

55. Protecting children from harmful material

As mentioned above, Collective Shout has lobbied for age verification systems to protect children from exposure to pornography (Alison 2019). This strategy is supported by the majority of parents (British Board of Film Classification 2019). When innocuous activities like key-stroke errors and searches for cartoon characters can lead children inadvertently to pornography sites, parents and carers have little hope of protecting them (Roper 2018). The powerful multi-billion dollar porn industry has so far successfully blocked any attempt to implement this basic protection.

Recommendation:

States to introduce age verification measures to protect children from pornography exposure.

57. 84. 85. 86. 121. End-to-End Encryption and other safety measures

According to Australian Federal Police, paedophiles are "fuelling the market for online footage of children being tortured and murdered" (Schliebs 2019; Grigg and Chenoweth 2019). Collective Shout has taken a strong position on the prevention and prosecution of LDCA, highlighting grave harms to children in this growing crime (Tankard Reist 2017). We were recently invited to become part of the Australian Centre to Counter Child Exploitation (ACCCE) working group to address child exploitation (Kennedy 10 Sep 2020).

ISPs and Telcos provide the infrastructure for live-streaming abuse of children. We support the recommendation of Kevin Hyland OBE (UK's first Independent Anti-Slavery Commissioner 2014-2018):

> *With the increase of online trafficking, particularly for cybersex, legal instruments are long overdue to require those who supply and provide the internet 'virtual highways' to guarantee they will control the traffic and materials that transmit across their systems. This should be part of a legally binding framework and should be linked to the provision and upgrading as service providers seek to win contracts to supply 5G technology, which is expected to move to an even higher generation version in the near future. (Hyland 2019)*

We support the recommendations in the open letter signed by UK Home Secretary Priti Patel, US Attorney General William Barr, Acting US Homeland Security Secretary Kevin McAleenan, and Australian Minister for Home Affairs Peter Dutton, raising concerns about Facebook's plan to build end-to-end encryption into its messaging apps (Patel et al. 2020). If the plan goes ahead, it will prevent law enforcement agencies from finding illegal activity–including CSEM—shared via Facebook. The signatories called on Facebook to prioritise public safety by enabling law enforcement to gain access to illegal content.

A platform which combines "inaccessible messaging services with open profiles, providing unique routes for prospective offenders to identify and groom our children," is a risk to children's safety (Patel et al. 2020). Facebook may lose the ability to report 70% of the cases it currently sends to the National Center for Missing & Exploited Children because it will no longer have access to users' conversations (Brookes 2019).

We also share the views of Rachael Falk, CEO of the Cyber Security Cooperative Research Centre, responding to those who want to keep encrypted messages beyond the reach of authorities (Falk 2020):

> *This argument ignores the fundamental truth that we are just as vulnerable on messaging apps as we always have been on older platforms. The same crooks, fraudsters, pedophiles and terrorists have not restricted themselves to monitorable platforms, they now use messaging apps to plot their malevolent acts. They continue to scam us, defraud us, menace our children and threaten our public safety. Only now the convenience of messaging apps*

allows them to find one another and conspire more easily in a cyber world that is invisible, encrypted and beyond the reach of the law... The idea of privileging online privacy over these people's welfare is mind-boggling....

We also commend to you the Open Letter to the Technology Industry by the National Center for Missing and Exploited Children (2020):

> *... we are alarmed by the continued march toward end-to-end encryption without safeguards for children. We call on you to implement technological solutions that enhance consumer privacy while prioritizing child safety. Robust safeguards should transfer to a child's digital experience in an end-to-end encrypted environment. Without proper protections, children will be even more susceptible to potential online sexual exploitation. And countless survivors of child sexual abuse will continue to suffer knowing images depicting their sexual abuse are being shared with impunity.*

We support the *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*, developed by the Five Country Governments (Australia, New Zealand, Canada, UK, and USA) in consultation with Facebook, Google, Microsoft, Twitter, Snap, and Roblox, and backed by the WePROTECT Global Alliance (Five Country Ministerial 2020). The *Principles* aim to prevent the distribution of CSEM, child grooming and LDCA, however we believe stronger action will be needed to give force to these principles. End-to-end-encryption violates Facebook's commitment to child safety and we support efforts to block it until adequate measures have been taken to ensure children are not placed at greater risk of harm.

We recommend that the Committee urge States to ensure these policies are developed by digital platforms and ISPs:

- **ISPs must guarantee they will control the traffic and materials that transmit across their systems. This should be part of a legally binding framework and should be linked to the provision and upgrading as service providers seek to win contracts to supply 5G technology.**
- **Do not implement end-to-end encrypted communications for accounts where a user has indicated they are under 18 years old, or accounts of known predators.**
- **Implement detection technologies, at least as effective or better than those currently available, to prevent offenders from distributing CSEM.**
- **Adopt technology vetted by the child protection community to identify sexual grooming of children by adults.**
- **Promptly report apparent CSE to NCMEC's Cyber Tipline with actionable information to help rescue child victims and hold offenders accountable.**
- **Ensure that law enforcement can use existing legal processes to effectively investigate the sexual exploitation of children.**

References

Alison C (22 Nov 2019). Submission to Inquiry into Age Verification for Online Wagering and Online Pornography. Collective Shout.
https://www.collectiveshout.org/submission_to_inquiry_into_age_verification_for_online_pornography

British Board of Film Classification (2019). Age-verification for online pornography to begin in July. BBFC.
https://www.bbfc.co.uk/about-us/news/age-verification-for-online-pornography-to-begin-in-july

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/

Collective Shout (2011-2020). Advertising Industry Self-Regulation.
https://www.collectiveshout.org/advertising_industry_self_regulation

Collective Shout (2020). Child Sex Dolls Sold Online by Alibaba.
https://www.collectiveshout.org/child_dolls_alibaba

Dutton P (12 Dec 2019). Address at the Global Summit to Tackle Online Child Sexual Exploitation, Addis Ababa, Ethiopia.

Falk R (21 Feb 2020). We are powerless as evil is encrypted all around. The Australian.

Fitzsimmons C (2 Dec 2019). 'It's like any girl is up for grabs': Instagram a magnet for predators. The Age.
https://www.theage.com.au/technology/it-s-like-any-girl-is-up-for-grabs-instagram-a-magnet-for-predators-20191129-p53fkt.html?cspt=1575249264%7Cd6e880455f15ba3f7814900144d5ec6f

Five Country Ministerial (2020). Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse.
https://www.justice.gov/opa/press-release/file/1256061/download

Grigg A and Chenoweth N (23 Nov 2019). Westpac's Dirty Laundering. The Australian Financial Review.

Hyland K (9 Oct 2019). Submission No. 87 to the Inquiry into Modern Slavery Act 2018 and Associated Matters.
https://www.parliament.nsw.gov.au/lcdocs/submissions/66190/0087%20Mr%20Kevin%20Hyland%20OBE.pdf

Kennedy L (10 Sep 2020). "Australians should be outraged by this offending." Collective Shout.
https://www.collectiveshout.org/_national_child_protection_week

Kennedy L (2 Nov 2020). Submission to AANA Code of Ethics Review. Collective Shout.
https://www.collectiveshout.org/submission_to_aana_code_of_ethics_review

Kennedy L (27 Oct 2020). 'Disrupting the System': New Male Champions report challenges workplace sexual harassment while Honey Birdette Male Champ landlords perpetuate it. Collective Shout.
https://www.collectiveshout.org/malechamps_sexualharassment

Liszewski M (5 Mar 2020). Submission to Review of Australian classification regulation. Collective Shout.
https://www.collectiveshout.org/submission_to_review_of_australian_classification_regulation

Missing Kids (2020). End-to-End Encryption: Principles to Safeguard Children.
https://www.missingkids.org/blog/2020/an-open-letter-to-the-technology-industry

Patel P, Barr WP, Dutton P, Little A and Blair B (2020). International Statement: End-to-end encryption and public safety. Home Office.
https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety/international-statement-end-to-end-encryption-and-public-safety-accessible-version

Roper C (2020). Not a 'Victimless' Crime: How Child Sex Abuse Dolls Facilitate Crimes Against Children. FiLia.
https://filia.org.uk/news/2020/9/10/not-a-victimless-crime-how-child-sex-abuse-dolls-facilitate-crimes-against-children?fbclid=IwAR2tII8kynxHmdZ3ZlxChNc_fQl9Fb9G9lBf13MuDr86ytFc7I-2p6tTfPY

Roper C (9 Mar 2018). Parents vs the Porn Industry Isn't a Fair Fight. Huffington Post.
https://www.huffingtonpost.co.uk/entry/parents-vs-the-porn-industry-isnt-a-fair-fight_uk_5aa0df69e4b0ef2aaff70489?guccounter=1

Schliebs M (23-24 Nov 2019). Aussies fuel pedophile video surge, The Weekend Australian.

Tankard Reist M (6 Jul 2017). Why are Australian Telcos and ISPs Enabling a Child Sexual Abuse Pandemic? ABC Religion and Ethics.
https://www.abc.net.au/religion/why-are-australian-telcos-and-isps-enabling-a-child-sexual-abuse/10095644