Tech Council
of Australia

Online Safety Act Review

Tech Council of Australia Submission

June 2024

techcouncil.com.au

1. Introduction

Thank you for the opportunity to make a submission on the operation and effectiveness of the *Online Safety Act 2021* (**OSA**).

The Tech Council of Australia (**TCA**) is Australia's peak industry body for the tech sector. The tech sector is a key pillar of the Australian economy, employing over 935,000 people. This makes the tech sector equivalent to Australia's seventh largest employing sector.

The TCA represents a diverse cross-section of Australia's tech sector, including start-ups, scale-ups, venture capital funds, as well as global tech companies. Many of our member companies provide services which are likely to fall within the scope of the OSA but (note that our organisation does not represent most of the major social media companies).

We support the overarching objects of the OSA, which are to improve and promote the safety of Australians online.

We have also previously welcomed the broader online industry codes and standards process as important in creating a new shared baseline across Australia's technology sector, contributing towards a safer and more responsible digital environment for Australians by reducing the ability of Australians to access and spread seriously harmful content online. Our members strongly oppose the misuse of online services for these types of illegal and harmful activities, and many have already invested significantly to implement risk mitigation and response measures.

As the Government considers potential reform of the OSA, we continue to call for an outcomes- and risk-based approach. We strongly support tailoring the obligations for online safety to the level of risk posed by a service, and the type of content. This approach provides a regulatory response to online safety which ensures that measures are proportionate and compliance resources are appropriately targeted.

This submission considers the operation and effectiveness of the OSA and makes several key principles-based recommendations to improve the effective administration of Australia's online safety regime and the protection of Australians online. We make three recommendations, which are informed by the Tech Council's guiding principles for best practice tech regulatory design (see Appendix A):

1. **Recommendation 1:** the obligations in the OSA should be risk-based, proportionate and targeted to the harms that they seek to address.

2. **Recommendation 2:** to support effective implementation and enhance regulatory compliance, simplification and streamlining should be key objectives of the OSA review process. This is particularly important to improve consistency with other Australian laws and regulations and avoid overlap or duplication, while maintaining high standards.

3. **Recommendation 3:** the OSA should be harmonised with other jurisdictions where appropriate to ensure alignment with international best-practice and consistency in the obligations placed on service providers.

2. Risk-based and proportionate obligations

One of the key guiding principles of tech regulatory design is that regulations should be risk-based and proportionate. In the context of the OSA, this would help ensure resources are targeted where they are most needed to achieve desired safety outcomes, while also avoiding unintended consequences such as increasing barriers to entry or inadvertently capturing low-risk parts of the tech sector. OSA obligations on service providers should be proportionate to the level of risk from a particular service, and the nature and severity of the potential harm.

However, the OSA does not expressly assign or limit obligations based on factors such as the size, reach or function of a service. The types of services covered by the OSA are also distinctly broad by virtue of the Designated Internet Services and Relevant Electronic Services categories. This is in contrast to other online safety schemes, such as the EU's *Digital Services Act* (**DSA**), which applies obligations only to service providers that meet a particular risk, reach and size threshold, or the UK which focuses on user-to-user platforms.

While the OSA does implicitly recognise that different services may have different risk profiles, the consideration of risk in the obligations stemming from the OSA is not guaranteed. For example, the expectations on services within the social media services, designated internet services and relevant electronic services categories are the same according to the Basic Online Safety Expectations (**BOSE**), even though there are widely varying degrees of risk between these different types of services and between services within these categories.

Recommendation 1: The OSA should be amended to incorporate a risk-based approach in setting out its obligations.

Amending the OSA so that it explicitly incorporates a risk-based approach would align the OSA with other international approaches to regulating online safety, such as the DSA. This would mean that BOSE expectations on service providers would be tailored to the actual risk profile, instead of assuming that there is equal risk for all service providers across these categories. A risk-based approach would also facilitate service providers undertaking a risk assessment. This would enable service providers to implement proportionate safety measures, such as by designing systems and processes that are responsive to their nature, features, user base and reach of their content, while also ensuring accountability to service users and the broader public.

An increased focus on risk assessments would also eliminate the need for prescriptive and inflexible definitions of services and harms, that are quickly outdated when technology changes or use of services evolves. An explicitly risk-based approach would also improve accountability for service providers, especially for services employing new technologies that provide an increased risk of harm and would need to reassess risk as new technologies and potential harms emerge.

As part of a risk-based approach, we also encourage the Government to consider the appropriateness of the legislation capturing low-risk services such as business-to-business enterprise software. These could be explicitly excluded through definitions in the OSA, or by the Minister issuing a legislative instrument under section 14(2) of the Act.

3. Opportunities to enhance compliance through simplification and streamlining

There are many opportunities for the OSA to be simplified and streamlined, while maintaining high standards, which would deliver benefits for regulators, industry and the public. Areas that contribute to complexity and uncertainty in the regime that could be addressed through the statutory review process include:

- Overlap between frameworks set up within the OSA (e.g. BOSE, industry codes, industry standards and content take-down schemes)
- Overlap between the OSA and other legislative frameworks (e.g. consumer, criminal, defamation, anti-discrimination, privacy and telco laws)
- A lack of clarity on scope of the OSA (e.g. due to definitions being drawn from the National Classification Scheme)
- Legislative complexity driven by constant change in legislative requirements over short periods of time
- Overlap with other reform processes outside of the OSA (particularly privacy reform, but also AI, misinformation, anti-doxing and criminal code reforms), and
- Transparency and oversight arrangements with respect to key decision-making made under the OSA (e.g. processes for industry codes and standards).

Within the OSA, there are detailed frameworks for a range of online safety concerns, including image-based abuse, cyberbullying and cyber-abuse schemes. In addition to the obligations contained within the OSA, the OSA also provides the foundation for additional regimes through the BOSE, industry codes under the Online Content Scheme (**Industry Codes**), and industry standards through the Online Content Scheme (**Industry Standards**).

In addition to the multiple separate frameworks contained within the OSA, online safety and harms in Australia are governed by a range of other laws, including consumer, criminal, defamation, discrimination, electoral, privacy and telecommunications laws. These laws also have significant consequences for safeguarding Australians online.

These overlapping regimes – both within the OSA, and with regimes that fall outside of the OSA – can create compliance challenges for many service providers. The current level of legislative complexity for service providers in Australia significantly increases the costs of providing services in Australia, and raises the risk of instances of unintentional non-compliance with these laws, particularly for less mature or established service providers. The risk of unintentional non-compliance is further raised in circumstances where the OSA is not risk-based and may apply to a range of less sophisticated service providers for which the risks to online safety are relatively low.

A lack of clarity on the scope of the OSA has also led to regulatory overlap and complexity with other regulatory regimes. In particular, there is substantial overlap between the OSA and the *Classification (Publications, Films and Computer Games) Act* (the **National Classification Scheme**), which has led to increased compliance burdens on service providers that are captured by both these regimes for the same service. For example, the definitions in the OSA are underpinned by the same definitions which are used in the National Classification Scheme and are meant for professionally produced media rather than user generated content, and are therefore not fit for purpose. This review into the OSA should ensure that there are clear distinctions between the types of content that are captured by each scheme, with the National Classification Scheme covering services that primarily distribute professionally produced content and the OSA covering intermediary services that contain user-generated content. The nature and scale of harms addressed by the National Classification Scheme, which deals with harms related to professional produced content in legacy media formats, are not well suited to addressing online, user-generated harmful content.

It is also imperative that these schemes draw clear lines between what is illegal content on a platform, and content that may be considered harmful in some contexts but is lawful (which service providers address via terms of services and community guidelines on their platforms).

This legislative complexity also increases the risk of duplicative obligations within the OSA, and there are likely to be benefits from streamlining, consolidating and simplifying the obligations within the OSA and the other regimes that the OSA provides the foundations for.

We also consider that the review of the OSA must be coordinated with other related reform processes, such as the classification reforms, Privacy Act reforms, the development of industry codes, and the potential regulation of misinformation and disinformation, as well as the Government's approach to governance and regulation of AI. This would ensure appropriate balancing of safety, privacy and security, and ensure that each regime is appropriately scoped given the potential overlaps between other regimes.

Further, given the privacy implications arising from the use of age verification technologies, we consider that the Government should wait for the outcomes of the age assurance trial before imposing any requirements related to age verification or the use of age verification technologies in the context of the Class 2 industry codes.

The use (and abuse) of technology evolves quickly, and as concerns about online safety evolve in response to this, the capacity for existing regulations to respond is often questioned. As a result, digital safety laws have been and continue to be in a constant state of change, demonstrated by the transition to the OSA from the *Enhancing Online Safety Act*, and the subsequent development of regulations subordinate to the OSA. In addition to this, there have been a range or proposed additional overlapping reforms, such as the Privacy Act Review, the Government's consultation on 'safe and responsible AI', the *Combatting Misinformation and Disinformation Bill 2023* and recent anti-doxing consultations, and the *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024* which includes the creation of deepfake sexual material as an offence. There has also been consultation on legislation that was ultimately abandoned, for example the *Social Media (Anti-Trolling) Bill 2022*.

In addition to an ever-evolving regulatory landscape for online safety, there has been a large amount of political and community dialogue regarding online safety, and developments through technology pilots, parliamentary committees and other investigation and recommendations processes.

This changing landscape for online safety laws has introduced additional complexity and uncertainty about the operation of the OSA for service providers in Australia. The OSA should contain regulation that is adaptable for use across an ever-evolving landscape, without requiring constant changes or amendments to address specific evolving harms.

We also consider that there is scope for improved transparency and oversight in the OSA. In particular, the industry has concerns that much of the key decision-making in relation to the OSA occurs in subordinate legislation or through industry codes and standards and does not have appropriate oversight by Parliament or executive government, nor does it benefit from proper public debate to weigh-up the trade-offs of different courses of action.

Recommendation 2: to support effective implementation and enhance regulatory compliance, simplification and streamlining should be a key objective of the OSA review process. This is particularly important to improve consistency with other Australian laws and regulations and avoid overlap or duplication, while maintaining high standards.

The review should consider opportunities for the OSA to be simplified and streamlined, both in relation to the various frameworks that exist for online safety within the OSA, as well as in relation to streamlining and simplifying the operation of the OSA alongside other regulation.

We also consider that the review of the OSA should consider opportunities to improve transparency for key decision-making within the OSA, to ensure that there is sufficient Parliamentary, executive government and public oversight of key decision-making under the regime.

4. Alignment with international best practice

Improving online safety is a global objective, with many service providers in Australia complying with other online safety legislation in other jurisdictions. Improved alignment with international online safety regimes would allow Australia to harness the benefits of shared experience, global best practice, and collective influence to tackle online harms that cross borders. It is also an opportunity for Australia to develop unified regulatory tools and practices with other jurisdictions that deal with online safety.

For example, the EU's DSA approach to online safety represents a more systemic approach to online safety than the OSA does and is more clearly risk-based in its approach. We consider this approach would make Australian online safety regulation better placed to adapt to the rapid pace of technological change and patterns of harm.

Recommendation 3: the OSA should be harmonised, where appropriate, with international best practice for a risk-based approach to improving online safety, such as the DSA, to ensure cohesion with international best-practice online safety practices, and improve international consistency in the obligations on service providers.

A more coordinated, better aligned approach to international online safety would create a more predictable regulatory environment, reduce compliance costs, and result in significant benefits for both regulators, industry and the public.

5. Previous recommendations made by the TCA in relation to online safety

We also continue to support and advocate for previous recommendations that we have made in relation to the OSA. In particular, we refer to recommendations that we have made in relation to the *Draft Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024* and *Draft Online Safety (Designated Internet Services – Class 1A and 1B Material) Industry Standard 2024* (**Draft online safety standards**) consultation, including that:

- Government should ensure that the definition of high-impact generative AI designated internet service category is coordinated and aligned with broader whole-of-government approaches and definitions on high-risk AI.
- Government should clarify that foreign or international bodies include standards setting bodies, leading global institutions and industry best-practice.

Adoption of these recommendations would ensure that the online safety standards are risk-based, appropriate targeted and contains obligations that are clear and internationally consistent.

Appendix A: Tech Council's guiding principles for best-practice tech regulatory design

The TCA recommends the following five guiding principles for best practice regulation in the digital economy:

- **Informed and coordinated** – technology regulation and policy development inherently addresses novel concepts and issues. For this to be effective, it requires us to have sufficient time, stakeholder input, and expertise to make informed policy decisions. Rigorous analysis and industry engagement, with thoughtful consideration of the interrelationships with other policies and regulation, helps us avoid the pitfalls of technical infeasibility and enhances regulatory compliance.

- **Proportionate** –a risk-based approach targeted at clearly defined problems enables regulation to achieve the objectives that are sought, while also avoiding unintended consequences such as increasing barriers to entry for others, or inadvertently capturing other parts of the tech sector.

- **Timely** – premature regulatory intervention can disproportionately impact emerging startups, business models, and technologies. To ensure Australia maintains a competitive place in the global market, we should be proactive in considering a range of potential policy levers, ensure that industry is given appropriate clarity and guidance, while enabling the appropriate opportunity and space for innovation.

- **Consistent and interoperable** – the technology industry is global by nature and few policy questions are unique to Australia. Regulation should consider and align, where appropriate, with domestic and global regulation to strive towards harmonisation and interoperability.

- **Supports innovation and growth** – becoming a leading digital economy means that Australia should aim to encourage the responsible and early introduction and deployment of technology, this means avoiding prescriptive technical requirements that may become quickly outdated or inhibit innovation.