

OFFICIAL

eSafety submission

Statutory Review of the Online Safety Act 2021

21 June 2024

OFFICIAL

About eSafety

The eSafety Commissioner (eSafety) welcomes the opportunity to contribute to the statutory review of the *Online Safety Act 2021* (Cth) (OSA).

eSafety is Australia's national independent regulator for online safety. Our purpose is to help safeguard Australians from online harms and to promote safer, more positive online experiences.

The OSA sets out our legislative functions and powers. This includes coordinating online safety activities across the Australian Government, supporting and conducting educational and community awareness programs, undertaking research and administering four investigations schemes¹. The OSA also enables eSafety to require online service providers to report on the steps they are taking to comply with the Basic Online Safety Expectations (BOSE). Additionally, it allows eSafety to register industry codes and/or develop standards to protect Australians from illegal and restricted content.

The multifaceted nature of eSafety's functions and powers – which we approach through the three lenses of prevention, protection, and proactive and systemic change – is vital to ensuring we can holistically address online safety issues.

We also recognise that the online safety ecosystem is both multidimensional and multistakeholder and that success requires coordinated efforts. We thank all our stakeholders for their work in contributing to safer online environments for Australians.

This submission draws on lessons eSafety has learned through administering the OSA, as well as insights from across all our work streams, including our investigations, research, education, and ongoing horizon scanning activities. This ensures the points and goals raised in this submission are grounded in experience and designed to address potential future needs.

Overview of Online Safety Act

Many aspects of the OSA are working well. For example, we have a high success rate in removing harmful content reported to us, and the Basic Online Safety Expectations transparency scheme is assisting to hold services to account and compel them to improve their safety practices.

Our website provides an extensive range of online safety guidance, and we undertake research to better understand the online issues facing Australians and ensure our programs are evidence based. The evaluations we've done on our education, information and awareness raising activities suggests they, along with the work of other stakeholders in this space, are leading to encouraging shifts in the Australian community's awareness of and response to online safety issues². For example, we see increasing numbers of people aware of eSafety, reporting to

¹ eSafety's four reporting schemes are a cyberbullying scheme for children, a cyber abuse scheme for adults, an image-based abuse scheme for all Australians and the Online Content Scheme, which applies to illegal or offensive content.

² Institute for Public Policy and Governance. (2023). *eSafety DPO Grants Program Final Evaluation Report*. University of Technology Sydney. <https://www.esafety.gov.au/research/evaluation-dedicated-project-officer-grants-program>, Orima Research. (2022). *Teacher professional learning program evaluation report*. <https://www.esafety.gov.au/research/evaluation-teacher-learning-program> Orima Research. (2022). *Evaluation of eSafety Women's disability workforce and frontline worker program*. <https://www.esafety.gov.au/research/evaluation-disability-workforce-frontline-worker-program> Synergistiq. (2020). *Online safety for under 5s: Final report*. <https://www.esafety.gov.au/research/evaluation-early-years-program>. Social Innovation Research Institute and the Centre for Social Impact. (2020). *Improving the digital inclusion of older Australians: The social impact of Be Connected*. Swinburne University. <https://www.dss.gov.au/evaluation-of-be-connected>.

OFFICIAL

eSafety, and increased uptake of educational resources and training³. We also see some encouraging trends over time in the Australian public's knowledge and confidence in responding to online harms which we will continue to monitor⁴.

However, the OSA also has certain limitations. Critically, these limitations lead to limitations in how eSafety can protect and support Australians experiencing online harm.

eSafety's hopes for the review of the Online Safety Act

We have **five overarching goals** for the OSA review.

We believe achieving these goals will position eSafety to more effectively safeguard Australians from online harms and promote online safety for all Australians.

1. A clearer and more coherent conceptual framework and logic for how existing and proposed new elements of the OSA fit together, and enhanced enforceability across these elements.
2. Greater clarity in relation to the industry sections covered by the OSA, and alignment of definitions and regulatory tools with the practical realities of how the internet and digital technology works, now and into the future.
3. Relatedly, increased flexibility for eSafety to be nimble, effective, and able to adapt to evolving challenges and paradigm shifts in the digital environment.
4. Greater consistency across the investigation schemes, and updates to ensure they remain fit-for-purpose and future-proofed to deal with existing and emerging online harms emanating from conduct as well as content.
5. National and international regulatory coherence and coordination, including ensuring that the penalties associated with the OSA are on par with other domestic and international digital platforms regulators.

Goal 1: Coherent and enforceable regulatory framework

Key objectives

- **Existing and proposed new elements of the OSA fit together in a clear, logical conceptual framework.**
- **Legislative coherence contributes to improved regulatory efficacy and enforceability.**

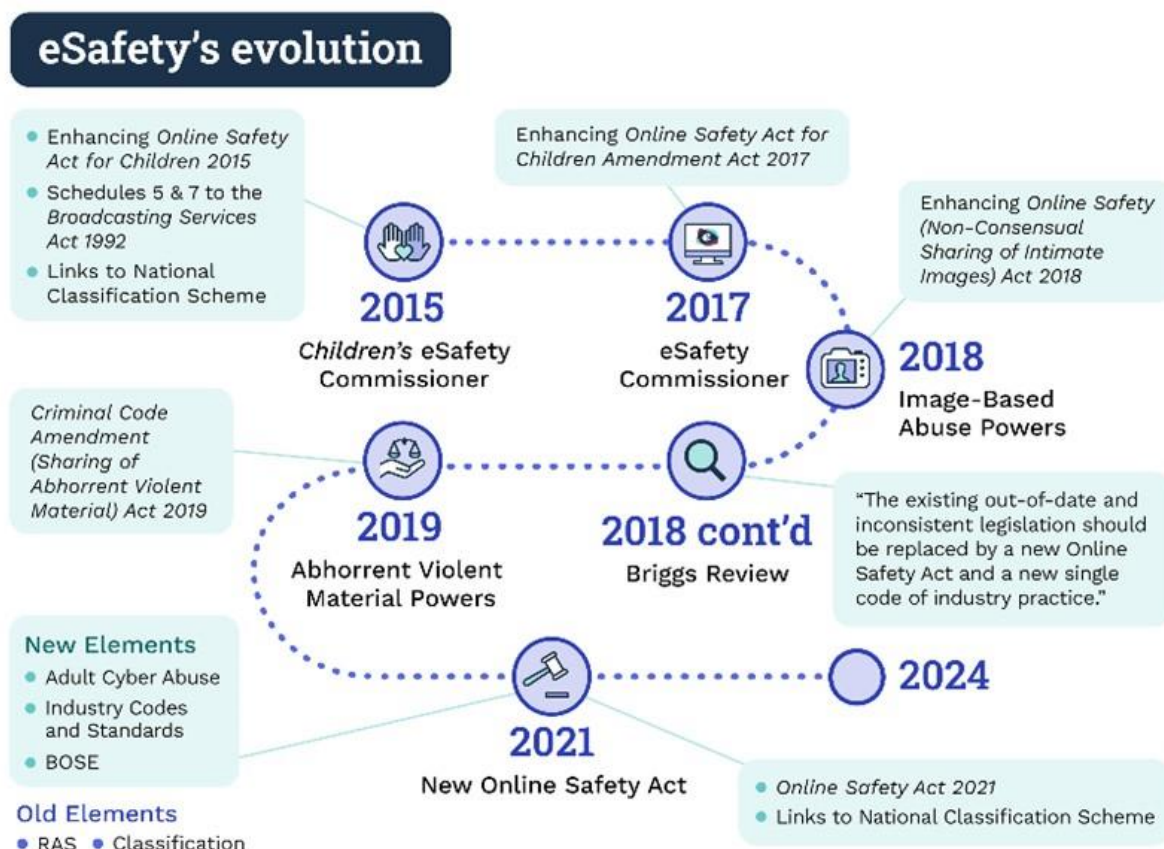
Since 2015, Australia's online safety regulatory framework has been evolving continuously to keep pace with the rapidly evolving digital landscape and emerging online harms. The Children's eSafety Commissioner became the eSafety Commissioner in 2017. In 2021, the OSA brought most of the Commissioner's existing powers into one Act. This included new elements such as the

³ Social Research Centre. (2023). Online Safety Issues Survey - Summary report. <https://www.infrastructure.gov.au/sites/default/files/documents/2023-online-safety-issues-survey-summary-report-june2023.pdf> eSafety, 2022. 'Mind the gap: Parental awareness of children's exposure to risks online'. *Aussie Kids Online*. <https://www.esafety.gov.au/research/mind-gap>.

OFFICIAL

Basic Online Safety Expectations, alongside older elements and eSafety's broader enablement work, such as the Safety by Design initiative.

New powers and schemes have been introduced to address specific harms and respond to crisis events.



This ongoing evolution has been essential – and broadly successful – in enabling eSafety to respond to online harms. However, it has also inevitably led to occasional inconsistencies in the OSA and the regulatory framework it supports.

We see this review as an opportunity to hone the OSA's strengths, improve the cohesion among its existing elements, and ensure that changes are woven into an overarching logic that promotes effective action for Australians' online safety. Any new regulatory options will be most effective as part of a coherent framework alongside existing responses, with clear aims for each element, and a focus on maximising compliance, enforcement, and safety.

Interconnected government reforms, such as updates to the Basic Online Safety Expectations Determination, developments in AI, doxing, and security and privacy reforms, must strive to achieve legislative coherence to the greatest extent possible. This coherence will contribute effectively to improved regulatory efficacy and enforceability.

OFFICIAL

Goal 2: Industry sections reflecting practical realities and likely evolution

Key objectives

- **Industry sections covered by the OSA are clarified.**
- **Definitions and regulatory tools are aligned to practical realities of how the internet works.**
- **The OSA ensures every layer of the digital ‘stack’ plays its part.**

The OSA outlines eight industry sections. However, how the OSA applies and the specific obligations of providers, and eSafety’s powers in relation to those obligations, partly depend on the industry section to which a provider belongs. For example, eSafety’s investigative schemes for adult cyber abuse, child cyberbullying and image-based abuse primarily apply to social media services, relevant electronic services, and designated internet services.

This holistic approach was designed to recognise the breadth of the online industry, which covers services ranging from social media to carriage services and equipment manufacturers. Australians interact with these services in various ways, and regulatory interventions appropriate and adequate for one sector might be unsuitable for another.

However, the current definitions of industry sections in the Act can be confusing for providers and may not always reflect practical realities. Based on consultation feedback, we understand it is sometimes difficult for a service to determine their appropriate section. Some services even meet the definitions of multiple sections, adding further complexity. As the purposes, functionalities, and types of communication available across the digital landscape continue to evolve and converge, applying the current section definitions to online services will become increasingly complex.

There is now an opportunity to make sure eSafety’s regulatory efforts are effective and future-proofed by revisiting the scope of industry sections. Ensuring they appropriately capture and categorise the full array of online services will support effective responses to online harms by providing practical enforcement levers across the digital stack and preparing eSafety to respond to emerging technologies and evolutions in the digital ecosystem.

Goal 3: Increased flexibility to respond to emerging environments and issues

Key objectives

- **eSafety’s enabling legislation and structures support effective responses to evolving challenges.**
- **eSafety can adapt nimbly to new technologies and paradigm shifts in the digital environment.**

OFFICIAL

The global digital landscape is constantly evolving, making online safety issues more complex, pervasive, and challenging to regulate. Since Australia's online safety legislation was last reviewed in 2018, which led to the OSA passing in 2021 and starting operation in 2022, technologies such as generative AI and immersive environments have developed significantly and become widely accessible, bringing new benefits and risks.

Part 9 of the OSA is the Online Content Scheme, which relates to restricted and illegal content. It is dependent on the National Classification Scheme, which includes the National Classification Code and related guidelines. Notably, the National Classification Scheme was devised to guide the classification of films, publications and computer games intended for commercial release in Australia. It was not devised for online environments, including for user-generated content distributed online.

This means there are inherent difficulties with the application of the national classification code to the OSA.

From a first principles perspective, this includes that the national classification code is based on principles of morality, decency and propriety, whereas the OSA is harms-based. It also includes that classification under the national classification code is based on specific context⁵, whereas the BOSE and codes and standards are seeking to create systemic, scalable expectations and obligations.

From a practical perspective, the nature of the content under the National Classification Scheme and the OSA is fundamentally different. Whereas films, computer games and publications like books are fixed and predetermined in advance of publication, user-generated illegal and restricted content is dynamic, fluid and even ephemeral. Content of this nature is designed to go viral and thus requires a regulatory toolset and approach tailored specifically to this content and its almost instantaneous distribution. It also requires the enabling and complementary functions, such as research, evaluation and education initiatives, to be specific to the dynamic nature of online content.

To add further practical challenges, slightly different guidelines apply under the National Classification Scheme depending on whether content is a computer game, publications, form or other, which can create confusion.

There are also several online harms that are only partially covered by our regulatory remit. This includes online hate, volumetric attacks and technology-facilitated abuse (TFA), including TFA subsets, such as technology-facilitated gender-based violence and technology-facilitated family, domestic and sexual violence. While we can address these harms in various ways, including through Safety by Design and educational resources, the options to address are more limited than in relation to other online harms more directly covered by our remit. The constantly evolving and interconnected nature of online harms demonstrates the need for eSafety to have flexibility to effectively regulate this dynamic industry, adapt to changes in online services, and respond to new harms as they emerge.

⁵ See how ['How a rating is decided | Australian Classification'](#)

OFFICIAL

This flexibility could include enforceable mechanisms to support systemic responses to a wider variety of harms, such as industry codes or standards covering harms beyond class 1 and class 2 illegal and restricted content⁶. It could also include improvements to existing measures, such as:

- provisions to review and, if necessary, alter codes and standards if they become outdated
- changes to support industry codes that cover part of an industry section
- allowing eSafety to move directly to an industry standard without completing the codes process first when an emerging technology or harm requires an immediate response
- decoupling the codes and standards process from the National Classification Scheme, so that they are untied from a classification scheme that was not devised for the internet and can better respond to the dynamic online environment.

Maintaining an up-to-date understanding of emerging technology is central to eSafety's operations and is a prerequisite for an effective regulatory response. In addition to our work to understand [Australians' experiences](#) and emerging [technology trends and challenges](#), the OSA should enable eSafety to directly and meaningfully investigate specific platforms, technologies or industry sectors where online harms are surfacing.

Goal 4: Consistent and future-proofed regulatory schemes and tools

Key objectives

- **All regulatory schemes are equipped to respond to existing and emerging online harms emanating from both content and conduct.**
- **Updates ensure Investigations schemes are consistent, fit-for-purpose and future-proofed.**

The staggered introduction of eSafety's regulatory schemes since 2015 has led to notable inconsistencies in the powers available to address the different harms under each scheme. Some schemes take account of future regulatory needs more comprehensively than others. Operational experience reveals that each scheme has different advantages in responding to the challenges of addressing online harms.

This presents an opportunity to align the powers across eSafety's regulatory schemes by extending the strongest aspects of each scheme to the others and making additional improvements where appropriate.

For example, a common issue across the four investigations schemes and the codes and standards is their emphasis on harmful **content** and its removal. However, online harms take many forms, including **contact**, such as between adults and children, and various types of harmful **conduct**, such as simulated sexual assault and other forms of attack in immersive environments.

The image-based abuse (IBA) scheme is currently best equipped to address conduct harms. It responds to threats to share intimate images as well as actual sharing. It includes a general

⁶ Class 1 and class 2 are defined in the OSA in reference to the National Classification Code. Class 1 material includes child sexual exploitation material, pro-terrorist material, and material that promotes or incites crime. Class 2 material includes non-violent sexual activity, or anything that is unsuitable for a minor to see.

OFFICIAL

prohibition on sharing intimate images and threatening to do so. Under the IBA scheme, eSafety can give a remedial direction requiring an end-user who has breached the prohibition on image-based abuse to take specified actions to reduce the risk of further breaches, such as deleting images from their devices. Similar provisions across the other schemes could offer options for dealing with harmful behaviour. For example, under the cyberbullying scheme, a successful complaint could result in a direction to an end-user not to create or post content targeting the complainant.

We also see other conduct related harms across all our investigations scheme. This includes recidivism and volumetric attacks (or ‘pile-ons’), and other changes to deal with harmful behaviour might include specific remedies directed at these issues.

Other areas that could be harmonised across eSafety’s current removal schemes include jurisdictional requirements and prerequisites for reporting content to eSafety.

For this strategic and streamlined approach to technical regulation to be effective, eSafety will need the supporting systems, processes and people with specialised technology skills. This includes the technical capacity to respond to increasingly complex and multiplex technical matters eSafety investigates and regulates.

Goal 5: Enhanced regulatory coordination and comparable penalties

Key objectives

- **National and international coherence and coordination.**
- **eSafety’s enabling legislation and structures are aligned with national and international regulatory frameworks.**
- **As the online regulator of a middle power, eSafety can leverage international coordination to promote compliance.**

The internet is globally distributed, and neither the risks people face online, nor the online services they use, are confined to national borders. Regulating a global industry that has significant scale, power and resources also presents challenges for individual countries. Global service providers must now comply with online safety legislation in multiple jurisdictions, and Australia is a comparatively minor market for most of them. These providers must also comply with other requirements, including from other Australian digital platforms regulators.

Therefore, strategic coherence with other domestic and international regulators is essential to achieve our shared goals, exercising collective influence to ensure that Australians’ online safety does not stop at the border, and that companies can benefit from compliance economies of scale and legal certainty.

Domestically, eSafety collaborates through the [Digital Platform Regulators Forum \(DP-REG\)](#) to share information and collaborate on cross-cutting issues involving digital platforms. Internationally, we foster collaboration and regulatory coherence through the [Global Online Safety Regulators Network](#), which brings together independent regulators to cooperate across jurisdictions. The coordinating power of the Network allows its members to collectively drive greater coherence in regulatory approaches across areas of similarity, and share learnings with

OFFICIAL

each other where there are areas of difference. We also consult regularly with international counterparts, including Ireland, the UK and USA and draw on global approaches, such as the Digital Services Act. Lessons from these engagements inform our activities and assessments of interventions that might promote online safety in Australia.

The OSA review presents an opportunity for reform to facilitate improved alignment between eSafety and its domestic and international regulatory colleagues. This should include ensuring that the penalties and powers available to eSafety are in line with those available to comparable regulators in Australia and elsewhere. It could also involve aligning on shared expectations for addressing specific online harms or identifying common reasonable steps services can take to address specific harms and risk factors.

There is also opportunity to enhance information and insights sharing. This includes ensuring that eSafety can share information with regulatory colleagues in appropriate cases. For example, sharing information with international partner NGOs to facilitate removal of child sexual exploitation and abuse material, and sharing information received in response to transparency notices with international regulators.

It also includes eSafety being able to share its regulatory learnings with a wider range of stakeholders in the online safety ecosystem, including policymakers, researchers, academics and technical experts. In turn, eSafety can learn from these stakeholders and other regulators around the world to ensure Australia's approach comprises multidisciplinary best practice.

Through greater regulatory coordination and international alignment, we aim to exercise collective influence to achieve better online safety outcomes. Greater international alignment may also reduce compliance challenges for companies, providing greater legal certainty across jurisdictions.

eSafety into the future

In the almost 9 years eSafety has been in operation, we have established ourselves as the national leader of online safety and foremost among international online safety experts.

We see this review as an opportunity to provide eSafety a stronger and more robust legislative basis, which will allow us to more effectively and efficiently achieve our ultimate goal: safeguarding Australians from online harms and promoting safer, more positive online experiences for all Australians.