Statutory Review of the Online Safety Act 2021

Collective Shout: for a world free of sexploitation

Email to OSAReview@COMMUNICATIONS.gov.au

Introduction

We are pleased to submit our recommendations to the Statutory Review of the Online Safety Act 2021. The new measures outlined in the discussion paper are welcomed by our team.

Our submission addresses serious and urgent concerns relating to digitally-facilitated sexual exploitation as related to human rights, child protection, women's safety and public health. We must address the range of harms enabled by global Big Tech companies. This Statutory Review is a critical opportunity to improve regulation of harmful online content and tech-facilitated abuses, including pornography, Child Sexual Abuse Material (CSAM), image-based abuse/non-consensual image sharing, and emerging digital threats such as AI generated deep-fake nudes, nudifying/undressing apps and other forms of digitally-enabled sexual exploitation.

We note in particular the devastating impact of the global pornography industry, especially in its malign influence on the developing sexual templates of children and young people.The links between pornography and violence against women have been extensively documented.[1] Pornography is commercial sexual exploitation, fuelled by human trafficking, child sexual abuse material (CSAM), slavery, non consensual material, deepfakes, and violence.[2]

We also draw attention to the ongoing challenge of predators who continue to find new ways to use the internet to access, groom, and abuse children. Tech companies enable this by serving up sexualised content featuring children to men with sexual interests in them, through their algorithms.[3] Meta's move to encryption has enabled groups of men to share

[1] Our Watch (2020). Pornography, Young People, and Preventing Violence Against Women: Background Paper. www.ourwatch.org.au; Australian Government Department of Social Services (17 Oct 2022). The National Plan to End Violence Against Women and Children 2022-2032. https://www.dss.gov.au/ending-violence; Collective Shout (19 Sept 2023). Open Letter: Women's safety and child protection experts call for age verification pilot. https://www.collectiveshout.org/open_letter_age_verification

[2] Collective Shout (23 Mar 2021). Submission to Canadian Parliamentary Ethics Committee: Protection of Privacy and Reputation on Platforms such as Pornhub. https://www.collectiveshout.org/submission_ethi_mindgeek; Liszewski, Melinda (1 Mar 2021). Collective Shout signs global letter calling for MindGeek/Pornhub criminal investigation. https://www.collectiveshout.org/signs_global_letter_calling_for_mindgeek_pornhub_criminal_investigation

[3] See our Instagram campaign at https://www.collectiveshout.org/_instagram

CSAM with impunity.[4] Online sexual exploitation is a rapidly growing threat to children and young people.

Summary of Recommendations:

1. The most critical elements of BOSE should be legally enforceable.
2. Service providers' Terms of Use should not be the primary system for ensuring online safety.
3. Create a legally binding, public-facing complaints scheme for the digital sector with clear, effective and timely mechanisms, policies and procedures.
4. Establish an independent Ombuds for dispute resolution in the Digital Industry.
5. Pornography should be reclassified as Class 1 material and treated as such in the Online Safety Act.
6. An Age Verification should be trialled as soon as possible, with the trial conducted by the most experienced body in the field, with defined timelines and public knowledge of who will be appointed to assess and evaluate the results.
7. Bystanders should be empowered to report illegal or seriously harmful material to the Commissioner.
8. Apps that create deepfakes should be outlawed for Australian consumers, those who create them should be held responsible, and advertising such apps should also be illegal.
9. At all stages in the generative AI lifecycle, the use and production of CSAM should be illegal.
10. Strong support systems should be created to assist victims of deepfake pornography and CSAM in the short and long term.
11. Create a law similar to the UK's Clare's Law, allowing people the right to know if their current or ex-partner has a previous history of violence or abuse.
12. Invest in education and training to ensure everyone knows the law on deepfakes and AI pornography.
13. Increase penalties for technology-facilitated abuse and violence.
14. Additional resources must be allocated for law enforcement and legal and psychosocial support for victims of technology-facilitated abuse and violence, to ensure the law is enforced.
15. Increase civil penalties for violations of the Online Safety Act and the BOSE.
16. Introduce a formal statutory Duty of Care framework into the Act.
17. Introduce Best Interest of the Child requirements into the Act.
18. Recommendation: Industry should be contributing to law enforcement, police training, education and tools to ensure that victims are supported and justice is done.

About Collective Shout

[4] Collective Shout (Oct 2022). Submission on Draft Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material). https://www.collectiveshout.org/submission_draft_codes_class1a_1b

Collective Shout (www.collectiveshout.org) is a grassroots campaigning 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[5] and in child sex abuse dolls and replica child body parts.[6]

Our work puts us in touch with the unique and specific ways children are at risk, especially in their vulnerability to online grooming by predators and exposure to pornography. Young people are at special risk of sexualisation, objectification and exploitation online. They are vulnerable to cyberbullying, sexual harassment, image-based abuse, predatory behaviour, grooming and exposure to pornography. This causes physical and psychological harm.

We have documented these harms for the past 14 years, including in the following:

- Submission to Draft Online Safety (Relevant Electronic Services and Designated Internet Services – Class 1A and 1B Material) Industry Standard 2024.[7]
- Submission to the previous inquiry on this matter - Draft Consolidated Industry Codes of Practice for the Online Industry (Class 1A and 1B Material) 2024.[8]
- Submission to the Amendment to the Online Safety (Basic Online Safety Expectations) Determination 2023.[9]
- Submission to Select Committee on Social Media and Online Safety 2022;[10]
- Submission to eSafety Consultation on the implementation roadmap for a mandatory age verification (AV) regime relating to online pornography 2021;[11]
- Submission to the inquiry into Law Enforcement Capabilities in Relation to Child Exploitation 2021;[12]

---

[5] Tankard Reist, Melinda (2017). Why are Australian Telcos and ISPs enabling a child abuse pandemic? *ABC Religion and Ethics.* https://www.abc.net.au/religion/why-are-australian-telcos-and-isps-enabling-a-child-sexual-abuse/10095644; Collective Shout (6 Sep 2021). *National Child Protection Week 2021: Join our campaigns to protect children and young people.* https://www.collectiveshout.org/child_protection_week_2021)

[6] Roper, Caitlin (2022). *Sex Dolls, Robots, and Woman Hating: The Case for Resistance.* Spinifex Press. https://www.spinifexpress.com.au/shop/p/9781925950601; see also Roper, Caitlin (9 Jan 2020). "Better a doll than a real child:" The spurious logic used to justify child sex dolls. *ABC Religion and Ethics.* https://www.abc.net.au/religion/spurious-logic-used-to-justify-child-sex-dolls/11856284

[7] Collective Shout (22 Jan 2024). *Submission to Draft Online Safety (Relevant Electronic Services and Designated Internet Services – Class 1A and 1B Material) Industry Standard 2024*. https://www.collectiveshout.org/tags/submissions

[8] Collective Shout (Oct 2022). *Submission on Draft Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material).* https://www.collectiveshout.org/submission_draft_codes_class1a_1b

[9] Collecting Shout (Feb 2024). *Amendment to the Online Safety (Basic Online Safety Expectations) Determination 2023*. https://www.collectiveshout.org/amendment_to_the_online_safety_bose

[10] Collective Shout (Jan 2022). *Submission to Select Committee on Social Media and Online Safety*. https://www.collectiveshout.org/submission_social_media_online_safety

[11] Collective Shout (2021). *Submission: eSafety Consultation on implementation roadmap for a mandatory age verification (AV) regime relating to online pornography.*

[12] Collective Shout (20 Aug 2021). Submission: Law Enforcement Capabilities in Relation to Child Exploitation. https://www.collectiveshout.org/submission_law_enforcement_child_exploitation

- Submission to the United Nations' review Children's Rights in the Digital Environment 2020;[13]
- Submission to the Inquiry into Age Verification for Online Wagering and Online Pornography 2019;[14]
- Submission on Harm Being Done to Australian Children Through Access to Pornography on the Internet to the Senate Environment and Communication References Committee 2016;[15] and
- Numerous other publications and commentaries.[16]

We track the activities of online predators on popular social media sites, documenting and reporting thousands of accounts for preying on underage/prepubescent girls. These predators are attempting to engage with them privately, describing sex abuse acts they wish to carry out on these girls, and soliciting, selling and trading child exploitation material. We have also documented the tracking, tagging and sharing of the Instagram content of hundreds of underage girls to paedophile forums operating on the open web.

Our joint global #WakeUpInstagram campaign with the National Center on Sexual Exploitation (USA), Courtney's House (US) and Defend Dignity (Canada) exposed Instagram as a platform for predators to access children, pornography companies to promote and link to hardcore porn sites, for hosting offers of paid sexual content featuring children, and for facilitating other practices harmful to children and young people.[17]

Questions for the Consultation

4. Should the Act have a strengthened and enforceable BOSE?

---

[13] Collective Shout (30 Nov 2020). *UN Submission: Children's Rights in the Digital Environment.* https://www.collectiveshout.org/un_sub_children_digital_rights

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

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

[16] For example, see Tankard Reist, Melinda (2016). Early sexualisation and pornography exposure: the detrimental impacts on children, *Australian Childhood Foundation blog.* https://professionals.childhood.org.au/prosody/2016/07/melinda-tankard-reist/; Tankard Reist, Melinda (2016). Growing Up in Pornland: Girls Have Had It with Porn Conditioned Boys, *ABC Religion & Ethics*. https://www.abc.net.au/religion/growing-up-in-pornland-girls-have-had-it-with-porn-conditioned-b/10097244; Tankard Reist, Melinda (2018). Never Again? Addressing Sexual Violence Must Include Pornography, *ABC Religion & Ethics*. https://www.abc.net.au/religion/never-again-addressing-sexual-violence-must-include-pornography/10094568

[17] See https://www.collectiveshout.org/_instagram.

> Recommendation: The most critical elements of BOSE should be legally enforceable.

Currently, the BOSE sets out excellent guidelines for safe design of digital services. But it does not create legally enforceable duties. The only legal requirement in the BOSE is to supply any requested report. This transparency reporting has not resulted in widespread safety improvements - we see this as further proof that Big Tech needs to be forced into making its products safe. Reputational harm is demonstrably insufficient to motivate change - digital platforms are so embedded in our daily lives that despite rock-bottom levels of public trust, most people cannot avoid them.

The following are examples of important child safety features which should be legally required for social media platforms:

- Age verification to prevent children from accessing sexually explicit content;
- Detection and removal of all child exploitation material, including user-reported content;
- Removal of all pre-teens from the platforms;
- Banning ‘parent run’ accounts which allow users to circumvent minimum user age policies;
- Timely and effective responses to user complaints and reports (see question 9).

Elements of the BOSE that should be legally required include:

- Proactively minimising material or activity that is unlawful or harmful, and ensuring users can use a service in a safe manner.
- Protecting children from content that is not age appropriate like pornography
- Preventing harmful use of anonymous and encrypted services.
- Putting in place user-reporting mechanisms, and clearly outlining their terms of service and enforcing penalties for people who breach these terms.
- Cooperating with other service providers.
- Responding to requests for information from the eSafety Commissioner.

6. To what extent should online safety be managed through a service provider’s terms of use?

> Recommendation: Service providers’ Terms of Use should not be the primary system for ensuring online safety.

We do not have confidence in the willingness and ability of digital platforms to manage online safety through their Terms of Use. This would act as a form of self-regulation - a failed regulatory model as demonstrated by the behaviour of the advertising industry. Please refer to our response to question 9 for our experiences of service providers failing to uphold their Terms of Use.

9. Are the complaints schemes accessible, easy to understand, and effective for complainants?

> Recommendation: The Online Safety Act should create a legally binding, public-facing complaints scheme for the digital sector with clear, effective and timely mechanisms, policies and procedures.

We recommend making clear mechanisms, policies and procedures to deal with reports and complaints. These systems should be legally binding. As identified by the ACCC in the Digital Platform Services Inquiry 2020-25, Australia needs an independent ombuds to deal effectively with disputes in the digital industry, especially regarding privacy and online harms (see question 25).

We support Reset Australia's recommendation that a public facing complaints system should be enacted for the digital sector.[18]

Complaints and user reports should by no means be the primary detection system for CSAM and other illegal content. If user reports comprise the only content management strategy, significant underreporting is the result.[19] It is also a grave abdication of responsibility by those who profit from the platforms and services.

However, user reports are essential for catching harmful material. We have significant evidence that Big Tech reporting mechanisms are not keeping children safe. For years, Collective Shout has been investigating social media platforms for child sexual abuse material and reporting it. Our investigations have found:

- AI images of prepubescent boys in fetish gear on Instagram are "not actionable" according to eSafety. We discovered AI-generated images of young children on Instagram we believe constitute illegal Child Sexual Abuse material. The images depict little boys in minimal clothing, some adorned with fetish gear, and their bodies oiled. When we reported the account to eSafety, we were informed the content was not actionable given the lack of nudity and "non-sexualised posing". When we enquired of eSafety what material would qualify as category 1 child sexual abuse material (and warrant removal) we were told "Material that describes or depicts child sexual abuse, or any other exploitative or offensive description or depiction involving a person who appears to be a child under 18 years." We believe that under the definition provided, these images should qualify.[20]

---

[18] Reset Australia (Feb 2024). *Response to the Amending Oline Safety (Basic Online Safety Expectations) Determination 2022 Consultation*. https://au.reset.tech/uploads/Basic-Online-Safety-Expectations-Reset.Tech-Submission-Feb24-.pdf

[19] Plan International (2024). *Submission to United Nations: Existing and Emerging Sexually Exploitative Practices Against Children in the Digital Environment.* https://www.ohchr.org/en/calls-for-input/2024/call-input-existing-and-emerging-sexually-exploitative-practices-against

[20] Roper, Caitlin (15 Apr 2024). AI images of little boys in fetish gear on Instagram "not actionable", says eSafety. *Collective Shout.* https://www.collectiveshout.org/ai_images_of_little_boys_in_fetish_gear_on_instagram_not_actionable_says_esafety

- Meta dismissed our complaints about accounts selling child sex abuse dolls, including dolls modelled on prepubescent and toddler girls, some pictured with toys. Meta removed the account only after News Corp pointed out that it included a link to its website selling the products.[21]
- We report dozens of accounts on Twitter and Instagram that display stolen images of children with sexual comments beneath them, some with sexualised emojis, indicating paedophile networking. Large networks of men are scraping content from girls' social media accounts and posting it onto X for sexual discussion and commentary. Meta and X are both failing to deal with accounts, posts, and comments that are obviously facilitating CSAM proliferation.[22]
- In August 2022 we made 100 reports of child exploitation activity using Instagram's in-app reporting tools. Months later, Instagram had reviewed less than half the reports. Only three pieces of content were removed. Of the remaining reviewed content, Instagram said it did not go against its Community Guidelines.[23]

> Recommendation: Establish an independent Ombuds for dispute resolution in the Digital Industry.

In response also to question 25, we support the establishment of an independent Ombuds for dispute resolution in the Digital Industry.

11. Does the Commissioner have the right powers to address access to violent pornography?

> Recommendation: Pornography should be reclassified as Class 1 material, and treated as such in the Online Safety Act.

The Commissioner does not have the right powers to address access to violent pornography as it relies on the National Classification Scheme to classify material and is therefore required to treat pornography as Class 2 material.

Pornography is easy to access, widely consumed and dominated by violence, coercion, cruelty, racism, and misogyny.[24] The pornography industry is rife with trafficking, prostitution, rape, exploitation of children, and non-consensual material. The industry profits from this

---

[21] Collective Shout (25 Jan 2023). Instagram slammed for 'fuelling' the sale of child-like sex dolls: our investigations in the media. *Collective Shout.* https://www.collectiveshout.org/instagram_slammed_for_fuelling_the_sale_of_child_like_sex_dolls

[22] Collective Shout (10 Nov 2022). Meta failing young girls: Our investigations in the media. *Collective Shout.* https://www.collectiveshout.org/meta_failing_children_inews

[23] Kennedy, Lyn (10 Nov 2022). We reported 100 pieces of child exploitation content to Instagram - they removed just three. *Collective Shout.* https://www.collectiveshout.org/100_reports_of_child_exploitation_instagram

[24] Collective Shout. Pornhub commits crimes against women and girls. Content warning: Images blurred but still very confronting and may be upsetting. https://www.collectiveshout.org/pornhub_commits_crimes_against_women_and_girls

content and has proven itself unwilling to regulate itself appropriately. This has resulted in a public health crisis.

The most popular genres are the most violent. The French equality watchdog, in a 2023 report, found as much as 90% of pornographic content online features verbal, physical and sexual violence towards women, with a significant amount of the violence portrayed being punishable under existing French laws: "The women are real, the sexual acts and the violence is real, the suffering is often perfectly visible and at the same time eroticized."[25]

Our previous submissions have explained why the Classification system should be modernised to account for real harm, rather than "offence, morality, or decency." Along with other grassroots organisations such as CEASE UK, NCOSE USA, and Defend Dignity (Canada), we have also made the case for why pornography should now be considered to be violent, harmful, and criminal material and regulated as such. As stated by the National Center on Sexual Exploitation:

> *Pornography is a deeply damaging social influence that corrodes relationships, erodes the sensibilities and sexual freedom of consumers, and dehumanizes those who make it.*[26]

We strongly recommend that pornography should be classified as Class 1 material - that is, "material that depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards or morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified."

12. What role should the Act play in helping to restrict children's access to age inappropriate content (including through the application of age assurance)?

> Recommendation: An Age Verification should be trialled as soon as possible, with the trial conducted by the most experienced body in the field, with defined timelines and public knowledge of who will be appointed to assess and evaluate the results.

Collective Shout has long campaigned for a system of age verification to protect children from pornography exposure. After the Federal Government announced its decision against an age verification pilot late last year, we spearheaded an open letter signed by leading women's safety and child protection agencies and prominent Australians.[27] In March, following additional pressure in the lead up to its national emergency cabinet meeting, the

[25] Alison, Coralie (29 Sept 2023). French equality watchdog finds 90% of online pornography abuses women. *Collective Shout*. https://www.collectiveshout.org/online_prn_abuses_women
[26] National Center on Sexual Exploitation (2024). Public Health Harms of Pornography. https://endsexualexploitation.org/issues/pornography/
[27] Collective Shout (19 Sept 2023). Open Letter: Women's safety and child protection experts call for age verification pilot. *Collective Shout.* https://www.collectiveshout.org/open_letter_age_verification

Government reversed its decision and announced an age verification pilot. The trial should be launched without delay.

The BOSE should require age verification of any digital service that hosts sexually explicit material. The evidence is clear that early porn exposure harms developing sexual templates, contributes to damaging stereotypes, the development of sexist ideas, the normalisation of violence against women and a rise in child-on-child sexual abuse. Adolescent males are now committing higher rates of sexual offences. They are also identified as the largest cohort of sex offenders against children.[28]

In the UK where age verification is mandated, the UK regulator Ofcom has found it necessary to conduct special investigations into adult video sharing services (VSPs) to ensure they are taking appropriate measures to protect children from pornography, despite statutory transparency reporting. On May 1, an investigation was opened into whether OnlyFans was doing enough to prevent children accessing the site, having grounds to suspect the platform did not sufficiently implement age verification measures. Ofcom will also investigate whether OnlyFans complied with its duties to provide complete and accurate information in response to statutory requests.[29]

Ofcom publishes the results of these investigations, including their concerns, the new commitments made by each company, for example, adult VSPs SoSpoilt, CamSoda, and MintStars, and further responses by Ofcom.[30] This is a potentially useful model for transparently monitoring compliance with future age verification legislation in Australia.

14. Should the Act empower 'bystanders', or members of the general public who may not be directly affected by illegal or seriously harmful material, to report this material to the Commissioner?

> Recommendation: Bystanders should be empowered to report illegal or seriously harmful material to the Commissioner.

The Online Safety Act should empower bystanders and members of the general public who are not directly affected by illegal or seriously harmful material for the following reasons:

- The victim may be unaware of the content or abuse.
- It should not be the victim's job to search the internet for videos of their abuse as evidence.
- The victim may be afraid of retribution.

---

[28] Mathew, B., Finkelhor, D., Pacella, R. et al. (Jan 2024). Child sexual abuse by different classes and types of perpetrator: Prevalence and trends from an Australian national survey. *Child Abuse & Neglect* 147:106562. https://doi.org/10.1016/j.chiabu.2023.106562.

[29] Ofcom (1 May 2024). Ofcom investigates OnlyFans' age verification measures. *Ofcom*. https://www.ofcom.org.uk/online-safety/protecting-children/ofcom-investigates-onlyfans-age-verification-measures/?language=en

[30] Ofcom (1 May 2024). Enforcement programme into age assurance measures on UK-established, adult video-sharing platforms. *Ofcom*. https://www.ofcom.org.uk/online-safety/protecting-children/cw_01266/

- Victims are often young or otherwise disempowered.
- The community needs to stop being bystanders to sexual exploitation.
- The consumption of illegal and seriously harmful material impacts us all, as it fuels a culture in which male violence against women is accepted.

Many of our supporters report sexually exploitative content online and in the real world. Our four-year ongoing investigation into Instagram has exposed rampant sexualisation of minors and highlighted the way Instagram is geared toward connecting men to underage girls. In response to our joint, global #WakeUpInstagram campaign, Instagram announced new safety features including a restriction preventing direct messages between teenagers and men they do not follow and an in-app reporting tool to report Instagram accounts that sexualise children. Of course, there is much more to be done to make Instagram safe.

16. What more could be done to promote the safety of Australians online, including through research, educational resources, and awareness raising?

Recommendation: Apps that create deepfakes should be outlawed for Australian consumers, those who create them should be held responsible, and advertising such apps to Australians should also be illegal.

Recommendation: At all stages in the generative AI lifecycle, the use and production of CSAM should be illegal.

Recommendation: Strong support systems should be created to assist victims of deepfake pornography and CSAM in the short and long term.

Recommendation: Create a law similar to the UK's Clare's Law, allowing people the right to know if their current or ex-partner has a previous history of violence or abuse.

Recommendation: Invest in education and training to ensure everyone knows the law on deepfakes and AI pornography.

Recommendation: Increase penalties for technology-facilitated abuse and violence.

Recommendation: Additional resources must be allocated for law enforcement and legal and psychosocial support for victims of technology-facilitated abuse and violence, to ensure the law is enforced.

The misuse of generative AI to create deepfakes and synthetic pornography exemplifies the problem of emerging digital threats.

Generative AI must be recognised as a tool created and utilised by real people. Collective Shout Campaign Strategist Lyn Kennedy writes:

> *AI itself is not creating child sexual abuse material (CSAM) or image-based abuse material. AI content is generated by real people who prompt machine learning software. This software is trained on a vast body of digitised images and videos including real child sexual abuse material, images of real children and other real pornography created by real people.*[31]

Professor Michael Salter[32] also explains:

[31] Collective Shout (2 Feb 2024). Made by men: How the term "AI generated" invisibilises sex offenders. *Collective Shout.* https://www.collectiveshout.org/ai_a_tool_for_abusing_women_and_children

[32] https://research.unsw.edu.au/people/professor-michael-alan-salter

> *We have to reject the self-mythologising of the technology sector. "AI" is not sentient machines. The "dark web" is not a secret parallel internet. These are all mundane technologies developed by people and legal entities who can and should be held to account.*[33]

We welcomed the announcement on May 1 that the Government will introduce legislation to ban the creation and non-consensual distribution of deepfake pornography.[34] With a maximum penalty of six years imprisonment, it sends a strong message to the community that we hope will filter through to every level, that both creating and sharing nonconsensual pornography material is a serious crime. Strengthening existing Criminal Code offences and introducing a new aggravated criminal offence are a good start in tackling this new digital threat.

We recommend that sufficient resources are allocated to investigation and prosecution. Additionally, victims may need legal representation and ongoing psychosocial support.

Laura Bloomer, CEO of Backed Technology and an advocate for technology supportive of people and communities, points out that legislation is only as good as its enforcement. Australia's 2018 'Revenge Porn Bill'[35] often did not accomplish justice for victims due to a lack of supportive structures around it. Currently the rate of criminal convictions is very low.

Due to the low rate of convictions in the Australian context, Laura Bloomer advocates for an in-between list similar to the UK's 'Clare's Law.' This law gives people the right to know if their current or ex-partner has a previous history of violence or abuse, and this would include online abuse.[36]

Why are these apps lawful and available in the first place – and to children? As in the case of the Bacchus Marsh Grammar students who had their social media photos turned into pornography by a fellow student,[37] if images of minors are used to make deepfakes, this constitutes child sexual abuse material.

Regarding technology-facilitated abuse and violence, Collective Shout staff have received extensive online abuse in relation to their public advocacy work. To date, nobody has been prosecuted for any of it.

Coralie Alison, Collective Shout Movement Coordinator, writes:

> *When I was abused on Twitter my name was trending in 6 continents. Here are the issues I had at the time:*

---

[33] https://x.com/mike_salter/status/1800802303299272890
[34] Prime Minister of Australia (1 May 2024). Tackling online harms. https://www.pm.gov.au/media/tackling-online-harms
[35] The Criminal Code Amendment (Private Sexual Material) Act 2018.
[36] Clare's Law (2024). The right to know if your partner has an abusive past. https://clares-law.com/
[37] Ortolan, Mikaela, and Tran, Danny (12 Jun 2024). Victorian teachers also victims of fake explicit images created by students using AI. *ABC News.* https://www.abc.net.au/news/2024-06-13/ai-generated-deepfake-pornography-school-students-teachers/103969414

- *Twitter took a while to contact me and check I was okay. When they did they had their global head of online safety have a 30 min call with me to check on my wellbeing and mental health but this should have been done a lot sooner. I can't recall exactly the delay but maybe 10 hours of intense rape and death threats before they reached out. In that time many feminists were reporting tweets on my behalf so their staff in that department would have seen the dramatic increase in reports.*
- *The original tweet itself was not deemed to be a breech of their terms and conditions so even though they knew it was a form of incitement and was leading to thousands of rape and death threats they refused to take it down. It is still up to this day. I don't think at the time you could remove a tag. But it just occurred to me that feature is now available on Twitter so if it had been available at the time it would have given me the option of removing myself to stop the abuse.*
- *I reported the rape and death threats to the police under using a carriage service to menace and harrass. The police asked for a USB to be dropped at a local police station so I gave them 200 screenshot examples. Shortly after they closed the case due to "free speech". They said that because the platform was run out of California that they go by their laws and therefore none of the rape and death threats were actionable. Shortly after this a person wrote a racist comment on an Essendon footballer's social media account and it was reported in the news that the police had offered to press charges if the footballer wished to proceed under the same law of menace and harass using a carriage service. Yet the social media platform the racist comment was written on was also US.*
- *To report all the tweets about me I had to type in "rape Coralie" "slut Coralie" "kill Coralie" "die Coralie" etc into keyword search on Twitter and scroll through every abusive message and then report it one by one. This further causes trauma and distress.*

Caitlin Roper, Campaigns Manager, was also abused online and says:

> *Police either don't seem to understand the law (or that it's illegal to use a carriage service to menace and harass someone) or that it is enforced inconsistently (in the case of famous male sportsmen, but not women/feminists). Plus the whole issue of when the original threat comes from a different jurisdiction. I've experienced similar, where police didn't act on rape threats or someone copying my profile to pimp me out, because he was based in the US. And in another case where a site was set up to destroy me (including plans to get me raped, photos of my family and friends posted, and my face superimposed on porn) all the police did was get the site eventually taken down - they didn't pursue the perpetrators.*

The final consultation question asks about whether industry should be funding eSafety. In principle we believe so. However we also propose that industry should be contributing to law enforcement; police training, education and tools to ensure that victims are supported and justice is done.

Laura Bloomer says:

> *How to prosecute online sexual offences is still unknown by police forces at a grassroots level. Police centres I interviewed couldn't even determine what department it came under (depts mentioned incl, domestic violence, communications, or cybercrime). Another example being when the Gov/eSafety announced the $100,000 fine for individuals sharing OIBA. None of the police officers I spoke to had heard about it.*[38]

For victims, going through the criminal court process is often traumatising, expensive, and invasive, with very low conviction rates - 1-5% in the UK. Laura Bloomer writes:

> *For these reasons, criminal court process is often actively discouraged to victims by both police and lawyers alike. Almost all lawyers we spoke to for Backed said they don't touch criminal cases, would only prosecute as a civil case. Many cases in the UK never make it to trial, they get thrown out under 'not in public interest', due to these high barriers and low success rates. Criminal court evidence procedures are outdated in this crime. For example, a victim needs to keep the content online for the duration of the investigation, and needs to hand over their mobile phone for sometimes months at a time. Australia's 'open justice' policy of public court records is not supportive of victims of sexual crimes (intimate/sensitive in nature). Both create a drop-out point, victims would rather remove the content immediately, deal with things privately & move on with their lives. This lack of justice in the system & false hope can be further traumatising in itself.*[39]

Given the barriers victims face in criminal court, Laura Bloomer believes this new legislation is unlikely to result in many reports or prosecutions. Even if victims are unable or unwilling to endure the court process, there needs to be some in-between measure to ensure repercussions for perpetrators. Clare's Law in the UK is one example. Domestic violence is a crime with low reporting rates, low rates of prosecution, and often abusers walk free. Unprosecuted offenders could be added to the existing Sex Offenders list or something similar to a 'Clare's Law' list under digital sex offences.

Online abuse reduces women's and girls' ambition to be politically active and involved in public affairs.[40] It is intimidating, scary, and has potential to spill into real world violence. We hope to see a stronger approach built into the Online Safety Act with serious consequences for offenders and more support for victims.

18. Are Australia's penalties adequate and if not, what forms should they take?

[38] Laura Bloomer, personal communication.
[39] Laura Bloomer, personal communication.
[40] Plan International (May 2024). Submission to the Special Rapporteur on the Sale and Sexual Exploitation of Children.

Recommendation: Increase civil penalties for violations of the Online Safety Act and the BOSE.

We support Reset Australia's recommendations in its document *Response to the Amending Online Safety (Basic Online Safety Expectations) Determination 2022 Consultation*, in which Reset puts the case for change to increase penalties for noncompliance:

> *For these businesses, returning a compliance report can be considered a 'goodwill gesture' that they can afford not to offer if they so choose. Where services afford to opt-out of compliance reports, they are a broken transparency measure.*

To improve accountability, we support Reset's recommendations of:

- Introducing an overarching, enforceable duty of care (see question 22).
- Create a public facing complaints system for BOSE violations (see question 9).
- Create a presumption that all examples of reasonable steps outlined in the BOSE will be adopted; and
- Increased civil penalties for non-compliance.

Following the precedents of comparable European and British legislation, we agree with Reset that it would be reasonable and effective to set penalties at 10% of global turnover. In Australia, as Reset points out, the ACCC can enforce this level of penalty for franchising violations.

19. What more could be done to enforce action against service providers who do not comply, especially those based overseas?

There is a strong precedent in Australia for regulators enforcing action against overseas-based service providers who violate Australian laws while operating in Australia.

In January 2011, Australian customers of Valve, owner of the Steam online gaming platform, made complaints to Valve that the games they had purchased did not operate correctly.[41] They were denied refunds, on the grounds that customers had been forced to agree to Steam's Terms of the Agreements, which stated that consumers were not entitled to refunds. The ACCC commenced proceedings against Valve in 2014, alleging deceptive conduct and making false representations about consumer guarantees. Valve was fined $3 million, and appealed to the Federal Court, which upheld the decision and affirmed the penalty. The courts did not agree with Valve's argument that it did not carry on business in Australia. Consequently, Valve introduced a policy of refunds for games that did not work, and since then consumers have benefited from this outcome.

[41] Laidlaw, Michele (Feb 2018). Valve appeal dismissed - the ACCC blows off steam. *Johnson Winter Slattery*. https://jws.com.au/insights/articles/2018-articles/valve-appeal-dismissed-%E2%80%93-the-accc-blows-off-steam

22. Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?

> Recommendation: Introduce a formal statutory Duty of Care framework into the Act.
>
> Recommendation: Introduce Best Interest of the Child requirements into the Act.

We support the introduction of a formal statutory duty of care framework, incorporating substantial penalties for non-compliance, to complement the BOSE and modelled on the best interests of the child principle. This framework should have four key aspects, outlined by the Carnegie Foundation:[42]

- The overarching obligation to exercise care in relation to user harm;
- Risk assessment process;
- Establishment of mitigation measures; and
- Ongoing assessment of the effectiveness of the measures.

We should follow the example of the EU and the UK of imposing a legally binding duty of care on digital services to identify, mitigate, and manage risks of harm to children from illegal content and illegal activity. These can include – age verification, parental control tools, mandatory measures to detect and report individuals engaged in predatory behaviour to authorities, mandatory measures to detect and report child exploitation to authorities, and tools for minors to signal abuse and obtain support.

As many others submitted in the previous inquiry, including Dr Michael Salter and the Centre for Digital Wellbeing, a legally enforceable compulsory duty of care should be placed on digital platforms.

It should not be controversial to require this. Just as one example, Snap's global revenue from minors in 2023 was $437 million USD.[43]

But children's experiences on the internet are far from safe. Findings from the first Childlight Global Index of Child Sexual Exploitation and Abuse Prevalence (2024) include:[44]

- Over 300 million children under 18 have been affected by OCSEA in the past 12 months.

---

[42] Carnegie UK (2022). *Submission to the House Select Committee on Social Media and Online Safety*.
[43] Goggins, Ben (29 Mar 2024). Big Tech companies reveal trust and safety cuts in disclosures to Senate Judiciary Committee, NBC News https://www.nbcnews.com/tech/tech-news/big-tech-companies-reveal-trust-safety-cuts-disclosures-senate-judicia-rcna145435
[44] Childlight (2024). *Into the Light: Childlight global index of child sexual exploitation and abuse prevalence.* https://childlight.org/sites/default/files/2024-05/executive-summary.pdf

- 1 in 8 children globally experienced online sexual solicitation, and 1 in 8 experienced non-consensual taking, sharing, and/or exposure to sexual images or videos.
- 11% of men in the USA, 7% of men in the UK and 7.5% of men in Australia report having engaged in online child sexual abuse offending at some point in their lifetime. Most frequently this involves flirting or having sexual conversations with a person below the age of 18 online, followed by knowingly and deliberately viewing sexual material of a child below the age of 18.

The Australian Institute of Criminology found in new research that online predators are targeting parents who share photos of their children on social media, asking questions of a sexual nature about children they know, making requests and offers of payment for sexual images, and pressuring people to provide the images.[45]

We also support the addition of the statutory requirement for all aspects of the industry to act in the best interests of the child.

The situation for children is worsening, for example with the Internet Watch Foundation reporting a 360% increase in the instances of 'self-generated' sexual imagery of 7-10 year olds from 2020 to 2022. Research into paedophile users of the dark web revealed 45% of respondents disclosing that they mostly seek abuse imagery of children aged 4-13 years.[46]

Platforms must be able to demonstrate that their services are focused on the best interests of the child. We agree with the National Children's Commissioner's suggestion in their submission to the previous inquiry that this should include protection from harm, considerations of privacy, security of personal data, the ability to seek, receive and convey information, and a voice to express their views. Practices that infringe upon children's rights should be prevented.

33. Should Australia consider introducing a cost recovery mechanism on online service providers for regulating online safety functions? If so, what could this look like?

> Recommendation: Industry should be contributing to law enforcement, police training, education and tools to ensure that victims are supported and justice is done.

---

[45] Doran, Matthew (1 May 2024). Shocking survey into online predators prompts warning to parents about sharing photos of kids online. *ABC News*. https://www.abc.net.au/news/2024-05-02/parents-urged-to-think-twice-about-posting-photos-of-kids-online/103795196; Original research published here: Savannah, M., Burton, M., Trengove, M. et al. (2024). Prevalence and predictors of requests for facilitated child sexual exploitation on online platforms. *Trends and Issues in Crime and Criminal Justice No. 692.* Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti77406

[46] WeProtect Global Alliance (2023). *Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response.* https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf

In principle we believe that online service providers should contribute costs for regulating online safety functions. However we also propose that industry should be contributing to law enforcement; police training, education and tools to ensure that victims are supported and justice is done, as we have outlined in question 16.

Collective Shout
June 28, 2024