

Australia: Digital Duty of Care to Redefine Online Safety

Abstract: The Government has released draft legislation that would overhaul Australia's online safety framework, transforming online service regulation.

In brief

On 8 September 2026, the Australian Government released an exposure draft of the **Online Safety Amendment (Digital Duty of Care) Bill 2026**. If passed, the legislation would significantly amend the Online Safety Act 2021 (OSA) and fundamentally reshape the regulatory landscape for online services in Australia.

The headline change is a new 'digital duty of care', which will replace both the Basic Online Safety Expectations (BOSE) and the existing Industry Codes and Standards. The duty would be accompanied by a range of transparency-related obligations, alongside a suite of reforms that would expand the powers of the eSafety Commissioner ("**eSafety**") and significantly increase penalties for non-compliance.

Consultation is currently open, with feedback accepted until **12pm on Tuesday, 22 September 2026**.

Contents

Key takeaways

In more detail

The Digital Duty of Care
New obligations to support the core duty
Repeal of BOSE and Codes & Standards
Other changes to the OSA
Enforcement powers and penalties
What still remains unclear?
What's next?

Key takeaways

- The draft bill proposes to amend the OSA to introduce a **digital duty of care**, requiring any person responsible for an online service to ensure, so far as reasonably practicable, a "safe online environment" in which Australians are protected from seriously harmful material and conduct, with additional protections for children (including from harms associated with certain service design features).
- The existing BOSE framework and Industry Codes and Standards would be **repealed** from the date on which the new duty takes effect.
- As part of meeting the duty, providers would need to conduct **mandatory risk assessments** at least annually (as well as before any material changes), take effective measures to address those risk assessments, and manage design features appropriately (including by implementing any prescribed user empowerment tools, which could include tools to opt-out of receiving personalised content recommended by an algorithm).
- The draft bill allows eSafety to publish guidelines to assist persons responsible for online services to meet their digital duty of care. However, compliance with the eSafety guidelines will **not provide safe harbour** protection (meaning in practice online services could not rely on adherence to the guidelines alone to satisfy compliance with their digital duty of care obligations).
- The duty would be accompanied by supporting obligations related to complaint and dispute processes, transparency reporting (replacing the BOSE reporting framework), information publication requirements, and data access schemes for online safety-related research.
- If passed, the proposed legislation would also expand eSafety's enforcement toolkit, including a range of new compliance, investigative, and transparency powers. Maximum civil penalties would double (with the highest penalties reaching over **AUD 109 million** – aligned with the recently increased penalties for the social media minimum age (SMMA) obligation, and the reforms would also see a tenfold increase to the maximum amount payable under an infringement notice (up to AUD 218,400 per infringement).
- At present, questions remain about the operation of the proposed digital duty of care and the accompanying changes. The draft legislation has not yet been accompanied by an explanatory statement, and there are many obligations that will turn on Ministerial rules or determinations, legislative instruments, or guidance to be released by eSafety. In particular, the extent to

which providers will be able (or expected) to leverage and build on work undertaken to comply with the current regulatory framework is unclear.

- The core reforms in the draft bill (including the introduction the digital duty of care and repeal of the BOSE and Industry Codes and Standards) are proposed to take effect after a **12-month transition period**. Some changes (the expansions to the powers to issue removal notices and link deletion notices) would take effect immediately upon royal assent.

In more detail

The proposed changes fall in three main categories:

1. Core digital duty of care.
2. New obligations that support the core duty, covering topics such as complaints and disputes processes, transparency reporting, and the publication of information about online safety.
3. Other reforms to the OSA, which repeal the BOSE and Industry Codes and Standards, expand eSafety's powers, and increase penalties for non-compliance.

We walk through each of these below, before considering what is still unclear, as well as what to expect next.

The digital duty of care

The proposed digital duty of care would require that:

'A **person responsible** for an **online service** must ensure, so far as is **reasonably practicable**, a **safe online environment**.'

Key questions include:

- Who must comply?
- What is meant by a 'safe online environment', and the standard of 'so far as reasonably practicable'?
- What does compliance require?

A key caveat to the proposed digital duty of care is that it does not require action to be taken in relation to **lawful communications occurring in private between consenting adults**. While unclear whether this is intended to apply only on a one-to-one or also on a one-to-several basis, this will be clearly be a relevant consideration for any services with messaging functionality.

Who must comply with the duty?

- The duty applies to a **person responsible for an online service**, which includes not only the person who **provides** the service, but also a person who is in a position to **exercise day-to-day control** of the service.
- This represents an expansion from the existing OSA framework, which places obligations only on providers. However, interestingly, whilst the duty itself has broader application, some (but not all) of the new obligations outlined below in support of the duty are expressed as applying only to providers.
- The bill also introduces a definition of **online service**, a term not currently used in the OSA. The definition is a very broad list, comprised of each of the eight industry sections currently regulated by the Industry Codes and Standards (with a slight reframing of the existing equipment provider category),¹ and adding one new category, being a service that allows users to generate material using artificial intelligence and share that material through another online service.

¹ These eight categories are: (i) an internet carriage service, (ii) a social media service, (iii) a relevant electronic service (RES), (iv) a designated internet service (DIS), (v) a hosting service, (vi) an internet search engine service, (vii) an app distribution service, and (viii) a service that manufactures, supplies, maintains or installs equipment for use in Australia in connection with categories (i) to (iv) – this would replace the current equipment provider category.

- Importantly, the Minister for Communications (“**Minister**”) would be able to **exempt** an online service, or class of services, that would otherwise owe the digital duty of care where the Minister is satisfied that the service has minimal usage in Australia or poses little risk to Australian users.
- The Minister would also have the power to determine whether an online service is, or is not, a social media service – noting that some of the new obligations are specific to this service category.

A ‘safe online environment’ and the ‘reasonably practicable’ standard

The digital duty of care requires online services to ensure that a safe online environment, which involves meeting the following conditions:

Condition	Detail
Persons in Australia are protected from seriously harmful material and conduct .	Seriously harmful material and conduct: This is an exhaustive list covering categories such as child sexual exploitation and abuse material, and material or conduct relating to grooming, sexual violence, extreme violence or cruelty, explicit threats of physical violence, harassment, self-harm, animal cruelty, terrorism, the commission of a crime, and illicit drug use. However, there is scope for the Minister to expand the list to capture additional categories of material or conduct that may cause serious harm. The categories have been decoupled from the National Classification Scheme. In other words, they apply on their own terms regardless of how the material has been or would be classified under those rules. The references to “conduct” (in addition to “material”) also represents an important expansion of the scope of the regulatory scheme.
Children in Australia are protected from material and conduct that is harmful to children and harms associated with platform design features .	Material and conduct harmful to children: This is a broader and less exhaustively-defined category, including pornography and material or conduct relating to eating disorders, hostile attitudes towards women or gender equality, any forms of abuse or bullying and any other material or conduct that could inflict serious harm to a child. This separate, broader threshold for material or conduct harmful to children reflects the ongoing regulatory focus on child safety and ensuring age-appropriate service delivery. Again, this has been decoupled from the National Classification Scheme. As with seriously harmful material or conduct, the Minister would be able to extend this list by legislative instrument. Harms associated with design features: The draft bill clarifies that ‘harm’ can be caused by material or conduct, whether or not a user of an online service engages in, or experiences that material or conduct. The draft legislation expressly includes five features in the definition of a design feature: • Recommender features, where a service can display material to a user by reference to information the service has associated with the user’s account; • Endless-feed features, where a service can display material in a feed that effectively has no end point; • Feedback features, where the service can provide information to a user about the extent to which other users have engaged with material they have posted; • Time-limited features, where a service only enables a user to view material on the service for a limited period after it has been posted; and • Logged-in features, where an endless-feed feature, feedback feature, or time-limited feature is unable to be accessed by an end user without an account. However, the definition of design feature is non-exhaustive and can extend to other features.

In the case of social media services, design features that have **negative behavioural impacts** do not operate for children in Australia who are **not yet 16 years of age**.

Design features with negative behavioural impacts: The five design features mentioned above, and any other feature determined by the Minister, are deemed to have negative behavioural impacts.

This condition is focused on the operation of social media services for children in Australia under 16. That might seem somewhat curious given the existing ban on under 16s holding accounts with age-restricted social media platforms will remain, but the key practical effect of this requirement may be that social media services would not be able to make the relevant design features accessible to users that are not logged in to an account (noting that U16s are still permitted to access age-restricted social media platforms without an account). It might also expose providers to additional enforcement where U16s are gaining access to the service in circumvention of age assurance measures.

The duty to ensure a safe online environment would be subject to a **reasonably practicable** qualification, meaning 'what is reasonably able to be done'. This would involve weighing up all relevant matters, including:

- The likelihood of the relevant harm occurring and the degree of harm that might result;
- What is known or ought reasonably to have been known about the harm and its associated risks;
- The availability and suitability of ways to minimise the risk; and
- The costs and impact on privacy associated with eliminating or minimising the risk, including whether such costs or privacy impact are **grossly disproportionate** to the risk concerned (a notably high bar).

What's required to comply with the duty?

The draft bill sets out the following mandatory requirements that a person must also comply with to meet their digital duty of care:

1. Manage **design features appropriately**, including by providing any required **user empowerment tools** (being tools that allow users to manage the way design features of a service operate for them, for example by controlling the content recommended):
 - a. The draft bill does not itself impose requirements for services to provide specified tools, but rather sets up a framework for the Minister to make legislative rules to that effect.
 - b. Commentary since the release of the draft bill has suggested that the most significant of these tools will be the ability for users to opt-out of receiving personalised content recommended by an algorithm. The Government has announced an initiative called "My Feed, My Way", which will require social media services to send a notification to new and existing users offering them a choice over their default feed.
2. Conduct **risk assessments**:
 - a. The provider of an online service would need to conduct a written risk assessment of the 'risk of harm' posed by the service in Australia – a broad obligation that seems to go beyond the harms described as subject to the digital duty of care. The provider would need to identify all foreseeable risks (including those relevant to their digital duty of care), as well as the content, systems, processes, and design features that give rise to those risks and the people who may be affected. The likelihood and severity of identified risks would also need assessment, alongside mitigating measures and their expected effectiveness.
 - b. Risk assessments would need to occur at least annually and before any changes that might introduce new risks, with a copy to be provided to eSafety within 30 days upon request. The assessments would also need to meet any additional requirements determined by eSafety and be retained for six years.
 - c. Practically, the proposed risk assessment obligations expand significantly on the current risk assessment requirements under the mandatory Codes and Standards – moving more in the direction of the broad risk assessment regime under the EU's Digital Services Act or the UK's Online Safety Act. Given the extremely broad scope of online services subject to the Australian OSA, this effectively imposes a risk assessment requirement on **all** websites and apps available in Australia, regardless of scale and content (as well as on manufacturers and suppliers of devices) (unless exceptions are granted for lower risk services by the Minister).
3. Take **effective measures** as necessary to address the risk assessments conducted.

Guidance

- The draft bill allows eSafety to publish guidelines to assist persons responsible for online services to meet their duty. This is a departure from the anticipated Ministerial rules that were expected to provide more specificity on compliance for providers. The consultation paper released on the digital duty of care in May this year anticipated that the duty would be “underpinned by Government made rules subject to Parliamentary scrutiny”, including “binding rules specifying compliance requirements for service providers or specified classes of services” with the duty.
- While the draft bill retains certain matters to be considered and implemented by the Minister, and requires eSafety to undertake certain tasks by way of legislative instrument, these are limited.
- The eSafety guidelines would not be subject to Parliamentary oversight and would not provide any safe harbour protection, meaning that in practice online services would not be able to rely on adherence to eSafety guidance alone to satisfy compliance with their digital duty of care obligations.

Consequences for non-compliance

- Non-compliance with the digital duty of care could attract a civil penalty of up to 300,000 penalty units for body corporates, amounting to **AUD 109.2 million** (at the time of publishing this alert), effectively a doubling of the current highest maximum penalty under the OSA.
- If eSafety reasonably believes that a person had failed, or was failing, to comply with their digital duty of care, eSafety would also be able to issue a formal warning or **a written remedial direction requiring a person to take specified action**. If an entity failed to take the remedial actions directed, they would also be liable for the AUD 100 million+ civil penalty. eSafety would also have powers to issue infringement notices for both a primary breach of the duty and a failure to comply with a remedial direction.

New obligations to support the core duty

The draft bill introduces a suite of new complaints, transparency, and publication obligations for online service providers, designed to support the digital duty of care. A recurring theme across these measures is that they will only take effect once eSafety makes a determination or issues a written notice with respect to a particular service or category of online service, they will not automatically apply to all online services without eSafety taking such steps. However, the draft bill grants eSafety considerable power and discretion to determine how and when these requirements will apply.

Complaint and dispute processes

A person responsible for a **prescribed online service** would be required to have **complaint and dispute processes** that are available equally to all Australians, and to comply with any requirements determined by eSafety in relation to those processes.

- eSafety is given power to determine which classes of online services will be prescribed for the purposes of this requirement. eSafety may also determine the specific requirements that must be met by those complaint and dispute processes.
- It is unclear how these new requirements will expand or alter the existing reporting and complaints obligations under the current Codes and Standards.
- Non-compliance would attract a civil penalty of 30,000 penalty units for body corporates (AUD 10.9 million at the time this alert is published), with eSafety also able to issue formal warnings, remedial directions, or infringement notices.

Transparency reports

eSafety would, by written notice, be able to require the provider of an online service to prepare and **give eSafety a transparency report** about the safety of the online service for Australians.

eSafety would also have the power to **publish a full transparency report**, or a summary of a transparency report, on eSafety's website.

- This new transparency reporting regime is set to replace the existing BOSE reporting framework. The scope of the proposed regime is **extremely broad**, removing any previous uncertainty over the scope of eSafety's powers to request reports under the BOSE.

- eSafety may ask any questions, or require reporting on matters, so long as it relates to “the safety of the online service for Australians” which could include (without limitation):
 - The extent to which the provider is complying with the OSA (including the digital duty of care and SMMA obligations, as applicable); and
 - Other matters such as the effectiveness of compliance measures, available resources, the nature and extent of harms associated with the service (including emerging harms), features or systems that contribute to safety or increase risk, and performance against specified standards, benchmarks or other metrics.
- As with BOSE reports, eSafety would have the power to specify the manner and form in which transparency reports must be prepared, the reporting intervals (between six and 24 months), and the period within which the report must be given (no shorter than 28 days).
- Non-compliance with a transparency notice would attract a civil penalty of 30,000 penalty units for body corporates (AUD 10.9 million at the time this alert is published), with eSafety also able to issue formal warnings.
- Of particular note are eSafety’s powers around publication of transparency reports, particularly the power to **publish a report in full** (expanding on eSafety’s existing power in the OSA to disclose summaries of de-identified information). The transparency report publication powers are subject only to relatively narrow exceptions that prevent publication of information:
 - In circumstances that could reasonably be expected to found an action for **breach of a duty of confidence** (a generally high bar);
 - Is **personal information** (within the meaning of the Privacy Act 1988); or
 - Is information of a kind prescribed in the legislative rules.

Requirements for providers to publish certain information

eSafety would be empowered to, by legislative instrument, determine that online service providers in a specific class **must publish specified information on their website** about the provider’s operations or activities relating to the online safety of its users in Australia.

- Again, eSafety is given power to determine which classes of online services will be required to comply with this requirement. eSafety may also determine the specific information requirements that must be met.
- This requirement could therefore go significantly beyond current obligations under the Codes and Standards.
- This breadth of this proposed power is notable. Provided eSafety is satisfied the exercise of this power would improve or promote transparency, accountability, or industry best practice, eSafety may require publication of a broad range of information. The draft bill gives a non-exhaustive list of examples of the kinds of information that may be required to be published, including:
 - Risk assessments and mitigation measures relating to the digital duty of care;
 - Content moderation decisions, volumes and staffing;
 - The number, type and handling of user complaints, as well as the number of Australian accounts suspended or removed (and reasons); and
 - Average active end-user numbers over a specified period.
- The classes of online services to which these publication obligations would apply could be specified by reference to **any matter**, including the level of risk posed, the extent of Australian usage, or whether a provision of the OSA applies to the service. The draft bill **contemplates** – but **does not mandate** – possible exceptions for confidential and private information, setting up a framework for such exceptions to be built into the relevant determination at the discretion of eSafety.
- Non-compliance with the information publication requirements would attract a civil penalty of 30,000 penalty units for body corporates (AUD 10.9 million at the time this alert is published), with eSafety also able to issue formal warnings or infringement notices.

Requirements to provide information for online safety related research

The draft bill proposes to introduce a new Part 14 titled “Research and data access”, which would facilitate the establishment via legislative rules of one or more **data access schemes** requiring providers of online services to give **approved researchers** (being persons employed by an Australian university and approved by eSafety) access to data for online safety-related research.

- The relevant research would need to be approved by a human research ethics committee and prescribed by the legislative rules (to be known as the data access rules) to be in the public interest.
- The new requirement has scope to potentially require providers to hand over sensitive information and statistics about their service to support research around online safety. The data access rules may specify requirements around the security and confidentiality of data to be accessed, although the possible scope of any such protections is presently unclear.
- Non-compliance with the data access rules would attract a civil penalty of 30,000 penalty units for body corporates (AUD 10.9 million at the time this alert is published), with eSafety also able to issue formal warnings, remedial directions, and infringement notices.

Nominated point of contact

eSafety would also be empowered to require providers of online services to nominate a person who is **ordinarily resident in Australia** as a **point of contact**.

- Importantly, anything done under the OSA in relation to the nominated contact would be taken to have been done in relation to the provider itself (for example issuance of reporting notices, remedial directions etc.), effectively removing the ability of foreign-headquartered platforms to delay or resist regulatory action on jurisdictional grounds.
- Non-compliance would attract a civil penalty of 5,000 penalty units (AUD 1.82 million at the time this alert is published).

Repeal of BOSE and Codes & Standards

- As indicated above, a core component of the draft bill is the **repeal of the existing BOSE framework** under Part 4 of the OSA, and the **existing Industry Codes and Standards** made under Division 7 of Part 9 of the OSA. These frameworks would cease to have effect from the date the new digital duty of care will commence, being 12 months after the draft bill receives royal assent.
- With many providers of online services in Australia having invested substantial time and resources since the OSA's commencement into compliance with the BOSE and the Industry Codes and Standards, a core question will be the extent to which such work can be leveraged as a base for compliance with the new digital duty of care. This was a focus of many submissions to the digital duty of care consultation that took place earlier this year, and something we would expect to be clarified through the guidance to be released by eSafety.
- The SMMA remains unchanged by the draft bill. Providers who are required to comply with the SMMA will need to consider carefully how these obligations intersect with the new digital duty of care, noting also the proposed requirement to ensure design features that have negative behavioural impacts do not operate for children in Australia who are under 16.

Other changes to the OSA

The draft bill also proposes to introduce a suite of supporting reforms to the OSA, including:

- A new power for eSafety or approved researchers to assume **sock puppet identities** (false identities) when exercising regulatory functions or conducting (overriding any prohibitions to the contrary in a service's terms of use);
- A restatement of and expansion on eSafety's functions, including around the administration of the digital duty of care;
- A modification to eSafety's existing removal notice powers, enabling eSafety to waive the requirement for a complaint to be made to a relevant service prior to a removal notice being issued, as well as the introduction of new removal notice powers targeting fake nude material; and

- A significant expansion of the existing powers to issue link deletion notices to internet search engine services, allowing such notices to be issued in relation to cyber-bullying material targeted at an Australian child, intimate images, and cyber-abuse material targeted at an Australian adult (in addition to class 1 material). The test for when a link deletion notice may be issued has also been simplified.

Enforcement powers and penalties

- If passed, the proposed legislation would expand eSafety's enforcement toolkit, including a range of new compliance, investigative, and transparency powers.
- In addition to the increases in maximum civil penalties discussed above, the draft bill would also see a tenfold increase to the maximum amount payable under an infringement notice, from 60 penalty units (currently AUD 21,840) up to 600 penalty units (AUD 218,400).
- The ability of eSafety to issue remedial directions related to the digital duty of care, complaints and disputes process requirements, and data access scheme requirements is notable, given eSafety must only hold a **reasonable belief** of an actual or likely contravention of the relevant requirement, and failure to comply with eSafety's direction carries the same penalty as the primary offence. eSafety would also have a new express power to publish any formal warnings it issues.
- A range of eSafety's other investigation powers (including around summoning persons to give evidence) are also proposed to be restated and expanded, representative of the continuing trend in Australia towards equipping regulators with greater visibility over industry conduct and stronger tools to drive compliance before harm occurs.

What still remains unclear?

At present, much about the operation of the proposed digital duty of care and the accompanying changes remains unclear. The draft legislation has not yet been accompanied by an explanatory statement, and there are many obligations that will turn on Ministerial rules or determinations, legislative instruments, or guidance to be released by eSafety.

Particular points of uncertainty include:

- Expectations around what will be required to meet the digital duty of care, beyond the mandatory requirements specified;
- The scope and application of the complaint and dispute process, information publication, and data access requirements;
- To what extent providers will be able (or expected) to leverage and build on work undertaken to meet the BOSE and comply with the existing Codes and Standards; and
- The practical realities of transitioning from Codes and Standards compliance to the new digital duty of care model.

Industry participants may wish to consider making submissions on the draft bill.

What's next?

The draft bill is only open for feedback for a two week period, with consultation closing at **midday on Tuesday, 22 September 2026**.

If passed, most of the key changes will take effect **12 months** after the bill receives royal assent. Some changes (the expansions to the powers to issue removal notices and link deletion notices) will take effect straight away.

For specific advice on the proposed amendments and how they might affect your obligations under Australia's online safety regime, please contact us.

This alert was prepared with the assistance of Kirsten Foley, General Associate, Maxine Betty, Camilla McDonald and Hamish Galbraith, Junior Associates.

Contact Us



Adrian Lawrence
Partner
adrian.lawrence
@bakermckenzie.com



Andrew Stewart
Partner
andrew.stewart
@bakermckenzie.com



Allison Manvell
Special Counsel
allison.manvell
@bakermckenzie.com



Nicholas Kraegen
Special Counsel
nicholas.kraegen
@bakermckenzie.com