5 July 2024

Director – Strategy and Research
Online Safety, Media and Platforms Division
Department of Infrastructure, Transport, Regional Development, Communications and the Arts
Canberra ACT 2601

By email: OSAReview@COMMUNICATIONS.gov.au

Dear Director,

Statutory Review of the Online Safety Act 2021

Thank you for the opportunity to provide our views to the *Statutory Review of the Online Safety Act 2021* (Statutory Review) and accompanying Issues Paper (Issues Paper).

About IAB

The Interactive Advertising Bureau (IAB) Australia Limited is the peak trade association for digital advertising in Australia. IAB Australia was established in 2005 and is one of over 45 IAB offices globally.

Locally there is a financial member base of approximately 180 organisations that includes media owners, platforms, media agencies, advertising technology companies as well marketers. The board has representation from the following organisations: Seven West Media, Nine, Guardian News & Media, News Corp Australia, Google, Meta, Yahoo, Carsales, REA Group, Domain.

Key concerns in relation to online safety

IAB Australia supports the Government's commitment to protecting Australians online and ensuring that the Online Safety Act keeps pace with the evolving online environment. IAB would like to make submissions on two questions raised in the Issues Paper:

- What considerations are important in balancing innovation, privacy, security, and safety? (Part 6, Q28)
- Should the Act have strengthened and enforceable Basic Online Safety Expectations? (Part 2, Q4)

We set out our concerns in relation to these questions below.

1. Considerations in balancing innovation, privacy, security and safety - Exclusion targeting

Question 28 of Part 6 of the Issues Paper asks, "What considerations are important in balancing innovation, privacy, security, and safety?" In our view, an element that is not discussed in the Issues Paper but that we think should be considered, is that the practice of 'exclusion targeting'. Exclusion targeting is the subject of a proposal in the 'Privacy Act Review Report' (see below for further commentary), and in our view it is a relevant to consider in the context of the Statutory Review due to the tension between what is being proposed under reforms to the *Privacy Act 1988 (Cth)* (Privacy Act), and the objects of the Online Safety Act, which are to improve and promote online safety for Australians.[1]

Exclusion targeting refers to the use of data to exclude individuals or categories of individuals from seeing certain content or advertising. It is a key technical tool available to our industry to prevent

[1] *Online Safety Act 2021(Cth)*, Section 3.

advertising or other material being served to individuals, where that might be inappropriate or have the potential to cause harm to those individuals (or cohorts of individuals).

While the Issues Paper notes that online platforms can be used to 'promote content that may be harmful';[2] it is important to note that the same practices (that is, the inclusion of data in cohorts or segments) that are used to serve groups of consumers with advertising or other material, are also used to withhold material from individuals, for the purposes of implementing online safety laws and policies.

For example, exclusion targeting may be used to prevent age-inappropriate advertising being served to under 18s, to prevent certain high risk financial products being advertised to vulnerable individuals or demographics, or to facilitate in the serving of individualised communications to vulnerable customers, as may be required by law.[3]

As noted, exclusion targeting is currently the subject of a proposal in the 'Privacy Act Review Report'. The proposal is that individuals should be able to opt-out of the practice of 'targeting' – including targeting that has been undertaken for the purposes of withholding advertisements or content from an individual.[4]

While it is not entirely clear how this is intended to work in practice, we are concerned that, if individuals are able to simply opt-out of exclusion targeting, this would completely undermine organisations' online safety and harm minimisation policies, as well as various laws and regulatory instruments that require care to be taken to protect against competing harms.

In our view, this should also be considered in the formulation of amendments to the Privacy Act, to ensure that privacy and online safety are appropriately balanced within the regulatory framework. The proposed opt-out right should be more narrowly framed and should not enable a broad opt-out right in relation to exclusion targeting.

Recommendation: That the Department of Infrastructure, Transport, Regional development, Communications and the Arts engage with the Attorney-General's Department to remove the broad opt-out right in relation to exclusion targeting to ensure there are not contradictory approaches between the Privacy Act and Online Safety Act.

2. Considerations in balancing innovation, privacy, security and safety – privacy enhancing technologies

Another important consideration in balancing innovation, privacy, security, and safety, is ensuring that privacy law protections are not expanded to such an extent that they inadvertently disincentivise the development of new technologies and practices designed to promote a more safe and secure online ecosystem.

The industry is continuing to develop and improve technologies and innovations that make it easier to use and secure data, and to extract insights from data for a range of purposes, without the need the use or share the underlying personal information. For example, clean rooms are part of a group of Privacy Enhancing Technologies ('PETs'), that have been specifically developed to undertake critical online functions while protecting user privacy.

[2] Issues Paper, 52.
[3] For example, the National Energy Retail Law and Rules – see here.
[4] Privacy Act Review Report, 12.

Cleanrooms are used by organisations with an online presence to undertake critical business activities such as verification of data to ensure it is accurate and consistent, quality assurance of data, and to remove fake or fraudulent accounts. These activities are designed to both facilitate activities that maintain the security of systems and data sets, as well as protect consumer privacy.

In our view, use of these technologies should be incentivised by ensuring the Privacy Act clearly distinguishes between anonymised and de-identified data, and personal information. Overly expansive privacy laws risk undermining these activities that are designed to promote security online and would also disincentivise the development of new privacy enhancing technologies.

Recommendation: That the Department of Infrastructure, Transport, Regional development, Communications and the Arts engage with the Attorney-General's Department to ensure that the Privacy Act appropriately balances privacy with online safety and security, including by ensuring that the use of privacy enhancing technologies and cleanrooms are not impeded.

3. Basic Online Safety Expectations

Part 2, question 4, asks whether the Act should have strengthened and enforceable Basic Online Safety Expectations (BOSE).

IAB does not support this approach. The BOSE have been deliberately drafted to sit alongside the Online Safety Act, as a set of exceptionally broad expectations that encourage organisations across the economy to be proactive in relation to online safety. The drafting of the BOSE reflects this approach and, in our view, would give rise to a substantial amount of uncertainty in relation to the precise nature of the obligations that organisations would need to comply with, if these broad expectations were mandatory. For example, see our submission to the review of the BOSE amendments,[5] which made recommendations including that:

- The scope of the obligations in relation to recommender systems and transparency reporting be clarified and substantially narrowed:
    - to more specifically reflect the concerns raised in the *Online Safety (Basic Online Safety Expectations) Determination 2022 Consultation Paper*;
    - so that online service providers can better understand their intended operation; and
    - to ensure that they don't overlap or conflict with other regulatory obligations and reporting requirements.
- Further guidance and clarity be given in relation to the obligation that service providers assess whether 'business decisions' will have a 'significant adverse impact on the ability of end-users to use the service in a safe manner'.

Our concerns in relation to the framing of the BOSE remain. We therefore consider that the existing framework where the e-Safety Commissioner can require online service providers to respond to a notice and prepare and publish a statement of non-compliance with one or more expectations, is more appropriate, given the nature of the expectations.

Recommendation: That the existing approach to the BOSE should not be amended as proposed by Part 2, Question 4.

[5] IAB submission, *Amending the Online Safety (Basic Online Safety Expectations) Determination 2022*, 26 February 2024.

Contact

Please contact me on [redacted] if you have any questions or would like to discuss any of the issues raised.

Yours sincerely,

[redacted]

Sarah Waladan
Director of Policy & Regulatory Affairs
IAB Australia