Online Safety Legislative Reform

Submission

Collective Shout

February 2020

Contents

1PO Box 781, Neutral Bay, NSW 2089 ABN 30 162 159 097 e team@collectiveshout.org www.collectiveshout.org

Introduction

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.

Collective Shout welcomes the opportunity to contribute to Online Safety legislative reform. We support intentions to consolidate and harmonise current laws and to ensure streamlining and consistency in a range of digital offences. We are especially pleased to see plans for an expansion of protection against cyberbullying, cyber abuse, image-based abuse[1] and seriously harmful content. As the digital landscape is in a constant state of flux, new opportunities arise – and with them new dangers. This necessitates updated legislation to ensure a safer online environment prioritising human rights and community welfare.

Our recommendations relate primarily to our work combatting the objectification of women and sexualisation of girls, the damaging impacts of pornography on the developing sexual templates of young people, the sexual grooming and exploitation of minors, sexual abuse especially of children for Live Distant Child Abuse, and cyber abuse including of women (of which our team is unfortunately well familiar; see for example Roper, 2014).

Whether they be global billion dollar companies or small startups, any digital platform must be expected to take down harmful material when alerted, respond quickly to cyberbullying on their platform, and empower users to report harmful content. We refer to the United Nations Guiding Principles on Business and Human Rights (2011), the foundational principle of which is to respect human rights (Principle 11). Businesses, including social media companies and internet service providers, should "avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur." Furthermore, they should "seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts" (Principle 13).

With regard to harmful content, it is unfortunate that a clear definition of "menacing, harassing or offensive" content is not provided in the discussion paper. There must be no leeway for digital platforms to perpetrate or facilitate harm with impunity. The definition should be expanded to at least include the terms 'harmful' and 'exploitative'.

We strongly support all proposals in the Online Safety Reform discussion paper that strengthen the capacity of Australia's regulator to deal with digital technologies and to hold businesses accountable for the harm they cause or facilitate. Global support is growing for the empowerment of internet regulators, and Australia's eSafety Commissioner is a model for how this can be achieved, but more must be done as new developments with harmful potentials constantly emerge (Miller, Ohrik-Stott and Coldicutt 2018, UN 2011).

We note that the empowerment of a State regulator was *not* identified as a strategy framework by the Alliance to Better Protect Minors Online (2020) which includes signatories such as Facebook, Google, Disney and Microsoft[2]. Instead, these global mega corporations prefer to focus on 'user

[1] New research reveals that image-based sexual abuse has grown in Australia: in 2016, 1 in 5 respondents had experienced it, but in 2019 it rose to 1 in 3 (Powell, Scott, Flynn and Henry 2020).

[2] Signatories include ASKfm, BT Group, Deutsche Telekom, Disney, Facebook, Google, KPN, The LEGO Group, Liberty Global, Microsoft, Orange, Rovio, Samsung Electronics, Sky, Snap, Spotify, Sulake, Super RTL/Mediengruppe RTL Deutschland, TIM (Telecom Italia), Telefónica, Telenor, Telia Company, Twitter,

empowerment', 'enhanced collaboration', and 'awareness-raising' (Alliance to Better Protect Minors Online, 2020). However in our years of lobbying and advocacy for corporate social responsibility and ethical corporate behaviour, we have pointed out many times that these approaches along with 'self-regulation' - without government or independent regulatory or at least co-regulatory oversight - fail to meet the necessary benchmarks to protect vulnerable members of the community (Roper 2016). Over the past decade we have documented multiple examples of failures of the advertising industry to self-regulate[3] and have made submissions to Parliamentary inquiries in an attempt to have this addressed.[4] Facebook now appears to acknowledge that regulators are needed to help digital platforms reduce harm (Bickert 2020).

Evidence provided to the recent Inquiry into Age Verification for Online Wagering and Online Pornography (Tankard Reist 2019, Collective Shout 2019) demonstrated some of the harms to young people accessing pornography online:

- Researchers have found that sex offences by school-aged children have quadrupled in Australia in four years, and authorities attribute this to children's exposure to pornography. 75% of 7 to 11-year-old boys and 67% of 7 to 11-year-old girls in treatment for problem sexual behaviour reported early sexualisation through online pornography (Etheredge and Lemon 2015).
- A meta-analysis involving 59 studies and around 17,000 adolescents found those who offended were significantly more likely to have had early exposure to pornography, and to report higher rates of exposure to pornography (Seto and Lalumiere 2010).
- The late Emeritus Professor Freda Briggs AO wrote a disturbing submission to the 2016 Senate Inquiry into the harm being done to Australian children through access to pornography on the internet, drawing links between pornography and child sex abuse, paedophilia and child-on-child sex abuse (Briggs 2015).

Vivendi, Vodafone. Associated members are BBFC, Child Helpline International, COFACE, eNACSO, EUN Partnership, FFTelecoms, FOSI, Foundation T.I.M. (Against Internet Misconduct), FSM, GSMA, ICT Coalition, NICAM, Toy Industries of Europe, UNICEF.
https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online

[3] See Collective Shout's tag "Ad Standards Panel complaints dismissed" here:
https://www.collectiveshout.org/tags/ad_standards_board_complaints_dismissed

[4] Collective Shout (2018). Submission on the Enhancing Online Safety Act 2015 and Online Content Scheme Reviews.
https://d3n8a8pro7vhmx.cloudfront.net/collectiveshout/pages/2966/attachments/original/1535966033/Submission_on_the_%E2%80%8BEnhancing_Online_Safety_Act_2015_%E2%80%8Band_Online_Content_Scheme_Reviews.pdf?1535966033 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

- In 2016 the Australian Institute for Family Studies (Campo 2016) summarised the research evidence on the harmful effect of children's exposure to pornography as indicating that frequent and routine viewing of pornography and other sexualised images may:

  - ●reinforce harmful gender stereotypes;
  - ●contribute to young people forming unhealthy and sexist views of women and sex;
  - ●contribute to condoning violence against women;
  - ●be associated with sexually coercive behaviour by young men;
  - ●normalise sexual violence;
  - ●contribute to unrealistic understandings of sex and sexuality;
  - ●shape social norms around sex;
  - ●lead to young people feeling as though they should engage in the sexual behaviour frequently displayed in pornography, including violent acts;
  - ●be associated with pressure being put on girls to share naked images of themselves online;
  - ●influence young people's self-concept and body image; and
  - ●be linked to problematic sexual behaviour and sexual abuse among children and adolescents.

While Collective Shout has worked to help parents and caregivers protect young people in their care, we have also pointed out that an all-of-community response is needed to have any real effect, given the massive nature of the threat posed.[5] Global platforms, and too often government and regulatory bodies, have offloaded their ethical responsibilities, to the detriment of individuals, families and the community. Any new legislation must substantially raise the bar for corporate responsibility on the part of global businesses that control and oversee our online connections and relationships. As the UK Carnegie Trust states (2018):

> *Harm is protested not by well-funded companies but by individuals and a civil society lobby that are dispersed, represent a myriad of different perspectives, are short on resources and lack access to the levers of power. ...*
>
> *The social media companies, now some of the biggest firms in the world, have learned from previous cycles of disruption and regulation and have built strong lobbying positions. The net result appears that the lobby to regulate social media is*

[5] 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

more vocal, but less effective than the economic interests that campaigned during previous disruptive waves…

Summary of Recommendations

Collective Shout supports the proposed regulatory policy changes.

However, based on our grassroots activism and collection of evidence, we believe much more needs to be done to protect minors on digital platforms. We additionally recommend that:

- The BOSE should adopt the recommendations from the #wakeupinstagram campaign in which we are a global partner:
    - Strengthened requirements that apps and services protect all minors from being direct messaged by adults.
    - Algorithms, overseen by human moderators, should be included to proactively remove sexualising or sexually graphic comments on minors' images and posts.
    - Privacy settings should be much more visible in order 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 to high by default. Nudge techniques should not be used to encourage children to weaken their settings. Location settings should also be switched off by default. Data collection and sharing should be minimised and profiling that can allow children to be served up targeted content should be switched off by default (Information Commissioner's Office 2020).
    - 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 pedophile 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 the 'explore' feature from promoting minors' pages and connecting predators with children.

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

- Sexual grooming and exploitation should be a distinct category of online harm.
- The BOSE should use an age-specific approach to internet safety, recognising that minors have unique needs and vulnerabilities.
- Children's rights should be understood in the context of the Convention on the Rights of the Child, with special reference to Article 34.
- Privacy and problems caused by encryption should be included in the scope of this legislative reform.
- Transparency reporting should include the requirement to report on the qualitative nature of complaints and responses, rather than merely the quantity of complaints and takedowns.
- For companies which fail to meet the BOSE, we recommend additional sanctions. For companies such as PornHub who repeatedly and knowingly allow seriously harmful content and image-based sexual abuse on their platform, we recommend that Australian ISPs be required, subject to penalties, to block all access.
- A clear definition of "menacing, harassing or offensive" material be provided for this legislation to move forward, with an expansion of the definition to include the terms 'harmful' and 'exploitative'.
- More focus on human oversight of algorithms, so that algorithms are monitored by actual humans, and final decisions in takedowns or blocks are made by humans. This would help to understand the meaning of suggestive comments and emojis that are currently not being picked up by algorithms.
- The eSafety Commissioner should have an expanded function of conducting or commissioning independent research into the prevalence and causes of technology-related impacts.
- The BOSE should encourage the development and provision of more stimulating quality content online for young people.

Current Approach

1. Are the proposed high level objects appropriate? Are there any additions or alternatives that are warranted?

We suggest four additions.

(a) Within the category of 'seriously harmful material', **sexual grooming and exploitation of minors should be addressed as a distinct category**. Such behaviour is currently not being addressed under the category of cyberbullying. We note that this is referred to on page 12

of the Discussion Paper under "online harms", and also implied in the discussion of BOSE particularly regarding restrictive privacy and safety settings for apps, games and services marketed to children on page 23.

(b) The BOSE should specify **an age-specific approach to internet safety**, as one in three internet users in the world are under 18, and children have unique needs and vulnerabilities as explained by Livingstone, Carr and Byrne (2016):

> *This paper specifically argues against an age-generic (or 'age-blind') approach to 'users', because children have specific needs and rights that are not met by governance regimes designed for 'everyone'. Discussions about users in general embed assumptions about their being adults. ...*
>
> *While this paper certainly does not advocate for identical policy approaches across infancy, childhood and adolescence, it argues that the legal status of children below the age of 18 should be distinctively recognized and addressed. This is because:*
>
> - *They are legal minors and so cannot enter into contracts or licenses, explicit or implicit (as often occurs on the internet), nor are they easily able to seek redress or have redress sought against them;*
> - *They often use online services not targeted toward them but rather to adults, or where site or service providers are unaware or negligent of their status;*
> - *They have particular educational and informational needs that are not readily met through provision for the general population;*
> - *They can be particularly vulnerable to sexual exploitation and abuse, which includes not only violent behaviour, but also any sexual activity with children below the age of consent;*
> - *They lack sufficient internet (and other) literacies to fully grasp the demands and norms of the online environment (where buyer beware generally holds sway over seller beware) and*
> - *They (and their parents) generally do not understand the data collected from them or otherwise held concerning them, whether directly or indirectly (as 'big data'), nor is provision made specifically to inform them or to provide redress.*

c) Children's rights should be understood in the context of the Convention on the Rights of the Child, with reference to Article 34:

> *States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent: (a) The inducement or coercion of a child to engage in any unlawful sexual activity; (b) The exploitative use of children in prostitution or other unlawful sexual practices; (c) The exploitative use of children in pornographic performances and materials.*

A pertinent example of internet policy being made for adults rather than children is the recent debate on age verification for online access to pornography.[6] The most vocal opponents of the proposal were concerned not with children's rights not to be exposed to pornography, but with adults' rights not to have their pornography-viewing habits potentially exposed.

(c) BOSE should be required to develop **more stimulating quality content online for young people** as put forward in the first pillar of the Better Internet for Kids Policy Map for European Union Member States, recognising the social and commercial benefits that can arise from this strategy (O'Neill and Dinh, 2018).

(d) **Privacy, and the problems caused by encryption technologies, should be included in the scope of this legislative reform**. It is an integral component of online safety. We share the views of Rachael Falk (2020), CEO of the Cyber Security Cooperative Research Centre, responding to those who want to keep encrypted messages beyond the reach of authorities:

> *"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… we wouldn't respect the privacy of a neighbor whose home was turned over to producing meth or child pornography, so we shouldn't respect the privacy of our digital neighbours who – evidence tells us – carry on the same conduct every day….The idea of privileging online privacy over these people's welfare is mind-boggling…".*

We commend to you the Open Letter to the Technology Industry by MissingKids.org (2020):

> *At the National Center for Missing & Exploited Children 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*

[6] Collective Shout (2019). *Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs Inquiry into age verification for onlinewagering and online pornography.* https://d3n8a8pro7vhmx.cloudfront.net/collectiveshout/pages/3258/attachments/original/1575331635/Age_Verification_Submission.pdf?1575331635 Tankard Reist, M. (2019). *Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs Inquiry into Age Verification for Online Wagering and Online Pornography*. Submission 177 at https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Submissions

countless survivors of child sexual abuse will continue to suffer knowing images depicting their sexual abuse are being shared with impunity.

We appeal to you to adopt the following Principles to Safeguard Children in End-to-End Encrypted Environments:

- *Do not implement end-to-end encrypted communications for accounts where a user has indicated they are under 18 years old.*
- *Implement detection technologies, at least as effective or better than those currently available, to prevent offenders from distributing child sexual abuse material.*
- *Adopt technology vetted by the child protection community to identify sexual grooming of children by adults.*
- *Promptly report apparent child sexual exploitation to NCMEC's CyberTipline with actionable information to help rescue child victims and hold offenders accountable.*
- *Ensure that law enforcement can use existing legal process to effectively investigate the sexual exploitation of children.*

Basic Online Safety Expectations (BOSE)

3. Is there merit in the BOSE concept?

We support the BOSE concept.

With regard to the safety of children online, we emphasise that online activity can lead to real physical dangers. Grooming, trafficking and abuse of women and children are some of the most urgent realities impinging on human rights.

What human rights are at stake? As an example, Article 34 of the Convention on the Rights of the Child (United Nations 1989) requires that:

> *States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:*
>
> *(a) The inducement or coercion of a child to engage in any unlawful sexual activity;*
>
> *(b) The exploitative use of children in prostitution or other unlawful sexual practices;*
>
> *(c) The exploitative use of children in pornographic performances and materials.*

On this basis, we commend to you the current campaign #wakeupinstagram, spearheaded by advocacy organisations in three countries: Collective Shout (Australia), National Center on Sexual Exploitation (USA), and Defend Dignity (Canada).

The recommendations in this campaign should also be part of the BOSE concept, as described in the next section.

4. Are there matters (other than those canvassed in the Charter) that should be considered for the BOSE? Are there any matters in the Charter that should not be part of the BOSE?

In line with our #wakeupinstagram campaign, we recommend an additional focus on grooming and exploiting children on social media networks.[7] There are several safety features that can be included to make social media platforms safer for children. The main problems are as follows:

- According to survivor testimony, sex traffickers and child predators appear to be increasingly using Instagram to identify, groom, and exploit children.
- Minors whose Instagram or TikTok accounts are set to private can still receive unsolicited direct messages from strangers, which has led to several instances of sex trafficking and child sexual abuse.
- We have documented large numbers of comments by predatory adults on the photos of minors, where they leave sexually graphic comments, sexualize children, or solicit naked images and proposition sex acts from children.
- Additionally, on popular social media platform TikTok, children are being bombarded with sexually explicit messages, and kids as young as eight are being groomed (Rouse 2020).

Collective Shout Campaigns Manager Melinda Liszewski (2019b) wrote about her work in collecting hundreds of examples of explicit, sexual comments on girls' photos on Instagram:

> *They say things like "please open your legs" and describe in detail exactly how they want to rape them. They ask for more photos, more videos and tell the girls to "check your DMs" (Direct Messages).*
>
> *Some of these accounts appear to be run by adolescent girls who post photos of themselves doing gymnastics or ballet. We've also seen many accounts that are "managed by mum"*

[7] See Collective Shout's press releases: *Instagram a 'predator's paradise': Collective Shout joins anti sexploitation groups in global campaign (21st November 2019)* https://www.collectiveshout.org/wakeupinstagram. *Why is Instagram letting men share sexual fantasies about 7 year old girls?* (23rd November 2019) https://www.collectiveshout.org/predators_on_girls_insta_accounts *No Facebook, you're not doing enough to protect children.* (23rd November 2019) https://www.collectiveshout.org/facebook_instagram_response *Insta must act on predators: Collective Shout letter to platform heads.* (5th December 2019) https://www.collectiveshout.org/insta_must_act_on_predators_collective_shout_letter_to_platform_heads

> *under the guise of "child modelling." Their daughters are labelled "influencers" and "supermodels" and some are signed to modelling agencies.*
>
> *Some parents sell photos of their daughters in bikinis dancing, blowing kisses and washing the dog. They offer tiered subscriptions providing more "exclusive content" to men who sign up and pay a monthly fee. I've reported these accounts but Instagram tells me they don't violate their "community guidelines." By allowing these accounts to flourish, Instagram has effectively partnered with the account holders in carrying out the sexual exploitation of a child (Liszewski 2019b).*

Utilising the established complaints process often does not help:

> *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." (Alison 2019)*

And arguing that the sheer volume of content prevents Instagram from monitoring it is unconvincing:

> *Instagram isn't even using adequate reactive let alone proactive technology. Technology isn't much use if Instagram's community guidelines allow for adults to sell sexualised photos of minors and men to post photos of little girls that appear to be unlawful. Instagram is one of the fastest growing social media platforms in the world and is estimated to be worth $100 billion. Instagram, how about putting some of those billions into protecting children on your platform? (Liszewski 2019)*

Sex trafficking is facilitated on social media platforms. The Online Safety Act is a great opportunity to address it:

> *"Sex traffickers are social-media savvy, Krebs said. The majority of cases MSP investigates are unfolding on Snapchat, Kik and other messaging apps, she said." ... Victims are manipulated by people they already knew. The promise of a romantic relationship is used as a grooming technique. Police call this "boyfriending," Krebs said. (Moore 2020)*

Here is an example of how it plays out:

> *"This "young and cute boy" to whom Maria had sent her sexually explicit images was not a boy at all. He was an adult man who promptly used these graphic photos to blackmail Maria. He threatened to send Maria's sexually explicit photos to her parents and to all her classmates if she didn't have sex with him and then with others. Maria felt trapped. Before she knew it she was a victim of sex trafficking and was being sold to one stranger after another. This went on for three months, while she was still living in her parent's home, until she finally gathered the courage to tell someone and get help." (NCOSE 2019)*

In a letter from Collective Shout to Instagram Global Head of Policy (2019), Melinda Liszewski writes:

> *The evidence we have gathered demonstrates the sexual exploitation of underage girls on Instagram. Your company is allowing predators almost unfettered access to them. Content hosted on your platform violates their right to grow up free from activity that harms them (United Nations Convention on the Rights of the Child, Article 36). Because of how common predatory behaviour has now become on Instagram, girls learn to think of it as normal which sets them up for even more harm.*
>
> *We urge Instagram to prioritise this issue and act in a way that places the wellbeing of vulnerable young people above the interests of predators and reflects accepted standards of corporate social responsibility and ethical behaviour.*

The eSafety Commissioner Julie Inman Grant and Associate Professor Michael Salter share the same concerns (Fitzsimmons 2019):

> *Michael Salter, associate professor of criminology at the University of NSW, said social networks should keep minors in a "walled garden" similar to the new YouTube Kids for children aged 12 and under. He said 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."*

Cybersafety expert and Collective Shout ambassador Susan McLean says that TikTok also has been known to fail to remove suspicious accounts even after being warned they could be run by a child groomer: "TikTok does not have the same safety sessions as some of the more well-known apps and routinely do not remove accounts that have been flagged as potentially a predator" (Rouse 2020). TikTok has rapidly become equally notorious for grooming, bullying, and privacy concerns.

Recommendations that should be included in Australia's BOSE based on our #wakeupinstagram campaign:

- Strengthened requirements that apps and services protect all minors from being direct messaged by adults.
- Algorithms, overseen by human moderators, should be included to proactively remove sexualising or sexually graphic comments on minors' images and posts.
- Privacy settings should be much more visible in order 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 to high by default. Nudge techniques should not be used to encourage children to weaken their settings. Location settings should also be switched off by default. Data collection and sharing should be minimised and profiling that can allow children to be

served up targeted content should be switched off by default (Information Commissioner's Office 2020).

- When an account is set to 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. NCOSE has found that many teens and adults are unsure how to define sexual harassment, and are also unsure how to deal with it. Sexual harassment includes but is not limited to, unwanted sexual advances or attention including physical actions, speech that is sexually provocative, and unsolicited sending of or requests for pornography or nude images/videos. Recent research shows that less than half of respondents in Australia, New Zealand and the UK are aware it is a crime to share intimate images without their consent (Powell, Scott, Flynn and Henry 2020).
- Revise 'Community Guidelines' 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.
- Prohibit adults from using 'live' posts to contact minors.
- Update Instagram's system used to detect and remove sexualised, predatory comments.
- Recognising that Instagram serves as a supply source of images of children for web-based pedophile 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.
- Stop the 'explore' feature from promoting minors' pages and connecting predators with children.
- 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.
- Prohibit the republishing of images of minors on Instagram pages that also feature porn-style images of adults.

5. What factors should be considered by the eSafety Commissioner in determining particular entities that are required to adhere to transparency reporting requirements (e.g. size, number of Australian users, history of upheld complaints)?

We support the concept of requiring transparency reporting requirements for any entity that has a history of upheld complaints.

Although we have little information about the details of the proposed transparency reporting requirements, we would advocate for expanded requirements to report on the nature and quality of complaints and responses, rather than merely the quantity. Transparency reporting of extremist and violent content was proposed in 2019 by the Australian Government at G7 to include data on

number of items removed after being reported, the proportion removed before users engage with them, and average time in which action is taken (Miller 2019). In our view, transparency reporting requires more useful detail than this.

Currently, Facebook and Instagram transparency reports appear more like public relations materials. As MacKinnon and Wingfield (2019) explain, "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.

It is encouraging that Mark Zuckerberg has very recently flagged the possibility that Facebook may open up its content moderation systems for external audit (Zuckerberg 2020). TheOnline Safety legislative reform could push for this to be actualised.

6. Should there be sanctions for companies that fail to meet the BOSE, beyond the proposed reporting and publication arrangements?

Collective Shout has had significant success with our strategy of publicly identifying companies which engage in exploitative practices. Therefore we believe the reporting and publication arrangement has potential to be successful to some extent. Australian Federal Police Commissioner Reece Kershaw is also prepared to name and shame tech companies who refuse to cooperate with federal agencies to protect children online (Lewis 2020).

However - as is demonstrated by the self-regulated advertising industry - some companies make a public show of refusing to abide by community standards. For example, Honey Birdette refuses to take down advertising that violates the ad industry's Code of Ethics , highlighting the fact that Ad Standards - the overseeing body responsible for handling advertising complaints from members of the public - has no power to enforce community expectations. This demonstrates the limited effectiveness of a 'name-and-shame approach' for those corporations for whom ethics have little to no role in their operations (Alison 2020).

Between February 2018 and May 2019, 23 Honey Birdette ads were found in breach of Australian Association of National Advertisers' Code of Ethics (the total number of breaches is now 42). Honey Birdette either ignores the rulings, or responds with mockery toward those who make complaints. Honey Birdette and its shopping centre landlords continue to act in violation of community standards and human rights - the Australian Human Rights Commission definition of sexual harassment includes 'unwanted exposure to sexualised imagery'. Over the Christmas period, property companies - including those whose CEO's identify as 'Male Champions of Change' who pledge to work to end sexism (Kennedy 2019) - continued to host Honey Birdette's explicit and objectified portrayals of women in their 'family-friendly' shopping centres, including full-size window

displays just metres from where children had their photos taken with Santa and others serving as the backdrop to a children's Santa parade.[8]

Over a period of 10 years, Wicked Campers also refused to respond to widespread community pressure to remove their offensive and sexually degrading slogans from its vans. In 2019, State Transport ministers announced a nation-wide approach that will give each State powers to deregister vehicles with offensive imagery and slogans, a move that highlighted the need for legislation to bring recalcitrant companies into line.

It is our view that some digital platform providers will be similarly recalcitrant in the absence of regulatory measures including meaningful penalties for non-compliance and powers of enforcement. Additional sanctions are warranted in such cases where businesses defy community expectations and ignore the real harm caused by sexual exploitation in its myriad forms.

Australia has the capacity to address harmful content on the internet. We support any moves to 'compel' compliance. Minister for Home Affairs, Peter Dutton, in an address delivered at the Global Summit to Tackle Online Child Exploitation in Ethiopia (2019) 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 also have a further Bill before our Parliament which, once passed, will allow us to hold online service providers to account for facilitating access to child abuse material. Previously, we could only prosecute individuals who explicitly accessed such content…*
>
> *For the like-minded nations committed to this objective, there's an overwhelming desire to partner with industry. We want industry to cooperate with us willingly, but it is clear that many companies have no intent to meet their moral obligations without being forced into it by legislation.*
>
> *We will compel their assistance because we put the protection of children above the greed and arrogance of some CEOs. 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."*

[8] See Collective Shout's records of Honey Birdette violations at https://www.collectiveshout.org/honey_birdette

Beyond naming and shaming, we hope to see sanctions for those companies who do not care about community wellbeing and refuse to abide by community and ethical standards.

For companies such as PornHub who repeatedly and knowingly allow seriously harmful content and image-based sexual abuse on their platform, we recommend that Australian ISPs be required, subject to penalties, to block all access. Otherwise any online safety regime will remain ineffective.

Cyberbullying Schemes

7. Is the proposed expansion of the cyberbullying scheme for children to designated internet services and hosting services, in addition to relevant electronic service and social media services, appropriate?

Collective Shout believes that the proposed expansion of the cyberbullying scheme is appropriate.

We note that this is not a strategy favoured by big tech businesses, as discussed back when the eSafety Commissioner first proposed the children's cyberbullying scheme:

> *In a submission from the Australian Interactive Media Industry Association (AIMIA) — which includes companies such as Facebook, Google, Yahoo, Twitter, Microsoft, and eBay — obtained by ZDNet, the group said that by appointing a chief bureaucrat to decide what can and can't be removed from social media, it would likely slow down the processes social media sites already have in place for removing harmful content, and could take up to five days to see content removed.*
>
> *It could also see children move to other platforms that are not subject to the same rules, the association said.*
>
> *In a separate submission on its own, Facebook said that it might even take weeks for content to be removed through the eSafety Commissioner process.*
>
> *"The scheme contains multiple steps that would seemingly take at least several days, if not a week, to progress through before the Commissioner issues a content removal order."*
>
> *Facebook also warned that legislating to require removal of content deemed harmful to children could be misused.*
>
> *"The proposed test is 'material targeted at, and likely to, cause harm to an Australian child' could apply to many types of content that young people share online, tagging their friends, which their parents and the eSafety Commissioner do not consider is appropriate," a Facebook spokesperson said.*

"It could potentially, for example, apply to a video game walk-through of Grand Theft Auto that one person posts and then tags their friend in, or it could apply to photos of planking that are shared, tagging friends.

"Rather than enhance the online safety of young people, the scheme has potential to legislate intergenerational conflict rather than encouraging conversations between parents and young people." (Taylor 2014 March 10)

We are wary of these various excuses to avoid regulation by big tech companies. At that time, the Institute of Public Affairs (IPA) did not believe there was any such thing as 'cyberbullying' and thought that the cyberbullying proposal was simply censorship against individual acts of expression (Taylor 2014 March 10).

However, it is our experience that the wider community is easily able to understand how the internet has allowed bullying to take new forms, hence 'cyberbullying', and that freedom of expression cannot be an excuse to allow bullying to continue.

8. Is the proposed take-down period of 24 hours reasonable, or should this require take-down in a shorter period of time?

A time frame of 24 hours is a reasonable takedown period.

Establishing a new cyber abuse scheme for adults

11. Is the proposed application of the cyberbullying and cyber abuse schemes to designated internet services and hosting services, relevant electronic service and social media services, appropriate?

Collective Shout supports the proposal of expanding the cyberbullying and cyber abuse schemes to more digital platforms.

12. Is the proposed take-down period of 24 hours reasonable, or should this require take-down in a shorter period of time?

Collective Shout supports the take-down period of 24 hours.

13. Do the proposed elements of a definition of adult cyber abuse appropriately balance the protection from harms with the expectation that adults should be able to express views freely, including robust difference of opinion?

Collective Shout believes it is urgent that a clear definition of "menacing, harassing or offensive" material be provided for this legislation to move forward, and that the reference should be expanded to include the terms 'harmful' and 'exploitative'.

Non-consensual sharing of intimate images (image-based abuse)

16. Is the proposed take-down period of 24 hours reasonable, or should this require take-down in a shorter period of time?

Image-based abuse is on the increase in Australia and globally, with severe consequences for victims, and little public understanding of the criminal nature of these actions (Powell, Scott, Flynn and Henry 2020).

It is our view that 24 hours is reasonable take-down time, but we hope that such an urgent matter can be resolved even more quickly, given how quickly intimate images can be spread.

18. What additional tools or processes, in addition to removal notices, could be made available to the eSafety Commissioner to address image-based abuse being perpetrated across the full range of services used by Australians?

We recommend action be taken against companies hosting user-generated content which repeatedly allow (and profit from) image-based abuse.

This is especially important in light of recent revelations that Girls Do Porn, a porn production company, had coerced young women to perform for pornographic films and then had distributed them without consent. The owner was charged with sex trafficking crimes and the channel was removed from PornHub.

However PornHub executives must also be brought to account:

> *... even with the official site [Girls Do Porn] shut down and its owners in jail or on the run, the ruling has done little to stop the spread of the videos online. Even today, hundreds of Girls Do Porn videos are easy to find, especially on Pornhub, which claims to get 100 billion video views a year and more than 100 million daily visits. Searching Google for Girls Do Porn videos leads users to Pornhub, where these videos are hosted against pre-roll and banner ads that Pornhub's parent company Mindgeek profits from.*

Pornhub claims that victims of nonconsensual porn—as many of the Girls Do Porn videos are—can easily request to remove videos from the site, and that those videos can be "fingerprinted." Broadly speaking, video fingerprinting is a method for software to identify, extract, and then summarize characteristic components or metadata of a video, allowing that video to be uniquely identified by its "fingerprint." According to Pornhub, this would automatically prevent future attempts to upload a video that was flagged.

But a Motherboard investigation found that this system can be easily and quickly circumvented with minor editing. Pornhub's current method for removing Girls Do Porn videos and other forms of non-consensual porn not only puts the onus of finding and flagging videos almost entirely on potentially-traumatized victims—those victims can't even rely on the system to work. (Cole and Maiberg 2020)

The eSafety Commissioner should develop further strategies to deal with image-based abuse. Image-based abuse is profoundly harmful and also involves callous perpetrators and a normalisation of this abusive behaviour. For example, a new research paper focusing on the perpetrators of image-based abuse, as well as front-line workers engaging with perpetrators on a professional basis, published these disturbing findings (Mortreux, Kellard, Henry and Flynn, 2019):

- Perpetrators demonstrated little remorse and downplayed their actions through minimisation, tending to blame the victim or even deny responsibility.
- With the exception of those involved in taking images of strangers and the taking and sharing of child exploitation images, few were aware that their behaviour was against the law.
- There was a strong sense that on-sharing intimate images without consent was fairly commonplace and becoming somewhat normalised. Some perpetrators highlighted that they were aware of 'numerous people' getting away with similar actions.
- The research also highlights the need to see more action to disrupt the normalising culture around image-based abuse.

Addressing illegal and harmful online content

We must reject the argument that social media businesses are not responsible for the content they make available.

"... the role of platforms in relation to content has changed in recent years... online platforms are no longer entirely neutral in hosting and making available content online. Many platforms use algorithms which determine the manner and order in which content is available, make recommendations to users to access certain content, and promote targeted advertising. Many platforms also proactively monitor content to make decisions about its compliance with their Terms of Service. As such, they are no longer passive, neutral hosts of content generated by their users. And the greater their involvement in making decisions about the content we see, the greater their impact upon users' right to

freedom of expression and thus the greater their obligations under the Guiding Principles." (Bradley and Wingfield 2018, p9)

Collective Shout does not accept that 'freedom of expression' is the only issue at stake here.

The challenge to freedom of expression is the presence of children and teens online who are uniquely vulnerable to harm from people who intend them harm, or from people who do not care about their well-being. 'Freedom of expression' is precisely the argument used to justify the multi-billion-dollar pornography industry which normalises, eroticises and monetises violence against women and girls.

Predators have become tech-savvy and social media platforms offer limitless opportunities to contact and groom children:

Criminal offenders are highly skilled at exploiting new modes of communication to gain access to children and young people, and children and young people can easily access adults-only material if there are no protective mechanisms in place (Queensland Police, 2014).

Education and empowerment of children are not enough on their own. Children do not sufficiently recognise the risks or potential consequences of their actions. We need to implement measures to prevent children from encountering people or materials that mean them harm. We are not talking about protecting children from all unpleasant materials or from all risks, but rather from known and foreseeable harm.

Possible risks include encountering pornography, bullying/being bullied, sending/receiving sexual messages ('sexting') and going to offline meetings with people first met online. Also included, more briefly, are risks associated with negative user-generated content and personal data misuse. However, it is important to note that we also ask how children respond to and/or cope with these experiences. (Livingstone, Haddon, Görzig and Ólafsson, 2010, pp10-11).

Collective Shout's experience in collecting research evidence and the testimonies of children and teens reveals that the harm of being exposed to sexualised and pornographic content is not necessarily just about 'coping' or 'distress'. We must also take into account the impact on children's emerging sexuality and the grooming of children into being sexually complicit with abuse and exploitation.

The definition of 'harmful content' must be carefully discussed. If we cannot agree on a definition, it cannot be addressed. In fact this is central to good governance of the internet, as Mark Zuckerberg has outlined (2020):

It's impossible to remove all harmful content from the Internet, but when people use dozens of different sharing services—all with their own policies and processes—we need a more standardized approach ... Regulation could set baselines for what's prohibited and require companies to build systems for keeping harmful content to a bare minimum.

With regard to harmful content with an age-specific focus, we suggest a focus on the specific harms identified in the Convention on the Rights of the Child (especially Articles 19, 34 and 36), such as physical, mental and sexual violence and abuse, or different forms of exploitation. We know these are all being facilitated right now via the internet and particularly social media.

We hope that there can be a process by which the Australian community can constructively discuss the meaning of harmful content in the near future to give guidance to internet companies, as suggested by FaceBook in its White Paper, *Charting a Way Forward: Online Content Regulation* (Bickert 2020).

19. Is the proposed application of the take-down powers in the revised online content scheme appropriate?

Collective Shout supports the proposed take-down powers in the revised scheme. We see the proposed take-down powers as compatible with and supportive of the desire and will of concerned Australians who recognise the real-life devastation associated with harmful content online.

From our experience in grassroots activism over many years, our supporters tell us we have helped empower them to take action when they see harmful material in the public space. Research from the UK confirms what ordinary people in Australia experience on a daily basis:

> *The public has little voice. Doteveryone's People, Power and Technology research shows there's limited understanding of how digital technologies work, the business models behind them or how to exercise their rights – less than half know their rights when using social media online, or how rules and laws apply on the internet (Miller, Ohrvik-Stott and Coldicutt 2018, p11).*

20. Are there other methods to manage access to harmful online content that should be considered in the new Online Safety Act?

There needs to be more focus on human oversight of algorithms.

Bradley and Wingfield (2018, p22) point out that the benefits of algorithms and automated online content management processes are not well established, with clear evidence of limitations of these tools. The report *Mixed Messages: the limits of automated social content analysis* by the Centre for Democracy and Technology (Duarte, Llanso and Loup, 2017) highlights some of the limitations:

(1) variations in language use across different platforms and depending on topic of conversation,

(2) risks of further marginalising and disproportionately censoring minority or disadvantaged groups,

(3) lack of clear definitions of 'harmful content', 'hate speech', 'extremist material', or 'radicalisation',

(4) different cultural backgrounds and personal attributes of the coders creating the tools, and

(5) inability of tools to take into account context (tone, speaker, forum).

The #wakeupinstagram campaign was launched in November 2019 by The National Center on Sexual Exploitation (USA), Collective Shout (Australia) and Defend Dignity (Canada). Key to the campaign is calling for Instagram to proactively remove sexualizing or sexually graphic comments on minors' photos. Clearly the algorithms are failing to pick up on sexualised emojis, phrases and explicit, suggestive comments, and for the reasons outlined above, human oversight will be necessary to ensure the technology protects girls on Instagram. See the campaign here, with screenshot evidence: https://endsexualexploitation.org/instagram/

Opt-in tools and services to restrict access to inappropriate content

24. To what extent would an expanded accreditation scheme for opt-in tools and services assist parents and carers in mitigating the risk of access by minors to potentially harmful content?

Collective Shout supports any opt-in tools and services that assist parents in mitigating risk of access by minors, but also to assist parents to reduce access *to* minors by adults. We re-emphasise that parental controls and education *cannot be the only strategies used* to protect children and allow them to participate online safely.

Ancillary service provider notice scheme

31. Is there merit in the concept of an ancillary service provider notice scheme?

Collective Shout supports the ancillary service provider notice scheme as an additional tool for protecting internet users from harm. We believe this is essential because some businesses are unconcerned with the harm they cause, and in fact profit from it.

A current example is PornHub. Below we have included the entire text of a petition[9] posted on Change.org in February 2020 by Laila Mickelwait, Director of Abolition for Exodus Cry, and Founder and President of New Reality International. The exposing of PornHub's role in facilitating and

[9] https://www.change.org/p/shut-down-pornhub-and-hold-its-executives-accountable-for-aiding-trafficking

profiting from the exploitation of minors is timely and relevant to this review because it shows what happens when mega platforms like this operate beyond the bounds of regulatory control.

> *In the last few months, there have been several shocking cases of sex trafficking and child rape films that were hosted on Pornhub. A 15-year-old girl who had been missing for a year was finally found after her mother was tipped off that her daughter was being featured in videos on the site — 58 such videos of her rape and sexual abuse were discovered on Pornhub.*
>
> *Her trafficker, who was seen in the videos raping the child, was identified using surveillance footage of him at a 7-Eleven where he was spotted with his victim. He is now facing a felony charge.*
>
> *Also in recent news was the case of 22 women who were deceived and coerced by Michael Pratt, owner of GirlsDoPorn, into performing sex acts on film that were subsequently uploaded to Pornhub. These women sued GirlsDoPorn and won a $12.7 million lawsuit against the company. According to a federal indictment, Pratt and his co-conspirators produced filmed child rape and sexual abuse content and trafficked a minor. Pratt reportedly fled the United States for New Zealand and is currently wanted on a federal warrant.*
>
> *But there are other individuals complicit in these crimes who should also be wanted by law enforcement — CEO Ferris Antoon and COO David Tassillo of Mindgeek, the Canadian-based company that owns Pornhub.*
>
> *You see, Pornhub is complicit in the trafficking of these women and minors and probably thousands more like them.*
>
> *Pornhub is generating millions in advertising and membership revenue with 42 billion visits and 6 million videos uploaded per year. Yet it intentionally, and as a policy, has no system in place to verify reliably the age or consent of those featured in the pornographic content it hosts and profits from.*
>
> *In fact, all that is needed to upload pornography onto Pornhub is an email address. No government-issued ID is required, not even to become "verified" with its trusty blue checkmark that makes everything seem a-OK.*
>
> *I know this, because I tried it.*
>
> *It took me under 10 minutes to create a user account and upload blank test content to the site, which went live instantly. I could have then gone on to become Pornhub-verified, and all I would need to do is send a photo of myself holding a paper with my username. That's it.*
>
> *It is no surprise that Pornhub admitted to verifying the trafficked 15-year-old girl who was sexually abused in 58 videos on its site. The official Twitter account for Pornhub wrote in response to the breaking story that the 15-year-old girl had been a verified member. After quickly realizing it had just admitted to assisting in her being trafficked, the account deleted the tweets, but the evidence of the admission was cached and still exists.*
>
> *One of the most-searched terms on Pornhub is "teen" pornography, in fact it has been a top ten search term on the site for six consecutive years. The search will result in videos that are constantly being added faster than any individual could watch them. Many feature girls who*

look 13 years old at best — girls with braces, pigtails, flat chests, no makeup, extremely young faces, holding teddy bears and licking lollipops, all while being aggressively penetrated. A quick search for the word "teen" turns up titles such as "Young Girl Tricked," "Innocent Brace Faced Tiny Teen F---ed," "Tiny Petite Thai Teen," "Teen Little Girl First Time," on and on ad infinitum.

Pornhub intentionally and as a policy, has no reliable system in place to verify that those in the videos it hosts are not trafficked children being raped on film in order to line the pockets of its executives.

What all of this means is that at this very moment, there could be hundreds, if not thousands, of videos of underage sex trafficking victims on Pornhub. We already have evidence, and it is just the tip of the iceberg.

It's time to shut down super-predator site Pornhub and hold the executive megapimps behind it accountable.

Collective Shout supports this petition. Pornhub must be called to account for aiding and profiting from sex trafficking and rape and its crimes against women and girls.

Under the proposed ancillary service provider notice scheme, PornHub could be delisted and deranked, which would be a small start to decreasing their power and influence. Even better would be to require Australian ISPs to block the offending site. Ultimately, PornHub should be shut down and its executives called to account.

Role of the eSafety Commissioner

36. Are the eSafety Commissioner's functions still fit for purpose? Is anything missing?

We believe that the eSafety Commission has been working well in carrying out its responsibilities. However the internet is still not a safe place, especially for young people. There are many reasons why digital technology providers are still not being effectively held to account for the harm they cause, as identified by Miller, Ohrvik-Stott and Coldicutt (2018).

- Regulators lack resources and expertise. There remains a major imbalance between industry and regulators. This may be a funding issue regarding competitive salaries and opportunities.
- Regulators react too late, looking backwards rather than forwards. Regulators must respond quickly to disruptive change (innovation that significantly alters the way that consumers, industries, or businesses operate).
- Societal impacts are out of scope. Broader public interest must be considered alongside individual consumer welfare and the right to expression and free speech.

- There is an absence of robust evidence about the impacts of technology. It is therefore difficult to prioritise or evaluate. Industry-provided data is not objective nor audited (e.g. Facebook transparency reporting), so publicly-funded research is needed.
- The public has little voice. Doteveryone's research (Miller, Ohrvik-Stott and Coldicutt 2018) finds that there is limited understanding of how digital technologies work, the business models behind them, or how people can exercise their rights when using social media and the internet.

37. To what extent should the existing functions of the eSafety Commissioner be streamlined? Are there particular functions that need to be maintained, or new functions that should be specified?

We recommend an expanded function of conducting or commissioning independent research into the prevalence and causes of technology-related impacts. It is difficult to prioritise and evaluate what works in the absence of evidence.

References

Alison, Coralie (23rd November 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

Alison, Coralie (3rd February 2020). When 'ethical' funds invest in sexploitation. *Collective Shout* https://www.collectiveshout.org/tags/honey_birdette

Australian Institute of Family Studies (2018). *Online Safety*, CFCA Resource Sheet, Australian Institute of Family Studies. https://aifs.gov.au/cfca/publications/online-safety

Bickert, Monica (February 2020). *Charting a Way Forward: Online Content Regulation*. Facebook. https://about.fb.com/wp-content/uploads/2020/02/Charting-A-Way-Forward_Online-Content-Regulation-White-Paper-1.pdf

Bradley, C. and Wingfield, R. (May 2018). *A rights-respecting model of online content regulation by platforms*. Global Partners Digital, London. https://www.gp-digital.org/wp-content/uploads/2018/05/A-rights-respecting-model-of-online-content-regulation-by-platforms.pdf

Burke, Gail and Silva, Kristian (15th Feb 2017). Offensive Wicked Campers vehicles face de-registration on Queensland roads under new law. *ABC News.* https://www.abc.net.au/news/2017-02-15/wicked-campers-offensive-slogans-to-be-banned-queensland-roads/8270568

Burrows, Malcolm (15th January 2020). Proposed standards for online safety. *Dundas Lawyers*. https://www.dundaslawyers.com.au/proposed-standards-for-online-safety/

Campo, Monica (4th May 2016), Children and young people's exposure to pornography. Australian Institute of Family Studies. https://aifs.gov.au/cfca/2016/05/04/children-and-young-peoples-exposure-pornography

Cole, Samantha and Maiberg, Emanuel (7th Feb 2020). Pornhub Doesn't Care. *Vice.* https://www.vice.com/en_us/article/9393zp/how-pornhub-moderation-works-girls-do-porn?utm_campaign=sharebutton&fbclid=IwAR1gu_hA-57Ul8pjAdGjZKLhd8SrDKOP1MB2e6PoGxsjSwssIkwgJqD2HRk

Collective Shout (2019). Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs Inquiry into age verification for onlinewagering and online pornography. https://d3n8a8pro7vhmx.cloudfront.net/collectiveshout/pages/3258/attachments/original/1575331635/Age_Verification_Submission.pdf?1575331635

Duarte, N., llanso, E. and Loup, A. (November 2017). *Mixed Messages? The limits of automated social media content analysis*. Centre for Democracy and Technology. https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf

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

Etheredge L and Lemon J (2015). Pornography, problem sexual behaviour and sibling on sibling sexual violence. *Submission to the Royal Commission into Family Violence*. Victoria. SUBM.0220.001.0001 http://www.news.com.au/national/nsw-act/teenage-sex-offences-increase-australian-bureau-of-statistics-figures-show/story-fndo4bst-1226504441765

Falk, Rachael (21st February 2020). We are powerless as evil is encrypted all around. *The Australian*, p12.

Fitzsimmons, Caitlin (2nd December 2019b). '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

Information Commissioner's Office (21st January 2020). ICO Publishes Code of Practice to Protect Children's Privacy Online. *Information Commissioner's Office.* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/

Kennedy, Lyn (15th February 2019). Porn-style image in shopping malls: How 'Male Champions' fail to address sexism. Collective Shout. https://www.collectiveshout.org/porn_style_image_in_shopping_malls_how_male_champions_fail_to_address_sexism

Lewis, Rosie (19th February 2020). AFP Chief Reece Kershaw could call out tech giants. *The Australian.*

Liszewski, Melinda (10th October 2019a). A day of the girl on Instagram: posed, exposed, and at risk. *Collective Shout.*
https://www.collectiveshout.org/a_day_of_the_girl_on_instagram_posed_exposed_and_at_risk

Liszewski, Melinda (28th November 2019). I was so concerned about porn-themed portrayals of young girls on Instagram I reported to police. *Collective Shout.*
https://www.collectiveshout.org/instagram_community_guidelines_police

Liszewski, Melinda (5th December 2019). Insta must act on predators: Collective Shout letter to platform heads. *Collective Shout.*
https://www.collectiveshout.org/insta_must_act_on_predators_collective_shout_letter_to_platform_heads

Livingstone, S., Carr, J. and Byrne, J. (January 2016). One in Three: Internet Governance and Children's Rights. *Innocenti Discussion Paper* No. 2016-01, UNICEF Office of Research, Florence.
https://www.unicef-irc.org/publications/pdf/idp_2016_01.pdf

Livingstone, S., Haddon, L., Görzig A. and Ólafsson, K. (2010). *Risks and safety for children on the internet: the UK report. Full findings from the EU Kids Online survey of UK 9-16 year olds and their parents.* The London School of Economics and Political Science.
http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/National%20reports/UKReport.pdf

Livingstone, S., Kardefelt-Winther, D. and Saeed, M. (2019). *Global Kids Online: Comparative Report*, UNICEF Office of Research – Innocenti.
https://www.unicef-irc.org/publications/pdf/GKO%20LAYOUT%20MAIN%20REPORT.pdf

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

Miller, C., Ohrvik-Stott, J. and Coldicutt R. (2018) *Regulating for Responsible Technology: Capacity, Evidence and Redress: a new system for a fairer future*. London: Doteveryone.
https://doteveryone.org.uk/project/regulating-for-responsible-technology/

Miller, Nick (26th August 2019). Morrison lands at G7 with new plan to fight online extremism. *The Sydney Morning Herald.*
https://www.smh.com.au/world/europe/morrison-lands-at-g7-with-new-plan-to-fight-online-extremism-20190825-p52kli.html

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

Moore, Lindsay (17 January 2020). Police, survivors debunk human trafficking kidnapping myths. *Michigan Live*.
https://www.mlive.com/news/kalamazoo/2020/01/police-survivors-debunk-human-trafficking-kidn

apping-myths.html?utm_medium=social&utm_campaign=mlivedotcom_sf&utm_source=facebook&fbclid=IwAR12lSh-YvJI6iLvrgy4PQXc09VykeUX83Oc1KE_QfL-K0u3QNsChPBepQ0

Mortreux, C., Kellard, K., Henry, N. and Flynn, A. (2019). *Understanding the attitudes and motivations of adults who engage in image-based abuse.* Social Research Centre. Report prepared for the eSafety Commissioner, Melbourne, Victoria. https://www.esafety.gov.au/sites/default/files/2019-10/Research_Report_IBA_Perp_Motivations.pdf

NCOSE (26th November 2019). 13yo girl was abused and exploited on Instagram in her own home. It could have been prevented. *National Center on Sexual Exploitation.* https://endsexualexploitation.org/articles/a-13yo-girl-was-abused-and-exploited-on-instagram-in-her-own-home-it-could-have-been-prevented/

Novak, Kenny (13th July 2019). Why Facebook deletes your posts for community standards. *Boostlikes.* https://boostlikes.com/blog/2019/07/deletes-post-community-standards

O'Neill Brian and Dinh Thuy (March 2018). The Better Internet for Kids Policy Map: Implementing the European Strategy for a Better Internet for Children in European Member States. https://www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7

Powell, A., Scott, A. J., Flynn, A. and Henry, N. (February 2020). *Image-Based Sexual Abuse: An International Study of Victims and Perpetrators: A Summary Report*. Melbourne: RMIT University.

Professor Freda Briggs (2015) *Submission to the Senate Environment and Communications References Committee Inquiry into the Harm Being Done to Australian Children Through Access to Pornography on the Internet.* March 2016. http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Online_access_to_porn/Submissions

Queensland Police. (2014). *Who's chatting to your kids?* Brisbane: Queensland Police. www.police.qld.gov.au/programs/cscp/personalSafety/children/childProtection/

Roper, Caitlin (27th October 2014). Being pimped out online by misogynist harassers will not stop me from speaking out. *The Guardian*. https://www.theguardian.com/commentisfree/2014/oct/27/being-pimped-out-online-by-misogynist-harassers-will-not-stop-me-from-speaking-out

Roper, Caitlin (20th June 2016). 25 Reasons Why Ad Industry Self-Regulation is a Disaster. *Collective Shout.* https://www.collectiveshout.org/reasons_why_ad_industry_self_regulation_is_a_disaster

Rouse, Alisha (21st January 2020). 'Not safe for kids': Popular social media app TikTok is a magnet for pedophiles, claims Australian cyber safety expert. *Daily Mail UK*. https://www.dailymail.co.uk/news/article-7909685/How-paedophiles-target-Australian-kids-TikTok-push-button.html?ito=facebook_share_article-top&fbclid=IwAR1lVzxus-Y5Y_NsK3Opq1vnmK3YvWQDjWVr3NCyj7iQ1Kk_qhz-XpmnaAc

Seto MC and Lalumiere ML (2010). What is So Special about Male Adolescent Sexual Offending? A Review and Test of Explanations through Meta-Analysis. *Psychological Bulletin* 136(4): 526-575.

Stalker, Livingstone, Kardefelte-Winther and Saeed (2019), *Growing Up In A Connected World*, UNICEF. https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf

Tankard Reist, M. (2019). *Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs Inquiry into Age Verification for Online Wagering and Online Pornography.* Submission 177 at https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Submissions

Taylor, Josh (10th March 2014). Government pressured to drop social media censorship plans. *ZDNet* https://www.zdnet.com/article/government-pressured-to-drop-social-media-censorship-plans/

Taylor, Josh (22nd January 2014). Social media watchdog has 'serious risks': Freedom commissioner. *ZDNet.* https://www.zdnet.com/article/social-media-watchdog-has-serious-risks-freedom-commissioner/

United Nations (1989). *Convention on the Rights of the Child*. https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

United Nations (2011). *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. New York and Geneva. https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Wingfield, Richard (8th January 2020). Online Safety Legislation Reform in Australia: Our First Thoughts. *Global Partners Digital* https://www.gp-digital.org/online-safety-legislative-reform-in-australia-our-first-thoughts/

Zuckerberg, Mark (30th March 2019). "The Internet Needs New Rules. Let's Start in These Four Areas." Washington Post.

Zuckerberg, Mark (16th February 2020). Big Tech Needs More Regulation. *The Financial Times*.