

What can you expect from the proposed digital duty of care?

The government adds another string to its regulatory bow

Australia – September 2026

The Australian government has introduced a draft digital duty of care (the Duty) bill for consultation.¹ Initially proposed by the government in 2024, the return to this mode of regulation signals what the government itself referred to as a “shift away from reacting to harms by relying on content regulation alone, and moving towards systems-based prevention”.

However, after recent legislative efforts, such as the industry codes and Basic Online Safety Expectations (both now repealed), have codified obligations (rather than overarching duty-based regulation), the maze of online legislation continues, with a real risk of historically different laws creating confusion.

The future of the Duty is not assured, with the Coalition expressing significant objections. However, with the Greens on side, our prediction is that some form of it will make its way into Australian law. Meanwhile, the public’s time to provide feedback on the draft Bill will soon be up. The deadline of Noon 22 September – and the government’s emphasis that they are looking for only “targeted consultation”² – is consistent with recent, equally short time frames for other digital laws.

In this article, we answer some of your most pressing questions about the Duty and identify the provisions that we believe would benefit from greater clarity.

Who does the Duty apply to?

Much of the discourse around the Duty has focused on social media services – the prime minister himself introduced the bill by calling it “the next step following [the government’s] world leading social media age ban”³, and by referring specifically to social media algorithms. However, the impact of the Duty goes beyond social: the Duty covers internet search engines, app distribution services, hosting and internet services, relevant electronic services (including games and apps), equipment providers and services that allow the generation and sharing of gen AI material: see Section 25A.

Unlike other online safety legislation⁴, there is no express statement that a service’s obligations under the Duty will vary depending on the level of risk posed by that service, and where it sits in the online ecosystem (for example, whether the service provider directly engages with individuals). Given its breadth, this will need to be clarified in supporting materials.

What does the Duty require?

The Duty requires a person responsible for an online service to ensure, so far as is reasonably practicable, a safe online environment. This means:

- (a) Managing design features of the service appropriately, including through providing user empowerment tools (further discussed in “Does the duty really require opt-in to algorithms?”)
- (b) Conducting risk assessments (further discussed in “Are there related governance obligations?”)
- (c) Taking effective measures necessary to address those risk assessments.⁵

1 “Online Safety Amendment (Digital Duty of Care) Bill 2026—Exposure Draft”, Australian Government, 8 December 2026 (the Consultation).

2 See the Consultation.

3 “My Feed, My Way”, Anthony Albanese, 8 September 2026.

4 For example, the Head Terms to the Industry Codes of Practice for the Online Industry, which state the following:

Electronic products and services provided across different sections of the online industry may include different functionalities, which in turn may be relevant to:

- The connection between a product or service and risks associated with access or exposure to class 1C and class 2 material
- The relationship between a product or service and an end-user, including whether or not a service controls the end-user interface
- The visibility, control or administration of specific material accessible to an end-user

5 Section 26(3) of the Bill.

What is a safe online environment?

At a high level, providing a safe online environment will include protecting:

- All Australians from serious harmful material and conduct (e.g. child abuse, sexual violence, extreme violence or cruelty and promotion of illicit drug use).
- Australian children from both material and conduct that is harmful to children (e.g. pornography, encouragement of disordered eating or hostile attitudes towards women) and harms associated with the operation of design features. Where the online service is a social media service, then any design features which have “negative behavioural impact” must not operate for under 16s. Other online services may need to take a more nuanced approach to design.

And what is “reasonably practicable”?

The bill sets out what is meant by “reasonably practicable” in Section 25H. The standard expressly requires an organisation to take into account and weigh up relevant matters, including (on a non-exhaustive basis) the matters set out in Subsections 25(a) to (e), such as the likelihood of the harm concerned occurring, the degree of harm that might result and the availability and suitability of ways to eliminate or mitigate the risk.

This framing borrows heavily from work health and safety duties, which require a person conducting a business or undertaking to ensure, so far as reasonably practicable, the health and safety of workers while they are at work⁶, and which list factors for determining what is “reasonably practicable”⁷ that are almost identical to those set out in the bill. The intention appears to be to keep this concept as broad as possible, allowing different online services to craft their own approach towards ensuring a safe online environment.

Although they address different subject matter, we expect that recent enforcement on work health and safety duties – and, specifically, the “weighing up” that was undertaken – will prove informative.

Are the concepts of “harm” or “negative design features” static?

No, “harm” and “serious harm” can change over time. Much has been made of the minister’s new ability under Sections 25C and 25D of the Bill to prescribe new forms of “harm” and “serious harm” under legislative rules, with the opposition alleging that the “government is now actively seeking to censor and has been active in censoring, attempting to censor any view they don’t like”. Equally, under Section 25G, the minister may determine that a specific design feature shall be deemed as having negative behavioural impacts, in addition to those which are already listed.

While we understand that technologies can evolve, in preparing for the Duty, online services need to exhaustively and clearly understand what is meant by harm and which design features are in-scope. The fact that there is no effective limitation on the minister’s powers listed above frustrates this objective, which is all the more critical given the application of the Duty.

We have also identified that many forms of harm (or serious harm) are broadly defined. While the intention behind this is clear, the penalties under the Act are prohibitive, reaching to over AU\$100 million. There is a real risk that, where the characterisation of content posted is complex or unclear (for example, in the context of illicit drug use, where such content can serve to help those who are addicted), online services will err on the side of caution and act swiftly to contain.

Does the Duty really require opt-in to algorithms?

No, but watch this space. The Duty has automatically deemed certain hallmark features of online life as being unlawful. One of the most significant is recommender systems or algorithms, which is identified in Section 25G as having “negative behavioural impacts”.

The Bill explicitly requires that an online service provide “user empowerment tools” as part of satisfying the Duty, and that such a tool should allow a user to manage the way design features of the service operate for the user (such as through providing control over the kind of content that is recommended). However, in case this is not enough, the bill expressly reserves the right for the minister to require “specified” online services to provide “specified” user empowerment tools: see Section 26(4). It is not difficult to guess what these services and tools might be.

We have identified three issues with this approach:

1. The intention of the Duty is that it is principles-based, with online services able to determine what steps are reasonably practicable for that provider. As flagged in “Are the concepts of ‘harm’ or ‘negative design features’ static?” above, rules which propose a highly prescriptive approach to compliance for certain services detract from that objective.
2. A recommender system is not necessarily negative. As others like the Digital Industry Group, Inc. have persuasively noted, an algorithm is not just “one thing...they make digital services more relevant and useful for Australians’ different interests and needs”.⁸
3. Offering total opt-outs as a form of “user empowerment” becomes difficult for platforms that depend on certain personal information to deliver a meaningful service. For example, online retailers may struggle to provide a non-personalised feed, when understanding the location of their users helps determine which products and services are available.

⁶ See for example Section 19 of the *Work Health and Safety Act 2011* (NSW) (WHS Act).

⁷ Section 19 of the WHS Act.

⁸ “Digital duty of care to let Aussies opt out of social media algorithms”, Information Age, 8 September 2026.

While the other design features stated in both Section 25F and 25G are unlikely to generate the same level of attention (for example, feedback features, through which services display information to end-users about who has engaged with their material), some of these are unlikely to be relevant to many services captured by the Duty, making it unclear as to how the Duty is intended to operate beyond social media and gaming platforms (who seem increasingly to be the specific targets of a broad-brush approach).

Isn't online safety already regulated?

Yes, and some existing laws will be repealed. In particular, the bill proposes to repeal both the Basic Online Safety Expectations (BOSE) and the commissioner's ability to enact industry codes and standards, which will in practice also mean the phasing out of industry codes as and when the Duty takes hold.

If enacted, the Duty would require that online services comply with what is now a very broad obligation to put in place open-ended systems and processes to ensure a safe online environment. The trouble with this approach is that for a long time now, service providers have been subject to highly specific obligations. To use the Relevant Electronic Services Online Safety Code (Class 1C and Class 2 Material) (RES 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 games⁹
- Have terms and conditions in place that prohibit the sharing of illegal material
- Moderate content to ensure compliance with those terms and conditions¹⁰

The BOSE are even more prescriptive. For example, they expressly require a service which uses "recommender systems" (i.e. an automated system which shows users posts, ads and accounts to follow, typically based on what a user is most likely to engage with) to take reasonable steps to consider end-user safety and incorporate safety measures in the design, implementation and maintenance of recommender systems.¹¹ This is quite different from the blunter approach foreshadowed by the Duty: "see Does the Duty really require opt-in to algorithms?" above.

There are real questions about whether repealing highly prescriptive legislative instruments is appropriate. The BOSE have been in place for four years, meaning that the industry would have already taken significant steps towards ensuring compliance with them. Conversely, the latest of the codes have only been in place since March 2026, meaning that there has been no time to truly test their impact on the online ecosystem. If enacted, there is no guarantee that steps taken to comply with these laws would still satisfy the Duty – industry may find themselves establishing an entirely new set of compliance standards.

Equally, age-restricted social media services have taken steps to remove under 16 accounts from their platforms, in accordance with Part 4A of the *Online Safety Act 2021* (Cth). While this remains law, the Duty includes as part of its assessment of whether there is a "safe online environment" and whether negative design features have been "switched off" for under 16s. This shifts focus and distracts from the main obligation introduced by law not yet two years ago.

What will this mean for upcoming laws and for age assurance?

As any digital enthusiast will know, laws in this space have been rapidly shifting. Over the next few months, we can expect to see several amendments to existing laws (including the *Privacy Act 1988* (Cth)), as well as a brand-new Children's Online Privacy Code (COPC), coming into effect in December.

While still in draft form, the COPC covers similar ground to the Duty, and proposes equivalent protections (including a requirement to handle personal information consistently with 'the best interests of [a] child' and a qualified right to erasure, which applies to large digital platforms). Imposing an entirely new obligation on online service providers, before the impact of these changes is understood, seems premature. Equally, any contradictions between these two laws need to be addressed. For example, the COPC requires that an entity only collect personal information about a child that is strictly necessary to provide an online service – it will need to be clear that "strictly necessary" includes implementing steps which satisfy the Duty.

As to age assurance, unlike the COPC, the Duty does not expressly require that services take steps to ascertain the age of their users. In practice, though, this will be required for online services who are required under the Duty to protect children from harmful materials, conduct and design features (if they elect not to remove any such risks altogether). While the Duty creates an exception in Section 26(7) for lawful private communications between adults, online services will still have to put in place measures to assess whether the senders and recipients of such communications are in fact over 18.

⁹ Section 7.1, RES Code.

¹⁰ Section 8.1, RES Code.

¹¹ Section 8B, BOSE.



Are there related governance obligations?

As expected, yes. Most relevantly, a provider of an online service must conduct a written assessment of the risk of harm posed by that service: Section 26A. This needs to be retained for six years and must be produced to the eSafety Commissioner on demand. A service provider must also prepare transparency reports about the safety of the online service, on request by the eSafety Commissioner: Section 192C.

A few comments:

- The scope of the assessment under Section 26A exceeds what is required by the Duty, with Section 26A(2) specifying that “all reasonably foreseeable risks” includes, but is not limited, to those relevant to the Duty. This potentially puts no limit on the “risks”, which should be included, although it is obviously limited by context.
- As flagged in “What will this mean for upcoming laws?”, digital regulation is a crowded space. An assessment is clearly necessary to determine the scope of the Duty but may in practice need to be combined with an organisation’s other related obligations, including to conduct a privacy impact assessment under the COPC.
- Transparency reports can only be issued if certain criteria are met (including if the Commissioner considers them necessary to promote best practice) but can, at least potentially, be required on a periodic, ongoing basis.

What are the penalties for non-compliance?

As mentioned above, penalties for breach of the Duty can extend past AU\$100 million for online services. Importantly, the bill clarifies that the Duty applies to a person responsible for an online service, indicating that individuals who either provide the service or exercise day-to-day control over it may have personal liability for breach – including, potentially, criminal liability for failing to comply with issues noticed by the Commissioner or requests for cooperation.

Author



Tanvi Mehta Krensel

Partner, Sydney

T +61 450 657 742

tanvi.mehtakrensel@squirepb.com