28 June 2024

Email: OSAReview@COMMUNICATIONS.gov.au

Mail: Director – Strategy and Research
Online Safety, Media and Platforms Division
DITRCA
GPO Box 594
Canberra ACT 2601

Dear Ms Delia Rickard PSM

Submission re: Independent Review of the *Online Safety Act 2021*

The Australian National University's Tech Policy Design Centre (TPDC) is pleased to make a submission to the independent Review of the *Online Safety Act (2021)* (the Act).

We urge the Australian Government to use this review to lay out its strategic vision for the online lives of Australians, articulating the part that the Online Safety Act can play alongside policy and legislation across the whole of government to bring this vision to life.

In this submission, we outline three ways that Australia can harness public appetite to shape the Online Safety Act. These three recommendations address the current challenges of today's tech landscape and future proof the mandate of the eSafety Commissioner to ensure the best outcomes for citizens.

Australia has a reputation as a world leader in online safety – the first country to establish a dedicated government organisation to keep citizens safe online in 2015. Australia's user-focused, complaints-based take down schemes – for cyber bullying, adult cyber abuse and image-based abuse - remain world leading in providing meaningful harm minimisation and support to individual Australians. Australia's content-focused take down schemes have served as a safety net to address harms after they have occurred and remain an important tool for citizens. However, this approach has a limited ability to scale up in response to increasing volumes of reports.

Since the Act was drafted in 2020, the scale and scope of online safety challenges and potential for harms online has increased significantly. Digital services form an increasing integrated part of Australians' everyday lives, and the volume and dynamics of content creation and distribution continue to evolve rapidly, particularly in the generative AI boom. The review represents an opportunity to introduce into the Act new ways to prevent harms before they occur (ex-ante), as well as enhancing redress avenues for victims of harms (ex-post).

We recommend three priorities for the Australian Government's review of the *Online Safety Act 2021*:

1. Ensure that online safety policy is part of a broader vision for Australia's digital future, where updates to the Act are developed in coordination with other areas of tech policy specialisation across government.
2. Increase corporate responsibility for digital services defined in the Act, by:
   a) continuing preventative, risk-based obligations
   b) increasing the consequences of non-compliance, through transparency obligations, greater fines, a direct right to action for individual users, and international coordination on regulatory reform and enforcement

3. Strengthen democratic protections underpinning the Act to ensure Australia maintains its status as a world leader in online safety by:
   a) enhancing the checks and balances, appeals processes, and oversight of the eSafety Commissioner's powers
   b) obligating the eSafety Commissioner to conduct international advocacy with an awareness of the potential harm of online safety regulations in non-democratic contexts

We provide the following submission to you for your consideration.

Sincerely

[redacted]

Zoe Hawkins
Head of Policy Design
ANU Tech Policy Design Centre

About the Tech Policy Design Centre

The Tech Policy Design Centre (TPDC) is a nonpartisan, independent research organisation at the Australian National University. Our mission is to shape technology for the long-term benefit of humanity. We work to mature the tech-governance ecosystem in collaboration with industry, government, civil society, and academia.

1. Ensure that updates to the Act are developed in coordination with other areas of tech policy specialisation across government, where online safety policy is part of a broader vision for Australia's digital future.

With the growing influence of digital technologies on every facet of the lives of Australians, there is increasing activity across different parts of the Australian Government on tech policy related matters.

Under section 27 of the Act, the eSafety Commissioner is responsible to 'coordinate activities of Commonwealth departments, authorities and agencies relating to online safety for Australians'. This allocation of responsibilities remains effective and appropriate given the deep expertise in online safety of the Commissioner and their office.

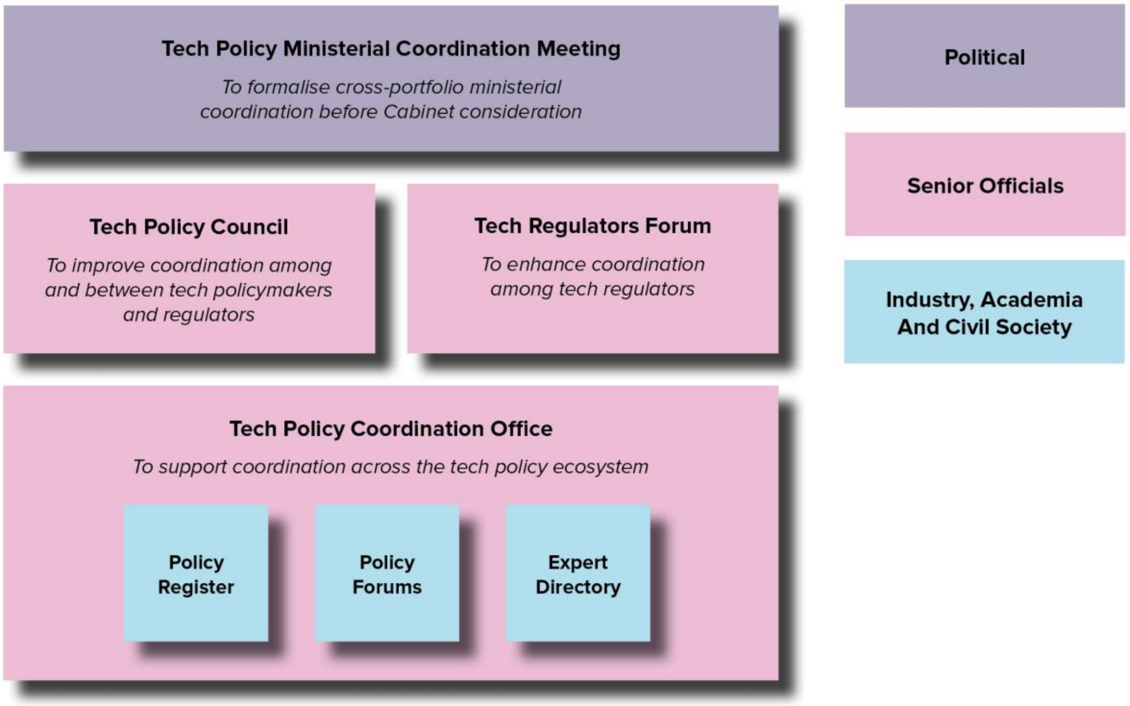
Technology is a horizontal societal enabler, and therefore it is appropriate for primary portfolios, where officials have existing relevant expertise, to lead on how their core policy issues manifest in interaction with technology. However, in maintaining this distributed approach, it is essential that tech policy is not made in silos but rather in a coordinated manner and in pursuit of a larger, coherent vision for Australia's digital future.

At the same time, in an age where many social and economic policy challenges manifest most prominently and rapidly in online environments, the Government should also be cautious to avoid framing any issue that appears in the online environment as only an online safety matter. Discrimination, competition, privacy, mental health and other important policy areas are the source of important policy development that should flow through into our online safety agenda.

Coordination is essential as many technology-related policy issues interact with each other in complex ways. The Australian Government is currently considering reforms across online safety, privacy, artificial intelligence, misinformation, and others (listed in Appendix 1 of the Discussion Paper). As such, in reviewing the Act, the Government should coordinate how online safety policy priorities fit in and integrate with broader government tech policy priorities.

TPDC's research report 'Cultivating Coordination' recommends a Tech Policy Coordination Model that delivers greater coherence between government priorities and policies across the tech ecosystem. The design of this model is based on desktop research and interviews with 32 heads and senior representatives of Australian regulators, the Australian Government, industry, academia, and civil society, as well as a comparative study of 14 jurisdictions internationally. The Model proposed in the report is ready for immediate implementation and is largely cost-neutral. It would build upon the Digital Regulators Coordination Forum (DP-Reg). 'Cultivating Coordination' and its companion report, 'Tending the Tech Ecosystem' is available here.

Figure 1: Best Practice Tech Policy Coordination Model



Tech Policy Ministerial Coordination Meeting

To formalise cross-portfolio ministerial coordination before Cabinet consideration

Tech Policy Council

To improve coordination among and between tech policymakers and regulators

Tech Regulators Forum

To enhance coordination among tech regulators

Tech Policy Coordination Office

To support coordination across the tech policy ecosystem

Policy Register

Policy Forums

Expert Directory

Political

Senior Officials

Industry, Academia And Civil Society

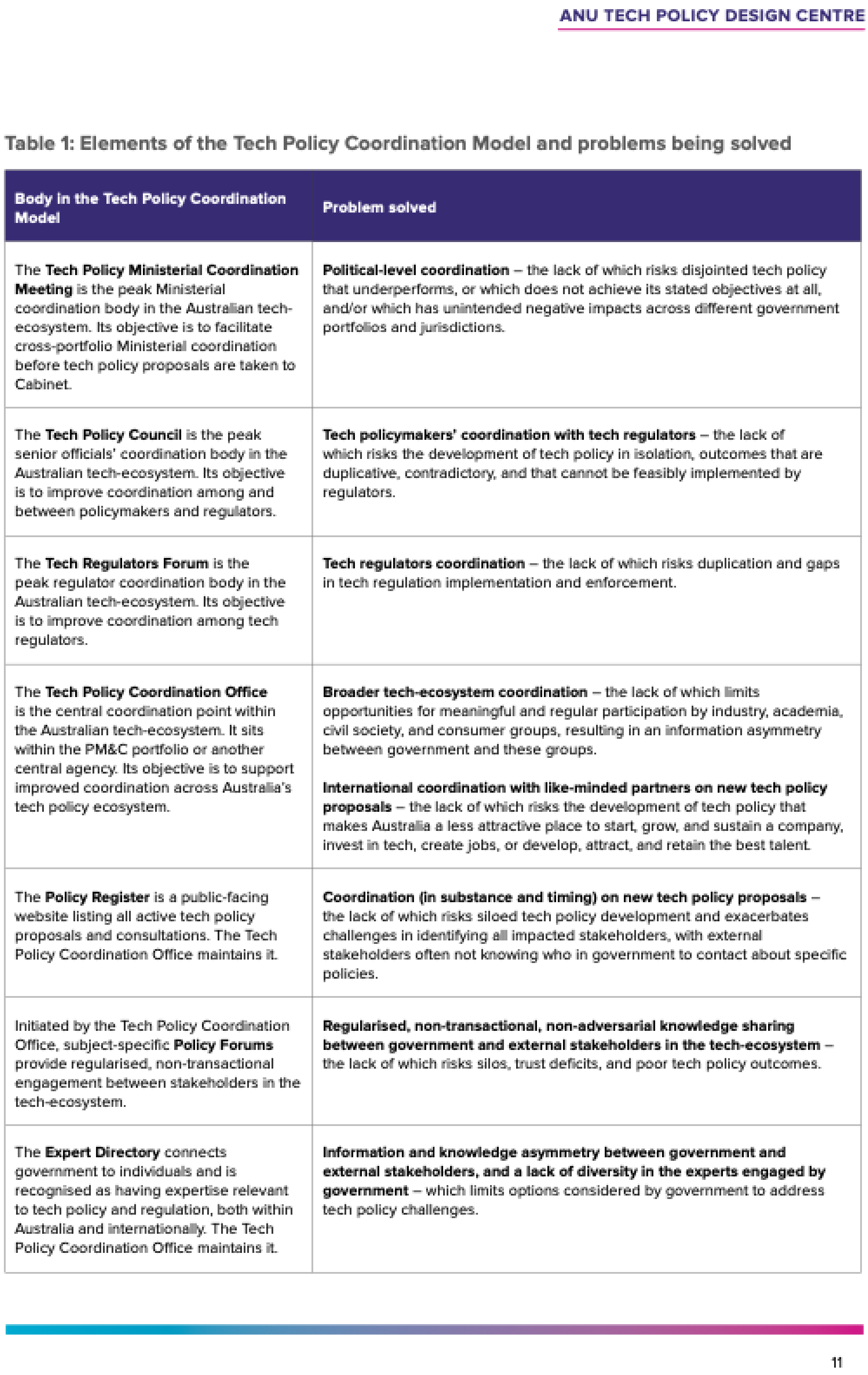


Table 1: Elements of the Tech Policy Coordination Model and problems being solved

Body in the Tech Policy Coordination Model	Problem solved
The **Tech Policy Ministerial Coordination Meeting** is the peak Ministerial coordination body in the Australian tech-ecosystem. Its objective is to facilitate cross-portfolio Ministerial coordination before tech policy proposals are taken to Cabinet.	**Political-level coordination** – the lack of which risks disjointed tech policy that underperforms, or which does not achieve its stated objectives at all, and/or which has unintended negative impacts across different government portfolios and jurisdictions.
The **Tech Policy Council** is the peak senior officials' coordination body in the Australian tech-ecosystem. Its objective is to improve coordination among and between policymakers and regulators.	**Tech policymakers' coordination with tech regulators** – the lack of which risks the development of tech policy in isolation, outcomes that are duplicative, contradictory, and that cannot be feasibly implemented by regulators.
The **Tech Regulators Forum** is the peak regulator coordination body in the Australian tech-ecosystem. Its objective is to improve coordination among tech regulators.	**Tech regulators coordination** – the lack of which risks duplication and gaps in tech regulation implementation and enforcement.
The **Tech Policy Coordination Office** is the central coordination point within the Australian tech-ecosystem. It sits within the PM&C portfolio or another central agency. Its objective is to support improved coordination across Australia's tech policy ecosystem.	**Broader tech-ecosystem coordination** – the lack of which limits opportunities for meaningful and regular participation by industry, academia, civil society, and consumer groups, resulting in an information asymmetry between government and these groups. **International coordination with like-minded partners on new tech policy proposals** – the lack of which risks the development of tech policy that makes Australia a less attractive place to start, grow, and sustain a company, invest in tech, create jobs, or develop, attract, and retain the best talent.
The **Policy Register** is a public-facing website listing all active tech policy proposals and consultations. The Tech Policy Coordination Office maintains it.	**Coordination (in substance and timing) on new tech policy proposals** – the lack of which risks siloed tech policy development and exacerbates challenges in identifying all impacted stakeholders, with external stakeholders often not knowing who in government to contact about specific policies.
Initiated by the Tech Policy Coordination Office, subject-specific **Policy Forums** provide regularised, non-transactional engagement between stakeholders in the tech-ecosystem.	**Regularised, non-transactional, non-adversarial knowledge sharing between government and external stakeholders in the tech-ecosystem** – the lack of which risks silos, trust deficits, and poor tech policy outcomes.
The **Expert Directory** connects government to individuals and is recognised as having expertise relevant to tech policy and regulation, both within Australia and internationally. The Tech Policy Coordination Office maintains it.	**Information and knowledge asymmetry between government and external stakeholders, and a lack of diversity in the experts engaged by government** – which limits options considered by government to address tech policy challenges.

2. Increase corporate responsibility for digital services defined in the Act, by:

a) continuing with preventative, risk-based obligations for industry

b) increasing the consequences of non-compliance, through transparency obligations, greater fines, a direct right to action for individual users, and international coordination on regulatory reform and enforcement

Q3: Should the Act have strengthened and enforceable BOSE?

Q21: Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?

The Basic Online Safety Expectations (BOSE) include the expectation that service providers 'take reasonable steps to proactively minimise the extent to which material or activity on the service is unlawful or harmful'. However, the BOSE are not enforceable and are instead designed to operate as a name-and-shame transparency mechanism.

The Online Safety Codes and Standards require that industry participants take proactive steps to create and maintain a safe online environment. These Codes are focused on specific content that would be Refused Classification (Class 1) or Restricted as age-inappropriate (Class 2) in accordance with the Australian Classification Scheme. Services are required to conduct a risk assessment, but this assessment is primarily used to determine what set of obligations they are subject to under the Code.

Australia's complaints-based content schemes remain an important safety net that empowers individuals to seek removal of harmful cyber bullying, adult cyber abuse and image-based abuse content. While this scheme is world leading in its harm minimisation for individuals, it addresses harms after they have been dealt, rather than reducing or preventing the harm at a systemic level before it occurs.

The obligation should sit with digital services to anticipate and prevent risks to their Australian users

There is a trend in international jurisdictions away from content-focused regulation towards systemic, ex-ante, risk-based regulation, as seen in the Duty of Care model adopted in UK's *Online Safety Act*. Risk assessments under the existing Australian Online Safety Codes are designed to categorise services into pre-determined obligation categories, not to inform the design of each services' own bespoke risk mitigation strategies, as in the European and UK models.

Any reforms should maintain a shift of responsibility onto services to identify, communicate about and mitigate risks to users, to:

- incentivise services to invest in safety innovations
- future proof the legislation (where amendments are not required to identify emerging user harms as new technical features introduced)
- shift from a content-category approach focused on harm minimisation to a systemic approach focused on harm prevention
- avoid incentivising over moderation by services to avoid content-specific fines

b) Increasing consequences, through transparency obligations, greater fines, a direct right to action for individual users, and international coordination on regulatory reform and enforcement

The consequences for failing to protect Australian users online has to date been insufficient to motivate meaningful change in service provider behaviour. To address this, Australia should consider transparency measures, greater financial penalties, direct right of action for individuals harmed, and global coalitions.

Transparency is an important element of creating accountability for services

Q23: is the current level of transparency around decision-making by industry and the Commissioner appropriate? If not, what improvements are needed?

Q16: What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?

The Basic Online Safety Expectations create a mechanism by which the eSafety Commissioner can request transparency reporting from social media, designated internet services, and relevant electronic services. However, the arrangement is designed to be ‘by exception’ with conditions to be satisfied regarding whether or not the service has contravened the Act or raised other specific concerns in the eyes of the regulator.

The Australian Government should establish a general obligation for annual transparency reporting by the largest services used by Australians. Requiring online services to be more transparent about their policies, enforcement decisions, and the trends on their platforms achieves several benefits:

- Research: helps to create an important evidence base for researchers to identify trends in online harms and user experiences across platforms.
- Accountability: creates a means of accountability between services’ stated policies and actions, enabling regulators, advertisers and users to hold services to account.
- Empowering users: to help users make informed choices about what services they want to use.
- Building trust: users can gain a better understanding of what content is being moderated and how (noting for some users, over enforcement and moderation is a point of concern, whereas others are concerned by a lack of the same).

Increase the financial consequences

Q18: Are Australia’s penalties adequate and if not what forms should they take?

Status quo structural incentives are not sufficient to drive meaningful corporate investment in safety research and development. The Government should explore adjusting the financial considerations behind these trade-offs to shift incentives:

Transparency to mobilise advertisers: enhanced transparency measures discussed above would draw a greater connection between responsible online safety and the revenue flow from advertisers looking to be associated with that service. Meaningful transparency will equip advertisers to make informed choices about where they invest their ad spend. This creates competition between services for a good online safety record and incentivises investment by services in safety and innovation.

From the regulator: the size of Australia's fines for non-compliance with the Act are out of step with other comparable jurisdictions. The Government should increase the quantum of its online safety fines to reflect the global standard, in proportionate terms (noting the other markets' size and contexts). The penalties should still reflect a graduated severity based on content type i.e. a higher fine for Class 1 content compared to cyber bullying.

Enforcing companies' terms of service

Q6: To what extent should online safety be managed through a service provider's terms of use?

Australia's online safety regime makes several references to services' terms of service: in the Basic Online Safety Expectations and in the Online Safety Codes and Standards.

Beyond complying with the obligations of the Online Safety Act, service providers should be held accountable for following through on their commitment to users in their terms of service.

In the US, a bipartisan coalition of 33 attorneys general filed a lawsuit against Meta alleging the company was knowingly deploying features on Facebook and Instagram that were harmful to young users. Notably, the case rests on allegation of *deceiving* consumers, rather than breaching a particular obligation to them. This is an interesting case study in the relationship between corporate commitments to users and obligations to deliver.

Australian users should be able to trust that if they engage with a service provider, its terms of service are going to be upheld. This also creates an opportunity for services to differentiate themselves based on their community guidelines, which will carry more significance.

Empowering individuals with a direct right of action

As the regulator, the eSafety Commissioner has a central role to play in enforcing obligations by imposing consequences on services that fail to meet their obligations to users. This should remain the case. However, this review presents an opportunity to also empower individuals with a direct right of action against services for violations of the Act. This would increase the agency of the individuals harmed, by providing an additional avenue for redress. It would broaden the source of consequences for services that fail to meet their obligations under the Act.

Adopting a direct right of action would be consistent with the Government's agreement-in-principle to explore a direct right to action on privacy violations as part of the reform of the Privacy Act.

Seek global interoperability and international coalitions to drive compliance

Q19: What more could be done to enforce action against service providers who do not comply, especially those based overseas?

Due to Australia's comparatively small population and market size, the Government should embrace international interoperability and coordination as an important means by which to facilitate corporate compliance. As demonstrated by uncertainty whether Meta will pull news services from Australia rather than participate in further Media Bargaining Code negotiations, Australia needs to regulate online safety in the knowledge that large multinational corporations will not necessarily choose to continue conducting business in Australia on terms they consider to negate the value of the commercial opportunity.

Working together in a coalition of international partners that have similar regulations, penalties and enforcement measures can increase the chances of compliance. Australia should reform and legislate in accordance with the needs and conventions of our jurisdiction. However, wherever possible, seeking out opportunities to harmonise and embed interoperability with existing international approaches and language from other major jurisdictions such as the EU and the UK will greatly increase the chances of compliance by global companies. Where Australia is looking to establish new approaches not reflected in existing models, the Government should seek to establish a coalition of other countries interested in pursuing similar reforms to expand the market weight beyond the direction of reform.

Aligning and coordinating approaches to online safety with comparable international peers can enable:

- Greater sharing of best practice policy related to online safety.
- Regulatory coherence across jurisdictions can make compliance easier for businesses as there is an overarching framework for regulation.
- Working with other jurisdictions can form a coalition of expectation, which will increase Australia's ability to enforce penalties as there are more people to leverage businesses.

3. Strengthen democratic protections underpinning the Act to ensure Australia maintains its status as a world leader in online safety by:

a) enhancing the checks and balances, appeals processes, and oversight of the eSafety Commissioner's powers

Q23: is the current level of transparency around decision-making by industry and the Commissioner appropriate? If not, what improvements are needed?

The eSafety Commissioner possesses significant powers over Australians' use of the internet. As online content takedowns can interact with freedom of speech implications, there needs to be appropriate checks on these powers to ensure that democratic practices are also being protected within the legislation. These include:

- The ability for users to contest or appeal decisions made by the Commissioner
- Transparency reporting obligations that reflect those expected of industry and Australian society

The inquiry could conduct an audit of checks and balances on other statutory positions that exercise powers of equivalent gravity, in Australia and in likeminded jurisdictions. A streamlined and more transparent version of the oversight provided by the Inspector General of Intelligence over the Australian Intelligence Community could also be instructive.

Regardless of the integrity with which the Commissioner has discharged their powers to date, it is essential that greater transparency, appeals and oversight mechanisms are put in place to future proof the democratic exercise of the powers in accordance with Australian law.

Not extending investigative Powers

Q17: Does the Act need stronger investigation, information gathering and enforcement powers?

We do not recommend expanding the Commissioner's existing investigative powers.

The eSafety Commissioner has robust powers to obtain identity information and contact details of users from service providers through the existing investigative powers in the Act. Creating more investigative powers would force providers to collect more information about users – such as telephone and financial information. This poses a range of privacy and security concerns that are not necessarily proportionate. Prosecuting or investigating criminal activity online is in the remit of other enforcement agencies in government, and greater investigative powers should remain within those agencies.

b) Obligate the eSafety Commissioner to conduct international advocacy with an awareness of the potential harm of online safety regulations in non-democratic contexts

Importance of responsible international advocacy for online safety

Q1: Are the current objects of the Act to improve and promote online safety for Australians sufficient or should they be expanded?

Q26: Are additional safeguards needed to ensure the Act upholds fundamental human rights and supporting principles?

Australia is a world leader in online safety and has done important work in coordinating and supporting the establishment of similar reforms and regulators around the world. The growing membership of the Global Network of Online Safety Regulators is testament to the Commissioner's ongoing international advocacy work.

Being proactive participant in a coalition of likeminded international partners can be an extremely valuable and impactful approach to maintaining online safety given the internet's borderless nature.

However, Australia should also ensure that it advocates responsibly for online safety legislation around the world. Australia must be discerning and nuanced when it advocates for greater content and expression regulations online. Many countries in our region watch Australia – but many do not have equivalent maturity in democratic institutions and protections. Online safety reforms involve bestowing governments with greater power and intervention over online expression, behaviour, and fundamentally, freedom of speech. A jurisdiction's broader political system and governance context is an important consideration when advocating for greater online safety regulations.

Australia therefore has a responsibility to be discerning with where and how the Government advocates for such reforms. There must be caution and discernment, and a need to advocate for nuanced and considered approaches to adopting online safety laws is different governance systems. It also behoves us to enshrine checks and balances on the Commissioner's powers, as democratic protection for Australia citizens *and* a best practice example regionally.

Section 27 of the Act lays out the 'functions' of the Commissioner, including promoting online safety for Australians, educational initiatives, and to 'consult and cooperate with *other persons, organisations and governments* on online safety for Australians'. The review could consider amending these functions to acknowledge the importance of conducting international advocacy as part of a broader support for democratic governance in other jurisdictions.

The Tech Policy Design Centre's Tech Policy Atlas, a global repository of technology legislation and regulation, can be used as a tool for policy researchers to find and compare international tech policy approaches being taken around the world.