THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: CCW:BMsb070624

7 June 2024

Dr James Popple
Chief Executive Officer
Law Council of Australia
PO Box 5350
Braddon ACT 2612

By email: Natalie.Cooper@lawcouncil.au

Dear Dr Popple,

Statutory Review of the *Online Safety Act 2021* (Cth)

Thank you for the opportunity to contribute to the Law Council's submission to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts' Statutory Review of the *Online Safety Act 2021* (Cth) (**Act**). The Law Society's Privacy and Data Law, Children's Legal Issues and Public Law Committees have contributed to this submission.

The Law Society is pleased that the statutory review of the Act has been brought forward, considering the pace of technological change and the fact that several likeminded jurisdictions have recently implemented regulatory schemes to combat online harms. We have addressed some of the general themes arising from the Issues Paper below.

Consistency of approach

As recognised in the Issues Paper, the Government is currently working on a number of significant initiatives that impact the regulation of digital spaces. In this context, we particularly note the Privacy Act Review, where the Government agreed, or agreed in principle, to recommendations seeking to address the vulnerability of children to online harm.[1] As was stated in the Government Response to the Review:

> The Privacy Act is one piece of legislation in a broader digital and data regulatory framework… In order to reduce complexity and compliance costs, the Privacy Act should provide a baseline set of protections that are interoperable with other frameworks that deal with the handling of personal information.[2]

For the purposes of clarity and consistency of approach, it will be important that initiatives arising from that Review are considered in tandem with, and can reinforce, any reforms to the Act. For example, the development of a Children's Online Privacy Code, which focuses on the design of online services in the best interests of the child, necessarily intersects with changes

[1] Australian Government, Government response to the Privacy Act Review Report (**Privacy Act Review Response**), 13-14.
[2] Ibid., 16.

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000
ACN 000 000 699 ABN 98 696 304 966
lawsociety.com.au

T +61 2 9926 0333 F +61 2 9231 5809
E lawsociety@lawsociety.com.au

Law Council OF AUSTRALIA
CONSTITUENT BODY

to the online safety regime, including the introduction of any duties placed on online services to design for safety and monitor the content published on their platforms.[3]

We also draw attention to the consideration being given to the development of a statutory tort of serious invasion of privacy. The statutory tort is intended to 'provide people with the ability to seek redress through the courts for serious invasions of privacy without being limited by the scope of the [Privacy] Act'.[4] The proposal is 'agreed in principle' by the Government and supported by the Law Council.[5] It will be important that consideration of provisions under the Act, particularly relating to harms and their impacts, is complementary to and harmonised with the measures under the *Privacy Act 1988* once reformed, acknowledging that many of the harms under the Act are likely to involve 'personal information', as defined under the *Privacy Act 1988*.

Similarly, work that is being undertaken on new challenges arising from generative artificial intelligence (**Gen AI**) for online safety should be addressed with a coordinated, cross-government perspective. As noted in the Government's interim response to the Safe and Responsible AI in Australia consultation, 'existing laws likely do not adequately prevent AI-facilitated harms before they occur, and more work is needed to ensure there is an adequate response to harms after they occur'.[6] These harms necessarily intersect with issues of online safety, including discussions around mandatory safety guardrails for Gen AI in high-risk settings, and should be considered together.

We note that the majority of online service providers to which the Act applies operate internationally. Consideration and comparison of online safety legislation in international jurisdictions, for example the existence of a duty of care on platforms, and the potential extraterritorial application of online safety legislation,[7] will be important for ensuring consistency in approach to management of both online risks and enforcement mechanisms.

Balancing innovation, privacy, security and safety

We recognise the need for online service providers to retain the ability to innovate. However, the current harms being experienced online, particularly by children and vulnerable adults, mean innovation must be balanced with privacy, security and safety.

Online platforms hold large amounts of personal information about their users. Much of this information may have been obtained without proper consent. It is very difficult, if not impossible, for individual users to withdraw consent, change user settings, and/or prevent harmful content being fed to them through algorithms over which the individual has little to no control.

We anticipate that implementation of the urgently needed reforms to the *Privacy Act 1988* will assist, noting the Government has agreed in principle that consent must be voluntary,

---

[3] Ibid.
[4] Ibid., 19.
[5] Ibid., 36. See also Law Council, Law Council supports statutory tort for serious invasion of privacy (Media Release, 8 February 2022).
[6] Australian Government, Safe and Responsible AI in Australia Consultation – Australian Government's Interim Response, 5.
[7] By way of example, we note that the *Privacy Act 1988* was amended in 2022 to allow for enforcement of penalties on an overseas entity conducting business related activities in Australia (ss 5A and 5B, *Privacy Act 1988*). We understand that the "Australian link" described in terms of ss 5B(2) and (3) of the *Privacy Act 1988* was contentious when the *Privacy Act 1988* was amended in 2022. Nevertheless, we suggest that, in a globalised environment, effective enforcement of the Act requires consideration of practicable provisions for the Act's extraterritorial application to protect Australians from defined classes of online harms.

informed, current, specific and unambiguous. It has also agreed the Act should allow individuals to withdraw consent in an easily accessible manner.[8] As noted above, it is therefore essential that there is a clear and consistent approach to this review of the Act and the reforms to the *Privacy Act 1988*.

Objectives of the Act

The objects of the Act are to improve and promote online safety for Australians. Consistent with our views set out below as regards the desirability of introducing an enforceable duty of care on digital platforms (**platforms**), we consider that the objects of the Act should be expanded to explicitly reference the goals of identifying, mitigating and managing risks of harm. As set out in the 2022 report of the House of Representatives Select Committee on Social Media and Online Safety:

> The time has come to fundamentally shift the burden of responsibility regarding ensuring online safety. For too long, the onus of maintaining online safety has been on the most vulnerable users, including children and their parents. This is unacceptable and unsustainable in an environment where users like children are exposed to the most risk online and suffer extreme forms of harm as a result.[9]

Expanding the objectives to include harm prevention and mitigation would need to be accompanied by legislative changes and regulatory settings. This would mean that a systemic focus on mitigating harm is introduced, over and above the current 'content-focused' approaches, whereby certain material is subject to mandatory and enforceable take-down notices.

Duty of care

The Law Society supports the introduction of a new duty of care on platforms. In our view, the current legislation is too heavily weighted towards a 'notice and take down' approach, which is reactive and unsuited to a digital environment. However, the introduction of a duty of care should not replace the current complaints mechanism under the Act, but rather supplement it.

Under the Act, the Basic Online Safety Expectations require the platform to take reasonable steps to ensure that end-users are able to use the service in a safe manner.[10] However, as noted in the Issues Paper, this does not create a legally enforceable duty.

A recent paper by Reset Australia described the focus on discrete pieces of content as leading to a regulatory 'whack-a-mole' which fails to address systemic risk.[11] It outlines five key elements of a 'comprehensive and enforceable regulatory framework' as follows: (1) Introduction of an overarching duty of care on the platform; (2) Requirements for platforms to assess all their systems and elements for serious risks they may pose; (3) Requirements for risk mitigation measures; (4) An effective framework for public transparency; and (5) Strong enforcement powers.[12]

---

[8] Privacy Act Review Response (above n 1) 15.
[9] House of Representatives Select Committee on Social Media and Online Safety, Social Media and Online Safety, (March 2022), [5.78].
[10] We note the changes to the Basic Online Safety Expectations have been made through the through the *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024* (Cth) which commenced on 31 May 2024.
While these address the emerging online safety issues to some extent (by outlining minimum safety expectations for online service providers) their enforcement is limited.
[11] Reset Australia, A duty of care in Australia's *Online Safety Act* (April 2024) 5.
[12] Ibid., 6.

On balance, we consider that the introduction of an overarching duty is preferable to the introduction of multiple duties, as under the *Online Safety Act 2023* (UK). That legislation imposes multiple duties of care on providers of regulated user-to-user and search services, depending on the type of content involved, for example illegal content and content that is likely to be accessed by children. While there are advantages in the nuance of this regime, which 'calibrates duties to match particular harms', we agree with the arguments put forward by Reset Australia that this approach introduces regulatory complexity.[13] Further, a truly systemic approach starts from the system level, with pro-active risk identification at the time of building the system (i.e. safety by design), rather than an assessment of risk that is focused on content after the system has been set up.[14]

Removal Notices

Under the Act, the recipient of a removal notice must remove or take all reasonable steps to remove the relevant material, or take reasonable steps to cease the hosting of the material within 24 hours (or longer as specified by the Commissioner).[15]

The impact of a removal notice is diluted if the platforms can subjectively determine their own reasonable steps, and the Act could be strengthened by defining the 'reasonable steps' requirement. Further, from the perspective of administrative fairness, we consider that if the perceived issue or threat is likely to be time limited, any takedown direction should be able to be reviewed by the Commissioner to mitigate the risk of encroaching on legitimate free speech and/or the implied freedom of political communication.

Penalties

The penalty provisions in the Act (including failure to comply with content removal and blocking notices, industry codes/standards, reporting notices, Basic Online Safety Expectations) attract penalties of up to 500 penalty units ($782,500 for corporations).

We agree with the concerns that have been raised as to the adequacy of these penalties in light of the size, power and resources of platforms, as well as the level of penalties that can be imposed by international online regulators and other Australian regulators for contraventions under the Australian Consumer Law (**ACL**), *Privacy Act 1988* and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

We consider that the better approach is that the Act closely mirror the level of penalties imposed by the ACL, *Privacy Act 1988* and the *Online Safety Act 2023* (UK), whereby the maximum amount of the penalty for which an entity is liable is whichever is the greater of £18 million (approx. AUD35 million) or 10% of the entity's qualifying worldwide revenue. The concept of penalties that are arrived at by way of calculation of global turnover is not unfamiliar to Australian legislation.[16]

Some concerns have been expressed that the introduction of substantial penalties, both civil and criminal, could create an incentive for platforms to 'err on the side of overmoderating the

[13] Ibid., 8.
[14] Ibid.
[15] See *Online Safety Act 2021*, s 79.
[16] See, for example, amendments introduced in 2022 to the *Competition and Consumer Act 2010* (Cth) where the maximum penalty for companies was raised to $50 million; three times the value of the benefit obtained; or 30% of the company's adjusted turnover during the breach turnover period for the offence.

online environment'.[17] This potential impact on freedom of speech may be exacerbated by the fact that automated systems used to detect harm may not have the level of sophistication to distinguish illegal and harmful material from that which might be described as political satire, dissent etc.[18] In our view, there is therefore good sense in the proposal to ensure penalties under the Act can be imposed in a nuanced and proportionate way to respond to the harm posed (the example in the Issues Paper compares the situation of failing to take down illegal material such as child sexual abuse or pro-terror material with failure to take down other harmful, but not unlawful, material such as cyberbullying and cyber-abuse material.)

The importance of tech-neutrality

A tech-neutral approach is one where the legislation focuses on outcomes, rather than the specific technologies used to reach those outcomes. We regard this approach as central for any legislative regime that is to remain relevant in light of the rapid pace of technological advancement and the evolution of harms that may be posed to children and other vulnerable people as a result.

Our position would not be impacted by the introduction of a statutory duty or Safety by Design obligations (both of which we believe are important).

Adequate funding for the eSafety Commissioner

It is important to note that if the regulatory purview, tools and powers available to the Commissioner are increased, there will need to be a commensurate increase in funding for the Office of the eSafety Commissioner to undertake this additional work, as well as to implement other measures to drive systemic change.

Thank you for the opportunity to comment. Please contact Sophie Bathurst, Policy Lawyer, on Sophie.Bathurst@lawsociety.com.au or (02) 9926 0285 in the first instance if you have any queries.

Yours sincerely,

Brett McGrath
President

[17] Centre for Strategic and International Studies, A New Chapter in Content Moderation: Unpacking the UK Online Safety Billl (18 October 2023).
[18] Ibid.