Client Alert

May 2024

Australia: Online Safety – Statutory review issues paper and Pilot of Age Assurance Technology

In brief

On 29 April 2024, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts opened public consultation as part of the ongoing independent statutory review ("**Review**") of the *Online Safety Act 2021* (Cth) ("**Act**") with the release of an Issues Paper ("**Issues Paper**"). For more information about the Review other related developments in the Australian online safety roll-out, please view our previous alerts here and here.

The Review is extremely broad ranging.

Public consultation will close on 21 June 2024, with the final report of the Review expected to be provided to Government by 31 October 2024.

Online safety remains a key topic of public debate and regulatory focus in Australia. In addition to the Review, and other recent developments such as classification reform, anti-doxxing and hate speech proposals, the Government recently announced it would take additional steps to address online harms relating to misogyny and violence against women, including a pilot of age assurance technology to protect children's access to pornography and other harmful content.

Contents

Key takeaways

- The Review is very broad and will consider the operation and effectiveness of the Act, including possible increases in scope, penalties and enforcement powers.
- A new statutory duty of care on providers of online services towards their users is being considered.
- The review provides a significant opportunity for industry participants and other interested parties to share their views with regard to the operation of the Act to date, and the various other matters within the scope of the Terms of Reference.
- In an effort to prevent violence against women and tackle misogyny, the Government has announced new measures to address online harms including approving a pilot of age assurance technology, and announcing the introduction of legislation specifically targeting deepfake pornography. This will occur in parallel with the Review, the development of Phase 2 Industry Codes and other recent developments around classification reform, anti-doxxing and hate speech proposals, some of which will now be fast tracked.

In depth

Issues Paper

The Issues Paper reflects the broad scope of the Review, and poses a range of consultation questions in five categories. Key points considered in the Issues Paper are outlined below.

Australia's regulatory approach to online services, systems and processes

- This section of the Issues Paper focuses on the operation of the two systems-focussed schemes within the Act, being the:

- Codes and Standards under the Online Content Scheme; and
- Basic Online Safety Expectations (BOSE),

and the scope and definition of the providers covered by each. (The Issues Paper focuses on the complaints/content-based removal and blocking mechanisms in the following section, as described below.)

- It compares the approach taken under the Act to international approaches in the United Kingdom, the EU, Ireland and Canada.
- The consultation questions regarding the operation of the Act, and these systems-focused schemes in particular, are extremely broad. Some key consultation questions of particular interest cover:
  - Whether the BOSE should be strengthened and become enforceable (presumably to make the expectations themselves mandatory, and subject to penalties for breach);
  - Whether there should be changes to who can draft Industry Codes under the Online Content Scheme and whether they should be extended to cover additional harms; and
  - Whether regulatory obligations should depend on a service provider's risk or reach.

Protecting those who have experienced or encountered online harms

- This part of the Issues Paper focuses on:
  - The four complaints/content-based removal notice schemes under the Act (for non-consensual sharing of intimate images, child cyberbullying, adult cyber-abuse and the complaints-based elements of the Online Content Scheme); and
  - The mechanism for the blocking of material depicting abhorrent violent conduct.
- This review of the Online Content Scheme (as it relates to child access to pornography and other high impact material) overlaps and interrelates significantly with the current classification reform process, development of the Phase 2 Industry Codes under the Act and the newly announced trial of age assurance technology discussed further below.
- The consultation questions here are again extremely broad. Some key consultation questions of particular interest cover:
  - Whether the complaints schemes operate effectively and easily for end-users including:
    - Whether thresholds for making complaints are appropriate. For example, the Issues Paper notes that the threshold for "adult cyber-abuse" is extremely high, limited to the most abusive material intended to cause serious psychological or physical harm;
    - Whether more needs to be done to provide vulnerable Australians at highest risk of abuse with corrective action under the Act; and
    - Whether the Act should empower "bystanders" or members of the public to make reports to eSafety; and
  - Whether existing powers to remove class 1 material should be supplemented with new provisions similar to the "post and boast" (or similar) legislation recently announced or considered in a number of Australian jurisdictions (namely legislation aimed at people who carry out criminal or violent acts and then boast about them on social media).

Penalties, and investigation and information gathering powers

- The Issues Paper notes that Australia's penalties regime has not kept pace with newer regulatory regimes adopted by Ireland, the UK and the EU which apply significantly higher penalties, including penalties based on a percentage of a platform's global revenue.
- Moreover, the Issues Paper raises the concern that penalties under the Act may not strike a balance between offences, for example, "the maximum penalty for failing to take down illegal material such as child sexual exploitation material or pro-terror material is the same as for failure to take down harmful but not unlawful material".
- It also raises the practical challenge of enforcing the Act and its penalties regime against individuals or platforms based overseas.

- Some key consultation questions of particular interest cover:
  - Whether the Act should include stronger investigation, information gathering and enforcement powers;
  - Whether current penalties are adequate;
  - What could be done to enforce action, particularly against non-compliant overseas-based service providers; and
  - Whether the Commissioner should be able to pose business disruption sanctions in a similar way to the UK where in "the most extreme cases, with the agreement of the courts, Ofcom will be able to require payment providers, advertisers, and internet service providers to stop working with a [s]ervice, preventing it from generating money and being accessed from the UK".

International approaches to address online harms

- The Issues Paper notes that international approaches are evolving with an increasing focus on systemic change as opposed to interventions based only on responding to "episode-based interventions". The Issues Paper considers a range of international developments and approaches.
- Key international regulatory developments of particular focus in the Issues Paper include:
  - The introduction of a statutory duty of care placed on the service provider;
  - Regulation that particularly focuses on the best interests of children;
  - Strengthening of safety by design requirements;
  - Strengthening enforcement powers;
  - Increasing transparency and data access (for both regulators and others such as academic researchers);
  - Better supporting users in particular through clear and transparent dispute resolution processes (e.g., an ombudsman scheme); and
  - Balancing and safeguarding fundamental human rights.
- The Issues Paper seeks input on whether Australia should incorporate any of the referenced international approaches.

Regulating the online environment, technology and environmental changes

- The Issues Paper notes that regulatory frameworks are rapidly evolving to adapt to the scale and speed of harms arising online.
- The Issues Paper identifies several online harms which "may not be fully addressed under the Act", noting that the Review "provides an opportunity to consider whether there are new or emerging harms that should be specifically addressed" in the Act.
- Additional harms subject to specific consideration in the Issues Paper include:
  - Cyber-flashing;
  - Online hate;
  - Volumetric ("pile-on") attacks, where a targeted individual is tagged or linked to a harmful post and other users continue to rapidly share and comment on such a post;
  - "Technology-facilitated abuse" namely "using technology to enable, assist or amplify abuse or coercive control of a person or group of people", Including "technology-facilitated gender-based violence";
  - Online abuse of public figures;
  - Promotion of self-harm and body image harm; and
  - Other potential online harms and emerging technologies including the amplification of online harms by the increasing use and sophistication of generative artificial intelligence, harms associated with immersive technologies, recommender systems and algorithms harms associated with end-to-end encryption in communications services, and increases in decentralized platforms.

- Finally, the Issues Paper poses questions surrounding the regulatory governance model. The questions posed are again extremely broad, but key questions include:
    - Whether online service providers should be required to contribute to the costs of regulation (i.e., a cost recovery model);
    - Whether harms against groups, in addition to individuals, should be covered; and
    - How innovation, privacy, security and safety should be balanced.

Misogyny and other related online harms

In addition to the Issues Paper, the Government has also recently pledged to take steps to combat online harms relating to extremist misogyny and the distribution of "deepfake pornography", referencing the existing work of eSafety including on Industry Codes and Standards.

The key commitments from this announcement include:

- Introducing legislation to ban non-consensual distribution of deepfake pornography;
- Clarifying that the creation and sharing of sexually explicit material without consent (including through use of artificial intelligence) will be subject to serious criminal penalties; and
- Providing resources to conduct a pilot of age assurance technology to protect children from accessing harmful content including pornography and other age-restricted online services.

A pilot of age assurance technology was previously mooted in 2023, following the publication of eSafety's Roadmap for Age Verification. At the time, the Government stated its intention to wait until after the development of Phase 2 Industry Codes (covering a range of content that is inappropriate for children) under the Online Content Scheme is completed to further investigate a potential pilot, on the basis that the market for age assurance was at that stage too immature. However, this has now been fast tracked.

As part of the current classification reform process, the Government is also considering options to reduce access and exposure to violent pornography. The Government announced it will also bring forward legislation to prohibit the release of private information online with an intent to cause harm ("doxxing") and reform the *Privacy Act 1988* (Cth) to provide women experiencing domestic and family violence with greater control and transparency over their personal information.

Next steps

Providers should consider making submissions on the Issues Paper. Public consultation on the Issues Paper will close on 21 June 2024. Further detail regarding the other proposals is anticipated in the coming months.

With thanks to Nina Kerwin Roman (Junior Associate) for her assistance with this alert.

Contact Us

Adrian Lawrence
Partner, Sydney
adrian.lawrence
@bakermckenzie.com

Andrew Stewart
Partner, Sydney
andrew.stewart
@bakermckenzie.com

Allison Manvell
Special Counsel, Brisbane
allison.manvell
@bakermckenzie.com