Prostasia Foundation
18 Bartol Street, #995
San Francisco, CA 94133

info@prostasia.org
Ofc:+1 415 650 2557
Mbl:+1 510 480 8449
https://prostasia.org

Vicki Buchbach
Director, Online Safety Reform and Research Section
Department of Infrastructure, Transport, Regional Development and Communications
GPO Box 2154
Canberra ACT 2601

September 16, 2021

Dear Ms Buchbach,

Draft Online Safety (Basic Online Safety Expectations) Determination 2021

Prostasia Foundation is a child protection organization that promotes the prevention of child sexual abuse and contributes towards funding of prevention research. Complementing this mission, we also critique laws and policies that purport to be driven by a desire to protect children, but that are not evidence-based, or would infringe human rights.

In this context, we are concerned that the Draft Online Safety (Basic Online Safety Expectations) Determination 2021 would enact restrictions on the use of the Internet that are vague, uncertain, and overbroad. These restrictions could not be implemented without massively restricting both freedom of expression and privacy online. This would primarily harm the most marginalised members of society, while failing to make children safer.

In this submission, we only address areas in which the Basic Online Safety Expectations exceed the minimum standards specified in the Online Safety Act 2021. Our broader objections to the Online Safety regime were set out in our response to the consultation draft of the Online Safety Bill[1]—which, like hundreds of other submissions to that consultation, was afforded a mere 10 days of review before being ignored with the passage of the Online Safety Act unchanged.

Our bottom-line recommendation is that paragraphs 7, 8, and 9 of Division 2 of the Draft Online Safety (Basic Online Safety Expectations) Determination 2021 be deleted in their entirety.

[1] Prostasia Foundation Submission to Australian Online Safety Bill consultation (February 11, 2021), available at https://prostasia.org/wp-content/uploads/2021/02/Australian-Online-Safety-Bill-consultation.pdf.

Part 2—Basic Online Safety Expectations

It is appropriate that Internet companies should take measures aimed at preventing the use of their platforms to disseminate content that is demonstrably illegal. For example, many service providers successfully utilise hash scanning technologies to filter out attempted uploads of known unlawful sexual images of minors. Prostasia Foundation supports these efforts.

But Part 2 of the Draft Determination, in Division 2, imposes a much broader and vaguer expectation in paragraph 7 that providers should "proactively minimise the extent to which material or activity on the service is ***or may be*** illegal ***or harmful***" (emphasis added). This is a significantly broader target than that of the Online Safety Act 2021, and describes a significantly more difficult standard to apply fairly and consistently.

In a joint article with human rights group Article 19 published in 2020 addressing the UK Online Safety Bill and the U.S. EARN IT Act—both similar laws to Australia's Online Safety Act—we described why an approach that appoints Internet platforms to take responsibility for online harms is misguided and dangerous:

> We can't expect that harm prevention can be successfully accomplished with the same single tool from the regulatory toolbox that we use to eliminate illegal content. The various harms that manifest themselves online are so vastly different that many different tools will be needed. Internet companies cannot take the place of sex educators, therapists, social workers, researchers, media literacy experts, and parole officers—and we should be fearful about the government encouraging them to attempt to do so.
>
> Relying on speech regulation to address a broad range of online harms is shortsighted. The ability of governments to regulate speech is very limited—and rightly so. Laws such as EARN IT and the Online Harms legislation are intended to circumvent these limits, by deputizing Internet companies to act on the government's behalf. But the more directly a law tells Internet companies how to police speech, the more constitutionally dubious it is. The more indirectly it does so, the more worried we should be about whether companies will act in a fair and accountable way.[2]

Given the amount of content that is uploaded to major Internet platforms every day—millions of images, videos, and text posts—there is simply no means available to determine proactively what content "may be illegal," let alone "may be harmful." Automated scanning technologies are the only option to proactively review content at scale, and these technologies simply do not have the capacity to make such context-dependent, subjective judgments.[3]

When faced with an impossible expectation such as this, we know from experience what response risk-averse providers will take: they will over-restrict content, by imposing blanket restrictions on sensitive topics such as sexuality, that will disproportionately restrict the speech of marginalised communities. For example, even the much more narrowly tailored law FOSTA/SESTA in the

---

[2] https://prostasia.org/blog/internet-companies-alone-cant-prevent-online-harms/

[3] See CDT (2021). *Do You See What I See? The Capabilities and Limitations of Automated Multimedia Content Analysis*, available at https://cdt.org/press/new-cdt-research-report-highlights-limits-of-automated-content-analysis/.

United States, which directly targeted only sex trafficking, resulted in platforms banning legitimate content such as dating forums, sex education material, and abuse prevention resources.[4] Such overbroad censorship will not make the community safer—quite the opposite.

Division 2 goes on in paragraph 8 to specify that providers of encrypted services are expected to "detect and address material or activity on the service that is or may be unlawful or harmful." While this expectation was already impractical to fulfil in the cases of non-encrypted services, the difficulty is compounded in the case of encrypted services. Even Apple's recent proposal for client-side scanning of its encrypted messaging service for child abuse images—which was widely criticized before being put on hold[5]—was only aimed at detecting images that were *known* to be illegal. The expectation that providers should be able to detect material or activity that "may" be illegal, or even merely "harmful," is fanciful. This provision appears to be an attempt to enact a *de facto* ban on end-to-end encryption, in clear contravention of international human rights norms.[6]

The same considerations apply to paragraph 9, which specifies that providers should prevent anonymous accounts from being used for "material, or for activity, that is or may be unlawful or harmful," going on to specify that appropriate measures to be taken could include "having processes that require verification of identity or ownership of accounts." The contradiction here hardly needs to be pointed out. The right to be anonymous online has been recognised at the United Nations.[7] Abridging that right will fall most heavily on those who depend upon it the most—including those such as victims of domestic violence and abuse whose interests this instrument claims to serve.

Conclusion

We recommend that paragraphs 7, 8, and 9 of Division 2 be deleted in their entirety. These provisions, which would significantly expand the effective scope of the already overbroad Online Safety Act, cannot be implemented without causing grave harms to both freedom of expression and privacy online. Children's safety online is a community responsibility, not something that we can or should delegate to Internet companies. Government should be investing more in education, research, social services, and support to improve child safety online, rather than censoring speech.

Yours sincerely,

Jeremy Malcolm
Executive Director

---

[4] Amicus Brief of Prostasia Foundation et al in support of Appellants in *Woodhull Freedom Foundation v United States*. 20 February, 2019, available at https://prostasia.org/wp-content/uploads/2019/02/Freedom-Network-AmicusBrief.pdf.

[5] Whittaker, Zack. "Apple delays plans to roll out CSAM detection in iOS 15 after privacy backlash", *Techcrunch*, 3 September 2021, available at https://techcrunch.com/2021/09/03/apple-csam-detection-delayed/

[6] United Nations Office of the High Commissioner for Human Rights, *Human rights, encryption and anonymity in a digital age* (1 July 2015), available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

[7] United Nations Office of the High Commissioner for Human Rights, *op cit*.