

Digital duty of care

Another layer in an expanding regulatory framework

Australia – July 2026

Earlier this year, the Australian government released an [issues paper](#) on a proposed digital duty of care (the Duty) framework under the *Online Safety Act 2021 (Cth)* (the Act) (the Issues Paper). While there is still a long way to go, if enacted, the reforms will complement, among other things, the social media minimum age law which took effect on 10 December 2025.

The Duty has been a topic of ongoing discussion in Australia and covers similar ground to other countries, including the obligation for “Very Large Online Platforms” (VLOPs) in the EU to identify, analyse and assess systemic risks that are linked to their services¹. Individual members of Parliament have also emphasised their desire for such obligations to be enacted, with Independent Zoe Daniel introducing a bill at the end of 2024, which has now lapsed.

Ultimately, the government’s main incentive is to action a key recommendation made in its [statutory review](#) of the Act, published in early 2025. That review suggested the introduction of an overarching duty of care, which would require all online services to take reasonable steps to prevent foreseeable harm. Prime Minister Anthony Albanese has given pride of place to the Duty in his recent speech on the future of AI regulation in Australia, naming the design of the Duty as part of the government’s “ongoing work” on AI.²

What does the Duty require?

As proposed by the government, the Duty will require all entities regulated by the Act to maintain effective systems and processes to:

- So far as is reasonably practicable, provide a safe online environment for all Australians
- Prevent, monitor and appropriately address illegal and harmful content
- Ensure the safety of service features such as AI systems, algorithmic content recommendation systems and bot accounts

Some observations:

- Illegal content will include content that is illegal under the Act or other Commonwealth law but may also extend to content that is a “seriously harmful threat” to public safety, noting that this would need to be balanced against an individual’s right to freedom of express and speech. Some of this content is already regulated under the [Phase 1 Codes and Standards](#), which sit under the Act and came into effect in 2024.
- Harmful content is typically harder to assess but will involve content or activity that is harmful to young people, including content which promotes eating disorders or seriously harmful activity. Some of this content is already regulated under the [Phase 2 Codes](#), which came into effect earlier this year.

A failure to take reasonable steps to maintain the systems and processes mentioned above would constitute a breach of the Duty. Importantly, the Issues Paper clarifies that entities will not be liable for individual instances of harmful content or activity, but rather a wider failure to appropriately address harmful content or activity. This is consistent with the approach taken to the social media minimum age law, which requires the eSafety commissioner to “[assess] the totality of the steps taken by a platform to comply...this is about systems and processes, not individual accounts”.³

Who would be subject to the Duty?

The Duty will apply to online services already within the scope of the Online Safety Act, including social media, messaging apps, online games, dating services, general websites/apps, pornography services, generative AI services, hosting services, internet service providers (ISPs), search engines, app stores and equipment/operating system services.

As with the consolidated codes of practice that were enacted under the Act, the Issues Paper acknowledges that compliance measures should be proportionate to the level of risk attached to an online activity or service, as well as a service’s opportunity to address risks “in the chain of service provision” to users.

¹ Article 34, EU Digital Services Act

² Anthony Albanese, “AI in Australia’s interests” on 15 July 2026.

³ [Social Media Minimum Age: Compliance update](#).



What could “effective systems and processes” mean?

In the Issues Paper, the government provides the following, non-exhaustive examples of what might be meant by this term:

- Moderation/classification tools
- Law enforcement engagement processes
- Internal dispute resolution
- Terms of use/community standards
- User safety controls
- Privacy/recommendation settings
- Parental controls and family safety settings

Some observations:

- For mature technology platforms, many of these measures will already be in place. However, even though the Australian government has flagged that the duty will apply proportionately to a service’s risk profile, it seems unlikely that even a nascent, lower-risk online service could satisfy the Duty without having any of the above in place.
- References to appropriate “privacy/recommendation settings” suggest, at first glance, that the Australian government is approaching the issue more flexibly than other lawmakers. For example, the EU Digital Services Act requires VLOPs to provide users with at least one recommender system option “not based on profiling” of individuals by automated systems⁴. Requiring adjustable settings would not go so far.

How does this interact with an already complex regulatory regime?

If enacted, the Duty would complement rather than replace existing regimes under the Act. For example, the Act penalises, and allows the eSafety commissioner to investigate, cyberbullying, adult cyber abuse, image-based abuse and illegal/restricted material. As mentioned, the codes enacted under the Act also govern illegal and harmful content.

To use the Relevant Electronic Services (Phase 2) Code as an example; under that code, a gaming service provider must:

- Implement appropriate age assurance and access control measures to prevent under 18s from playing 18+ computer games

- Have terms and conditions in place that prohibit the sharing of illegal material
- Moderate content to ensure compliance with those terms and conditions

Many of these obligations overlap with the sample “effective systems and processes” stated above. In addition to the duties set out in the Basic Online Safety Expectations and, of course, the social media minimum age rules, it will be important for online service providers to understand the delta between their existing obligations and the new Duty – if indeed such a delta exists, as many services will find that the steps that they have taken may already help to establish compliance. It is critical that, if and when the Duty comes into effect, legislators are clear that it does not impose wholly new obligations, but may instead cover many of the steps naturally taken by services to protect their users.

What does this mean for online regulation more generally?

The Act regularly interacts and overlaps with other laws, including the Privacy Act and the Australian Consumer Law.

In respect of the overlap with the Privacy Act in particular, two observations:

- The government offers AI tools that identify and prevent the generation and sharing of content by users of illegal or seriously harmful material, such as unwanted “nudification”, as a possible feature to reduce harm. Any use of AI in a way which significantly affects an individual’s rights or interests, including when there is justification to do so, still requires certain kinds of disclosures in a service’s privacy policy under amended Australian Privacy Principle (APP). It is conceivable that, for some online services and some moderation decisions, any decision to remove content or shadowban or, at worst, ban an account would fall within the APP 1 threshold. Any mandatory disclosures must strike the difficult balance between enough information to be meaningful, but not so much as to allow circumvention of protective measures.
- Another potentially dangerous feature put forward is systems that allow anonymous or pseudonymous accounts. For the government, these accounts could be misused to “...support or propagate seriously harmful inauthentic activity or to menace, threaten and harass other users”. However, APP 2 preserves the right for individuals to interact anonymously or pseudonymously with an entity, where that is reasonably practicable. With the advent of age assurance, this APP is already under threat, but it remains an important hallmark of Australian privacy law and online life when not used to shield unlawful or harmful behaviour.

What might be the penalties for breach of the Duty?

According to the Issues Paper, a key obligation attached to the Duty is recurring risk management. Services would need to assess risks of serious harm at least annually, reassess when significant changes are made to the service, implement appropriate mitigation measures and regularly evaluate whether those measures are effective, making changes where necessary. Unlike many other online safety laws (including the codes), services are given the discretion both to identify and rectify any failure to comply with the Duty.

Services will likely have in place periodic or targeted reporting obligations, and cannot withhold information from eSafety merely because it is commercial-in-confidence. eSafety may also require independent audits where there is a reasonable basis to believe systemic noncompliance exists.

The Issues Paper indicates serious civil penalties for egregious and systemic breaches, but the penalty figure will only be confirmed if and when the bill is released. Importantly, the government has proposed a 12-month transition period between the legislation passing and commencement of the Duty, with guidance to be developed during this period. At a minimum, we would hope that any such guidance covers the points that we have raised above.

What other reforms are on the table?

The Issues Paper also mentions other recommended amendments to the Act and indicates whether they are supported by the government, including if only supported in principle.

A few to note are:

- Requiring the best interests of the child to be a primary consideration for online service providers in assessing and mitigating risks arising from the design and operation of their services. Note: This has in part been reflected in the Office of the Australian Information Commissioner's (OAIC's) Children's Online Privacy Code (currently under consultation).
- Reducing the waiting period before eSafety can issue certain removal notices from 48 hours to 24 hours
- Allowing the regulator to waive the delay in certain circumstances
- Allowing removal notices for reposted material
- Requiring simple and accessible complaint mechanisms
- Exploring how to prohibit search engines and app stores from surfacing or distributing "nudify" apps and undetectable stalking apps
- Requiring major platforms to have a contact point for service in Australia
- Requiring services to maintain records of steps taken to comply with the Act

Contact



Tanvi Mehta Krensel
Partner, Sydney
T +61 4 5065 7742
tanvi.mehtakrensel@squirepb.com