

18 June 2024

Online Safety Act 2021: Statutory Review

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

Email: <https://www.infrastructure.gov.au/have-your-say/>

Statutory Review of the *Online Safety Act 2021*

Internet Australia appreciates the opportunity to respond to the Department’s Statutory Review of the *Online Safety Act 2021 (the Act)*.

Internet Australia acknowledges the growing threat of online harm, particularly to children and young people. Any Government response to those harms, however, must be balanced with the human rights of all Australians. We also call for an appropriate balance between the industry’s need for certainty in responding to those harms and flexibility in responding to emerging forms of online harm. Finally, we support the eSafety Commissioner’s dual role in administering industry responses to online harms and providing education and an online complaints mechanism for the public.

Our specific comments on the Act are below.

Yours Sincerely

Holly Raiche
Chair, Internet Australia Policy Committee

About Internet Australia

Internet Australia is a not-for-profit organisation representing all users of the Internet. Our mission – “Helping Shape Our Internet Future” – is to promote Internet developments for the whole community's benefit, including business, educational, government, and private Internet users. Our leaders and members are experts who hold significant roles in Internet-related organisations, enabling us to provide education and high-level policy and technical information to Internet user groups, governments, and regulatory authorities. We are the Australian chapter of the global Internet Society, where we contribute to developing international Internet policy, governance, regulation and technical development for the global benefit.

Submission by Internet Australia

Balance in Online Safety Protections

Addressing online harms necessarily involves balancing protection from online harms against individual freedom of expression and interference with the privacy of individuals. The current version of the Act does not explicitly recognise that balance. Part 15 of the Act - ‘Disclosure of Information’- lists the circumstances in which the Commissioner may disclose information to the Minister, government and governmental authorities. Such disclosure can also be to parents, teachers, and school principals. Nothing in that Part requires the Commissioner to consider respecting the privacy of individuals, including children, when disclosing such information.

The Act also recognises freedom of expression. Still, it is buried in Part 16, titled ‘Miscellaneous,’ and simply states that the Act does not apply to the extent that it would ‘impinge any constitutional doctrine of implied freedom of political communication’.¹ The doctrine of implied freedom of political communication is one of the defences available under defamation legislation; its relevance in this Act is puzzling.

¹ Online Safety Act 2021 (The Act) s. 233 <https://www.legislation.gov.au/C2021A00076/latest/text>

The current ‘Objects of the Act’ only include the improvement and promotion of online safety for all Australians with no reference to human rights issues.² The UK Online Safety Act 2023 offers a better model. That Act requires that a balance be struck between protection from online harms, freedom of expression, and privacy. Providers of services covered by that Act must ‘mitigate and manage’ the risks posed by their online services and ensure those services are both ‘safe by design’ and ‘designed and operated in such a way that:

- A higher standard of protection is provided for children than for adults,
- Users’ rights to freedom of expression and privacy are protected, and
- Transparency and accountability are provided for those services.³

Recommendation:

The Act's objects should be amended to explicitly require that users’ rights to freedom of expression and privacy are respected when implementing protections under the Act.

Simplification of the Online Safety Act

Internet Australia is concerned that the Act's piecemeal development has resulted in a confusing structure, making it difficult to know how best to comply with its provisions.

In its current structure, the Act deals in some detail with the handling of four listed harms and the power of the Commissioner to deal with those harms.⁴ Followed with “Basic Online Safety Expectations” and required reporting by providers against those expectations.⁵ Parts five to eight then, again, list the four specific harms and measures that can be utilised to address those harms: cyber-bullying targeted at an Australian child, non-consensual sharing of intimate images, cyber-abuse material targeted at an Australian adult and material that depicts

² Ibid s. 3

³ *Online Safety Act 2023* UK, ss 2-3 <https://www.legislation.gov.uk/ukpga/2023/50/enacted>

⁴ The Act, Part 3

⁵ Ibid, Part 4

abhorrent violent conduct.⁶ Also applicable, we note, is the more general Online Content Scheme with its industry codes.⁷ That Scheme is similar to the existing Code scheme set out in Part 6 of the *Broadcasting Services Act*, providing for industry-developed Codes to address harmful material (Class 1 and Class 2 material). As in the *Broadcasting Services Act* code regime, this Commissioner has the power to set industry standards when the codes have proved not inadequate.⁸

The Act's structure should be more explicit; some harms are specifically addressed, with no process for including others. Some actions providers can take are detailed within sections on harms, others covered by the BOSE, with Codes or Standards providing more detailed industry rules on their responsibilities for specific harms. Some complaint mechanisms are within the particular sections on harm, and others are within code provisions.

One alternative provided by the UK Online Safety Act 2023, where online services subject to that Act are generally defined as either a 'regulated user-to-user service' or a 'regulated search service'.⁹ Duties of care are imposed on the provider of those services, including risk assessment of the services and protection, particularly for children, from those services. Assessment includes how services are used, the nature and severity of harm that might be suffered, and the design of the services that may protect users. Those duties include duties to protect content of democratic importance, duties to protect news publishers and journalistic content and duties to protect freedom of expression and privacy.¹⁰

The Irish online content regulation also provides a model for dealing with known and emerging online harms. The Act includes definitions of known existing harms and allows for additional harms that meet the risk test involving a person's life or 'significant harm' to a person's mental or physical health, which are then proposed to the Minister for inclusion in the Act.¹¹

⁶ Ibid, Parts 5 to 8

⁷ Ibid Part 9

⁸ *Broadcasting Services Act 1992* Part 6; The Act Part, Division 7

⁹ Online Safety Act 2023 UK s. 4 <https://www.legislation.gov.uk/ukpga/2023/50/2024-04-01>

¹⁰ Ibid, See Chapter 2 for list of duties <https://www.legislation.gov.uk/ukpga/2023/50/enacted>

¹¹ Online Safety and Media Regulation Act 2022, Ss 139A and 139B
<https://www.irishstatutebook.ie/eli/2022/act/41/section/45/enacted/en/html#sec45>

In both cases, while some harms may be set out in legislation, there are clear guidelines for defining what constitutes online harms, clear responsibility of service providers to identify and address harms, and precise mechanisms for bringing emerging forms of harm under the relevant legislative regime. Mechanisms for industry responsibility to address those harms, with regulator oversight, are then provided.

The Australian Act needs to clarify the definition of harms, industries' responsibilities for those harms, and the power and responsibility of the eSafety Commissioner to respond to those harms. This should be completed by the ability of the public to make complaints to the Commissioner concerning online harms and the ability of the Commissioner to respond to those harms. Those changes would provide more clarity and certainty for the industry, more flexibility for the Commissioner, and more comprehensibility for the scheme for the public.

Recommendation:

The Act should be restructured to include a section with definitions of specific online harms and a mechanism – including Parliamentary oversight - for adding other online harms as they emerge. The following section should detail the industry's responsibility concerning those harms. This can be done by including Basic Online Safety Expectations and industry Codes and standards to address those harms. The Act should then cover the powers of the eSafety Commissioner, which should consist of specific responsibilities concerning the identification of online harms, oversight and enforcement of industry codes and standards, and the power of the Commissioner's office to handle complaints about those harms. Those complaints could be divided between complaints about harms deliberately targeted at an individual and the more general harmful material available online. For complaints targeted to one or a few individuals, complaints would have to be made by that individual, their parent or guardian, or someone authorised by the individual. The general public could make other complaints. Finally, information on how individuals could protect themselves from online abuse should be included.

Relationship between the Broadcasting Services Act 1997 and the Online Services Act 2021.

The Act includes the statement that: ‘This Act does not limit Schedule 8 to *the Broadcasting Services Act 1992*.¹² Schedule 8 of that Act is titled ‘Online Content Services’. The simplified outline of Schedule 8 appears to confine the operation of the Schedule to the ACMA, making rules about ‘gambling promotional material ... in conjunction with live coverage of a sporting event’.¹³ However, nothing else in that Schedule appears to confine service provider rules made under that part to ‘gambling promotional material’. Indeed, Part 2 of Schedule 8 allows the ACMA to make rules for prescribing matters required or permitted by this Act to be prescribed by the online content service provider rules.¹⁴

Recommendation:

Schedule 8 of the Broadcasting Services Act be amended to restrict the ACMA’s power to make service provider rules only in relation to online gambling promotional material in conjunction with live sporting events.

Penalties

Table 4.1 of the Issues Paper demonstrates that monetary penalties available to the Commissioner are well below those available to the relevant regulator in other jurisdictions. In other jurisdictions, available penalties are generally based on their annual turnover or a set sum, whichever is the larger. This is preferable to penalties of a set sum which cannot reflect on the size and reach of the provider.¹⁵

¹² The Act, s. 231

¹³ The Act, Schedule 8, Clause 1.

¹⁴ The Act, Schedule 8, Clause 11

¹⁵ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Statutory Review of the Online Safety Act 2021: Issues Paper (Discussion Paper)* Table 3.2.

Recommendation:

The penalties available to the Commissioner should be a percentage of the provider's annual turnover and apply each day the contravention continues.

Continuing IA concerns with Online Safety legislation

Internet Australia has participated in consultations on the online safety regime as it has developed. In addition to the above recommendations, we continue to have concerns about issues raised in those consultations.

Encryption

One of our deep concerns was the possibility, raised in draft standards, of proactive detection obligations on service providers to scan content to remove harmful material by what is termed 'client-side scanning'. We appreciate the eSafety Commissioner's assurances that her office is not advocating building weaknesses or 'back doors' to undermine end-to-end encryption services. However, that does not rule out what is called client-side scanning. We continue to urge the Commissioner against approval of any Codes or Standards that would compel the industry to undermine end-to-end encrypted services and the security they provide.

Determination of harms

The eSafety Commissioner must be flexible in determining whether new online harms have developed. In making those determinations, the eSafety Commissioner must consult widely with industry participants, particularly smaller providers with fewer resources, to address new requirements for handling online harms.

Structure of the eSafety Commissioner's Office within the ACMA

The Discussion Paper asks about the continued structure of the eSafety Commissioner within the ACMA's structure. In responding to the 2020 Review of the eSafety legislation, IA supported (and continues to support) the eSafety Commissioner's Office retention within the ACMA structure. As we argued at the time:

'The ACMA already has significant roles in online safety, including defining and addressing harmful content and providing education programs to promote online safety. A continued merging of the knowledge and resource base by the Commissioner's office and within the ACMA more broadly would be more efficient, more appropriate for sharing knowledge and experience, and less of a drain on Commonwealth resources than creating a new separate entity.'

Internet Australia Endorsement for the Input received as a submission from the Internet Society

Internet Australia is a National Chapter of this global Organisation and has worked in close association with the staff and community that has developed their input; as such and as an integral part of our submission, we wish to note our endorsement of the Internet Society's input and include in our submission copy and reference to the specific recommendations made by this internationally recognised global technical sector peak body:

'We strongly urge the Australian government to amend the Online Safety Act to add:

Section 24A: Nothing in this Act should cause services to weaken the security or confidentiality of encrypted communications or stored data.

Section 145(1C): The Commissioner must not determine a standard under subsection (1) that requires or otherwise encourages or causes participants in an online industry to engage in scanning of the content of end-to-end encrypted communications.'