E-Safety Online Safety Bill concerns

This bill is important to the livelihoods of specifically sex workers in any of the five eyes countries. This will put the products sex workers use to advertise, communicate, screen and organise at risk. Like the FOSTA/SESTA package, the Online Safety Bill will have chilling effects for sex workers and other marginalised communities worldwide.

These are the concerns we have identified over the past few days. This is in no way an exhaustive list as the bill is over 200 pages long (with supplementary legislation, the Broadcasting Services Act (BSA) of 1992). We are ne

w to many of the US anti CSA and anti trafficking orgs mentioned, so we do encourage you to share any info you have regarding these organisations and their links to governing bodies.

The Australian peak sex worker body, Scarlet Alliance has put together a fantastic and easy to digest guide to the bill and how it will affect specifically sexual content: https://scarletalliance.org.au/library/online_safety_bill_2020 We recommend reading this before reading our concerns so you have some context. Our concerns are listed below.

You can find the full draft bill and submission details over here https://www.communications.gov.au/have-your-say/consultation-bill-new-online-safety-act

We encourage you to raise awareness of this bill and make a submission before **Sunday the 14th of February 5:00PM AEST (Sunday Feb 14,1:00AM EST)** via: Scroll to the bottom of https://www.communications.gov.au/have-your-say/consultation-bill-new-online-safety-act) Submissions are public so please be aware of this when submitting. You can request to submit anonymously.

Issues with the commissioner and the commission:

- The eSafety commissioner is Julie Inman Grant, this is a 5 year appointment which started in 2017.
- She is US born and raised, appears to be exporting similar US conservative values that led to the passing of FOSTA/SESTA
- Previously worked for large silicon valley companies such as Twitter, Adobe and Microsoft.
- Her whole career has been spent working with government agencies. We do not think it's appropriate that someone who has been lobbying for large self interested silicon valley private interest.
- Was a lobbyist (https://www.childdignity.com/podcasts/2019/12/16/safeguarding-podcast-safety-by-design-with-julie-inman-grant)
    - joined Microsoft as their first lobbyist in Washington DC in 1995
- On the E-safety website sexually explicit content is listed as other prohibited content they may investigate despite sex work being legal in the majority of Australia.

  "**You can report child sexual abuse material to us. We may also investigate complaints about other prohibited material, for example, content that:**
    - promotes in matters of crime or violence
    - provides instruction in paedophilia
    - advocates terrorist acts
    - depicts gratuitous depictions of violence and sexual violence
    - is sexually explicit."
- While e-safety commissioner, referred to Australia as a "penal colony" in 2019
    - "I also worked on the first White House summit on online safety when Clinton was in the White House. So fast forward five years and a bruising engagement with the Government later, Microsoft sent me out to the formal penal colony in Australia to sort out their community affairs, industry and government relations programs, which I expanded to cover safety, privacy and security across Asia Pacific through 2009. And then I finished up with

them working as their global lead on internet safety and privacy outreach out of Redmond."

- She has explicitly mentioned OnlyFans when talking about the increase in "sextortion" content: https://twitter.com/tweetinjules/status/1265585261695496192
    - She classifies sextortion as including cases of blatant scatter gun phishing and fraud attempts. These are lumped in with real cases of intimate partner violence. Scammers have also targeted other government agencies such as the Australian Taxation Office, Australian Federal Police and Medicare.
- The eSafety Commissioner is on the board of WEPROTECT
    - are they being paid for these positions on boards?
    - are they on the board as apart of their duties as eSafety Commissioner?
    - Are there any other boards or seats she currently holds directly as the e-safety commissioner?
    - WeProtect's current chair is Ernie Allen, Former President and CEO of the National Centre for Missing and Exploited Children (NCMEC) and the International Centre for Missing and Exploited Children (ICMEC).
    - The CEO of Thorn is also a board member of WeProtect. They work together, alongside INHOPE, UNICEF and more.
    - WeProtect links to Nicholas Kristoff's NYT's article as a resource on their website.
    - WeProtect is active in all of the five eyes countries plus more.
    - WeProtect has also been involved with Canadian regulation around csa online
    - The WeProtect Summit (apparently) was started by conservative UK Ex Prime Minister David Cameron in 2014. See: https://www.gov.uk/government/news/weprotect-summit-tackles-online-child-sexual-exploitation-on-global-scale

- DHS/ICE employee, Jim Cole, also US born and raised, is the chair of the victims identification group of the ACCCE, who is collaborating with the

esafety commission. According to the ACCCE newsletter, Cole took over as the chair in late 2019. Despite this, he does not list any affiliation with ACCCE or any Australian government entities on his linkedin. Aside from the ACCCE newsletter, we cannot find any current reports of his placement at the ACCCE.

    - Is this person operating in any function for or with the ACCCE?

- Minister for Home Affairs, Peter Dutton has endorsed the bill. We are concerned given his history attempting to provide a backdoor in encryption or platforms, to circumvent users privacy. (also see: https://www.afr.com/technology/facebook-and-encryption-experts-unite-against-sith-lord-dutton-20201023-p56814)

    - He has a terrible history with human rights violations in general. We are also fighting the "Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020" which will have consequences for journalists and activists in particular (https://www.gizmodo.com.au/2021/02/peter-duttons-latest-cyber-surveillance-law-has-senators-asking-questions/)

- There is no transparency about who will work with eSafety commissioner.
    - What is the team make up? (Cultural, ethnic, sexuality and gender)
        - will there be public transparency reports to ensure diverse makeup?

Issues with the bill regarding sex work:

- The bill is based on Australia's arcane classification and broadcasting regulation, which previously related to publications, computer games and broadcast media. A review is desperately required for the Classification (Publications, Films and Computer Games) of 1995 as we'll be importing broken and vague definitions. (See definitions at the bottom of this doc)
    - The Australian Law Reform Commission (https://www.alrc.gov.au/publication/classification-content-regulation-and-convergent-media-alrc-report-118/2-the-current-classification-scheme-2/assessing-the-current-scheme-2/) has stated that: "Stakeholders have identified aspects of the current classification and content regulation

framework that have become dysfunctional, are failing to meet intended goals, and create confusion for industry and the wider community."

- A single unelected individual defines what is considered "offensive", "abhorrent" and is able to set new industry standards for platforms and how they handle all content online with little or no oversight, transparency, or consequence.
    - The current window for objection to new industry standards is 30 days. This is not enough time for small business specifically to express their concerns took
- Civilian Investigators outside of the judiciary system will be used to execute the bill
    - What is the hiring process?
    - What level background check is performed?
    - Will a working with children check be performed?
    - What support is being provided to these civilian investigators in terms of on-going mental health and support?
    - Will there be a public transparent report on wrong doing by investigators and complaints the eSafety commissioner has received? (including general conduct)
    - Will these individuals be held to legal accountability in the case of wrong doing? (see police not being held to account: https://www.abc.net.au/news/2020-09-01/queensland-police-officer-who-leaked-wife-address-wins-appeal/12617810)
- Potential scope creep of this legislation into publicly considered non offensive content
- No definition in the bill was provided for "reasonable person", but the BSA states that "reasonable person" (or adult) is "*possessing common sense and an open mind, and able to balance personal opinion with generally accepted community standards*"
- How will they ensure the reporting of "offensive content" in this bill is not weaponised by individuals to target and harass sex workers and marginalised communities?

    - How will they ensure that the scope creep we saw during the US passing of FOSTA/SESTA, which censored queer communities, communities of color and sex education services as well as sex workers, does not occur in Australia and world wide?
- Why is sexually explicit content listed under reportable prohibited, harmful and illegal content on the e-safety website, despite sex work being legal in the majority of Australia?
    - Why is this considered prohibited and what is the eSafety definition?
    - Why is this considered harmful? What research is this based on?
    - Why is sexual explicit content listed alongside, "matters of crime or violence", "provides instruction in paedophilia", "advocates terrorist acts", "depicts gratuitous depictions of violence and sexual violence"

Issues with general privacy

- In prominent Australian publications, Julie Inman Grant has referenced the US First Amendment when speaking about regulating tech in Australia despite Australia not having a constitutional right to freedom of speech. (The US constitution shouldn't come into the conversation, as Australia is not governed as an extension of the US)
- A Canadian court ruled that Clearview AI was breaking the law due to collecting images of the general public without obtaining consent. Canada's Office of the Privacy Commissioner said its investigation found Clearview had "collected highly sensitive biometric information without the knowledge or consent of individuals," and that the startup "collected, used and disclosed Canadians' personal information for inappropriate purposes, which cannot be rendered appropriate via consent." (https://techcrunch.com/2021/02/03/clearview-ai-ruled-illegal-by-canadian-privacy-authorities/)
    - Does the eSafety office work with Clearview AI? If so, how long and how many times have their product been utilized in investigations?

- Why are commercial vendors being used? This just feeds further into the anti-sex industrial complex. Ultimately, these non governmental private vendors are making money off scraping content from private websites, breaking Terms of Service and removing power from every day people.
    - Does the eSafety office have any comments on how to manage the prosecution of vendors scraping and breaking terms of service?
- Does the eSafety office work with any vendors such as Thorn (Spotlight)?
    - When prompted, Thorn has failed to respond to privacy concerns and other queries held by the sex working community and digital rights organisations at the UN IGF and Hacking // Hustling at Harvard.
    - Can Thorn (And any other vendors used by eSafety) confirm they do not break terms of service by scraping websites for data for their commercial systems?
        - Do these vendors gain explitict consent from these websites and platforms to scrape the content of their users?

- In a 2019 speech at the WeProtect Plenary Sessions, Julie Inman Grant as the e-safety commissioner said "Our challenge is to scale and automate, using the best of AI and other emerging technologies"
    - Who has developed the AI?
    - Was this developed by an Australian government body or tendered out to private contractors?
    - Will there be algrothimic transparency across the working of any AI or machine learning projects? Including data sets used to train.
    - How will you ensure there is no systemic biases (including racial, sexuality, gender etc.) built into the processes and software used by eSafety Office? (including but not limited to AI, machine learning, facial and other biometrics, interagency cooperation, etc)
    - How will you ensure non consenting, non offending members of the public aren't included in these data sets?
        - Will people be notified if their content is added to these databases?

        - Will there be a process that individuals can go through to remove and permanently opt-out?
    - How will you ensure that these datasets aren't used to target and harm marginalised communities in now and in the future?
- Will all and any technical resources practice data sovereignty, stay and be hosted on Australian servers?
    - Will there be a public transparency report on who the vendors are?
    - Will the be a public transparency report on:
        - whose information is being provided (demographics for example)
        - how many times it was accessed?
        - when it was accessed?
        - and who accessed this information, such as WEPROTECT, Thorn, Australian Federal Police and other governmental agencies.
- Parental responsibility is being shifted from the parents onto technology platforms which may have differing views. For example, certain religions hold the belief` that queer people are inherently evil and tainted, and that any education provided would be wrong and immoral - see SafeSchools in Victoria, Australia and the recent banning of gay conversion therapy in Victoria, Australia) Queer children often rely on online sex education due to the lack of public sex education. According to WeProtect, they are also one of most at risk communities for CSA online.

Issues with the bill regarding digital spaces:

- Small business and communities running online spaces will struggle to comply, not only through timing of requests but ability to execute and appeal requests.
    - Will there be an appeal process and will it be multi-stake holder review?
    - Will there be exclusions based on network size? Such as the Privacy Act exclusions based on turnover or industry (such as, political parties)
- There are no protections guarding the implementation of backdoors or protection of encryption.

- Privacy concerns regarding age gatekeeping via ID collection or facial biometrics (especially if govt run or tendered out to a preferred govt contractor)
- Lack of multi-stake holder approach meaning that an unelected person (or delegate) is able to to define what is considered "offensive" and "abhorrent', and is able to set industry standards with little to no proper oversight, transparency or consequence
- Specific guidelines and frameworks to ensure that the goal post for enforcement and management is possible, but also platforms and communities know when they are potentially breaking the law?
    - Can the changes in the law be retroactively applied?
    - How do we ensure political and historically relevant content stays online and accessible, despite being "abhorrent" and "offensive", example - political unrest, such as the videos caught from the US insurrection or police brutality)
    - Will the eSafety office be held accountable to a service level agreement on appeals or communications with individuals, platforms or communities?

Statistics the current e-safety commissioner endorses:

Many of the statistics/studies used to create these pieces of legislation are vague and do not provide transparency around research methods, sources or terminology, resulting in misleading and inflated numbers. For example, please see the 2019 WeProtect Global Threat Assessment: https://www.weprotect.org/wp-content/uploads/WPGA-Global-Threat-Assessment-2019.pdf

- Little to no transparency regarding research methods used to obtain CSA statistics. Key issues include:
    - Who conducted the research used to create this bill? What were their research methods?
    - Where can we find these studies as they don't seem to be listed on the e-safety website?
    - Were they an Australian based research team?

- How many images were shared from minor to another minor?
- How many incidents were classified as non malicious ie were families putting uncensored bath photos of their children on facebook? Minors dancing on tiktok etc.
- How many of these reports are determined to not be actionable?
- How many of those reports go on to a take down request?
- Have any of these been prosecuted? If yes, how many?
- How many of these reports are repeats of the same content?
- How many leaders or operational members of pedophilia rings have been prosecuted?
- Can you provide a clear explanation of what the e-safety team deems to be child exploitation material?

Given the track record of some of these anti trafficking organisations who work with WeProtect using false/misleading statistics around child sex trafficking:

- How do we know this isn't the case here given the lack of transparency around statistics used by Grant and WeProtect in an effort to expand surveillance or/and the e-safety commission? (**For example, despite statistics used by orgs such as these, according to the FBI, there were only 12 confirmed cases of domestic sex trafficking involving a minor for the entirety of 2019 in the US.**)

Bare minimum improvements:

- Sunset clause for review
- Commit to legislate changes to the Broadcasting Services Act to provide clearer, fairer and less vague classification tiers, in consultation with the wider community.
- Public transparency reports broken down to provide meaningful and accurate information.

- Multi-stake holder consultations from marginalized communities practicing harm reduction (not just big tech companies or not for profits with financial gains tied to the project, such as WeProtect) should be engaged on all industry standards and be involved in the appointment of the eSafety core team + commissioner.
- Time for consultation and objection to industry standards must be increased from 30 days to 90 days.
- Specific protections for encryption and to prevent backdoors.
- Many conversations about "ending CSAM" however, there is no mention in the bill of addressing the causes of CSAM:
    - education for parents and caregivers around what is socially acceptable and legal to share via internet platforms
    - sex, consent and internet safety education for minors and parents
    - public sex education for queer children so they don't have to rely on online sex education
    - consent is viewed through a binary lens, which dismisses any change in consent or nuance
    - treating people experiencing attraction to minors as a preventative public health issue instead of demonising those who have not offended. In supporting these individuals, we acknowledge the problem exists and with the guidance of harm reduction experts & mental health professionals to mange their feelings.
    - despite CSA and child exploitation being perpetrated by individuals often close to the victim, there is little to no information on combating this in a tangible way or efforts being made to address this.

Definitions of terms used in the Online Safety Bill from the guidelines for the classification board:

https://www.legislation.gov.au/Details/F2008C00129

The definitions in the online safety bill, allow for significant overreach. These are the current definitions of key terms in the bill according to the *Classification (Publications, Films and Computer Games) Act 1995*

Demean: A description or depiction, directly or indirectly sexual in nature, which debases or appears to debase the person or the character depicted.

Fetish: An object, an action, or a non-sexual part of the body which gives sexual gratification. Mild fetishes include stylised domination and rubberwear. Stronger fetishes include bondage and discipline.

Offensive: Material which causes outrage or extreme disgust. The Guidelines distinguish between material which may offend some sections of the adult community, and material which offends against generally accepted standards, and is therefore likely to offend most people.

Reasonable Adult or Person: Possessing common sense and an open mind, and able to balance personal opinion with generally accepted community standards.

Revolting and abhorrent phenomena: Fetishes or practices, sometimes accompanied by sexual activity, which are considered offensive.

In Summary

As a technology company, we are not trying to shirk responsibility but systemic abuse cannot be fixed by just regulating technology companies. This is a larger problem. We need more education, less moral policing and more social support programs to facilitate permanent change within our communities. The regulation necessary to tackle serious issues such as white supremacy and CSA needs to be developed by a non partisan, multi-stakeholder committee inclusive of the marginalised communities most at risk of harm due to legislation such as the Online Safety Bill.

The idea that hateful rhetoric expressed by white supremacist should be tolerated, treated with civility and given space in the public domain is harmful when you consider sex workers and other marginalised groups are often the victims of white supremacists and the systems that they create.

Especially online, they are unduly punished for trying to survive, pushed out of the public eye and unable to access vital resources. As demonstrated in the proposed Online Safety Bill, they have been ignored, infantilized and their concerns suppressed over the welfare of other groups, by government and not-for-profit organisations that have financial stakes in their oppression.

Action items: We have put together a small list of action items if you are concerned and want to help:

- Make your own submission which closes on **Sunday 14th of February 2021 5:00PM AEST (Sunday Feb 14,1:00AM EST)** (Scroll to the bottom of https://www.communications.gov.au/have-your-say/consultation-bill-new-online-safety-act) Submissions are public so please be aware of this when submitting. You can request to submit anonymously, but please know the body of your submission will still be uploaded.
- If you have an Aus userbase, please notify them and ask them to call their local federal member to express concern and make a submission.
- Amplify tweets by leading bodies (ie Scarlet Alliance, Digital Rights Watch AU) or send out your own tweets. We are also hoping to put together a thread of our concerns via the Assembly Four Twitter.
- Does anyone have reliable statistics on the existing rates of CSA? (or other research you think would be relevant)
- Please reach out to us if you have any advice around tackling this type of legislation given it's similarities to FOSTA/SESTA.

Links and further reading:

- You're wrong about human trafficking statistics: https://podcasts.apple.com/us/podcast/human-trafficking/id1380008439?i=1000465289965, https://podcasts.apple.com/us/podcast/wayfair-and-human-trafficking-statistics/id1380008439?i=1000487756926

- Surveillance and the anti trafficking movement: https://observer.com/2019/11/sex-workers-mass-surveillance-big-tech/
- The fallout of FOSTA/SESTA; https://www.antitraffickingreview.org/index.php/atrjournal/article/view/448/364
- https://gaatw.org/ATR/AntiTraffickingReview_issue14.pdf
- https://www.sbs.com.au/news/the-feed/opinion-australian-sex-workers-respond-to-fosta-sesta#:~:text=A recently introduced law in,over the world%2C including Australia.&text=In April 2018 a bill,US known as FOSTA SESTA.