THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL/BLC:JBml150925

15 September 2025

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,

PRODUCTIVITY COMMISSION INTERIM REPORT: HARNESSING DATA AND DIGITAL TECHNOLOGY

Thank you for the opportunity to contribute to the Law Council of Australia's submission in response to the Productivity Commission's Interim Report, *Harnessing data and digital technology* (**Interim Report**). The Law Society's Privacy and Data Law Committee and Business Law Committee contributed to this submission.

General comments

Our submission focuses on three issues: a regulatory regime for the use of artificial intelligence (**AI**); balancing the rights of copyright owners under the *Copyright Act 1968* (Cth) (**Copyright Act**) with AI developers' desire to use copyrighted works in training AI models; and the Productivity Commission (**PC**)'s recommendation to amend the *Privacy Act 1988* (Cth) (**Privacy Act**) to create an alternative outcomes-based compliance pathway for privacy.

We are concerned that the PC's recommendations may create a greater regulatory and compliance burden, especially at a time when multiple reforms on a range of issues will be coming into effect. Businesses, especially small business with limited resources, need to process legislative changes and adapt to an altered regulatory environment.

Any new additions to the regulatory burden should be the result of a clearly articulated and evidenced need, and not duplicative or overlapping with existing laws. We also consider that the PC recommendation 3.1 of creating an alternative for pathway for compliance with privacy laws may undermine the effectiveness of recent Privacy Act review and reforms, potentially creating confusion and additional compliance costs.

Enable AI's productivity potential

Draft recommendation 1.1: Productivity growth from AI will be built on existing legal foundations. Gap analyses of current rules need to be expanded and completed.

Draft recommendation 1.2: AI-specific regulation should be a last resort.

We support using the existing regulatory framework to regulate AI, rather than implementing AI-specific legislation. We also support the recommended gap analysis process, with solutions to identified gaps being framed in technology-neutral terms. We agree that AI-specific regulation should be considered as a last resort.

If additional new regulations or amendments to the existing regulatory framework are required, they should minimise the compliance and regulatory cost for intellectual property (**IP**) holders and AI developers, especially for small businesses and individuals. They should also be clear and concise, without duplication and overlap with existing laws or obligations. In parallel with the analysis of regulatory gaps, we recommend that an overlap analysis be conducted so that duplication of regulation is identified and minimised. For example, the requirement under the Privacy Act for transparency in automated decisions may already cover information on AI inputs and therefore additional regulation may not be necessary.[1] It is equally necessary that there are clear lines of responsibility for each regulator charged with overseeing parts of the regulatory framework.

It is important to distinguish between AI use and AI technology when considering regulation. It is AI use, rather than AI technology, that should be regulated using an adaptable set of principles for AI use. Often, AI use/deployment is specific to particular industries and organisations. For example, an AI application which is trained to identify early signs of carcinogenic melanomas will use different data sets for training to an AI model which automates routine data entry and document management, but the same set of principles-based regulation is applicable in both contexts. We consider that the regulation of AI should be flexible enough to operate in differing contexts, while providing a uniform minimum standard for industries, to enhance consistency and certainty in this period of change and transition.

In addition, we suggest that regulatory staff must be appropriately upskilled in order to be in the position to appropriately assess, balance and regulate risks and benefits associated with deploying AI.

We acknowledge the PC's position that it may not be preferable to regulate AI too quickly before all gap analyses are complete. We also acknowledge that there is a need to balance the protection of individual rights through regulation with innovation and investment into AI. To contribute to that balance, we suggest that the main principles when deploying AI should be determined by the Government, which will assist industries to establish and follow a shared set of community values regarding the use of AI. This includes not ruling out the possibility of prohibiting certain high-risk AI use cases.

[1] Under the *Privacy and Other Legislation Amendment Act 2024* (Cth), amendments to the *Privacy Act 1988* (Cth) will take effect on 10 December 2026, introducing new transparency obligations for entities engaging in automated decision-making. Australian Privacy Principles (APPs) 1.7 and 1.8 require that any APP entity using a computer program to make decisions that significantly affect an individual's rights or interests—and where personal information is used in that process—must disclose this in its privacy policy. Specifically, APP 1.8 mandates that the policy details the kinds of personal information used (for example; name, email, credit score), the kinds of decisions made solely by automated systems (for example; loan approvals, insurance premium calculations, eligibility determinations for government services, or algorithmic pre-screening of job applications), and decisions where automation plays a substantial role but is later reviewed by a human (for example; automated fraud detection flags or health diagnostics support tools). These provisions are to enhance transparency and accountability in the use of AI and algorithmic systems. failure to comply may result in enforcement action by the Office of the Australian Information Commissioner (OAIC), including civil penalties.

As noted in our submission to Department of Industry, Science and Resources' Proposal Paper for introducing mandatory guardrails for AI in high-risk settings,[2] we consider there is merit in banning AI practices that have an unacceptable level of risk, that is, where the risk cannot be mitigated, or the consequences of the practice pose unacceptable and irremediable harm to individuals and communities. To balance this with not stifling innovation in AI, any ban of AI practices could potentially be implemented by way of subordinate legislation, to allow sufficient flexibility while AI continues to evolve. We suggest any ban contain sufficient certainty in the definition and interpretation of the prohibited practice, and clarity about why the risk is unacceptable.

It may be instructive to refer to the AI practices that are prohibited under the European Union's *Artificial Intelligence Act* (**EU AI Act**), for their incompatibility with individual and collective rights and fundamental values, such as the rule of law.

AI practices prohibited under Article 5 of the EU AI Act include:[3]

(a) Subliminal techniques which can materially distort a person's behaviour by impairing their ability to make an informed decision in a way that causes, or is reasonably likely to cause, them significant harm.

(b) Exploiting the vulnerabilities of a person or specific groups of people (for example, due to their age, disability or economic situation) which can materially distort their behaviour in a way that causes, or is reasonably likely to cause, them significant harm.

(c) Social scoring systems based on known, inferred, or predicted personality characteristics which causes detrimental or unfavourable treatment that is disproportionate, or used in a context unrelated to the context in which the data was originally collected.

(d) Risk assessment systems which assess the risk of a person to commit a crime or re-offend (except in support of a human assessment based on verifiable facts).

(e) Indiscriminate or untargeted web-scraping for the purposes of creating or enhancing facial recognition databases.

(f) Emotion recognition systems in the workplace or educational institutions (except for medical or safety reasons).

(g) Biometric categorisation systems used to infer characteristics, such as race, political opinions or religion.

(h) Real-time, remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement except (subject to safeguards and within narrow exclusions) searching for victims of abduction, preservation of life, and finding suspects of certain criminal activities. Real time means live or near-live material, to avoid short recording delays circumventing the prohibition.

[2] Law Society of NSW, Mandatory guardrails for AI in high-risk settings (2024).
[3] Thomson Reuters UK, Practice Note: EU AI Act, https://uk.practicallaw.thomsonreuters.com/w-042-3394?transitionType=Default&contextData=(sc.Default)

Information request 1.1 Copyright and AI

Copyrighted materials being used to train AI models: Are reforms to the copyright regime (including licensing arrangements) required? If so, what are they and why?

In our view, Australia's existing copyright regime does not require substantive amendments to regulate use of copyrighted works in training AI models. There may be regulatory gaps or a need for a refined licencing process, but we suggest these can be incorporated effectively within the existing statutory framework. Copyright laws have responded to previous changes in technology, and there is no need to remove established rights and principles.

Proposal to amend the *Copyright Act 1968* (Cth) to include a fair dealing exception for text and data mining:

- **How would an exception covering text and data mining affect the development and use of AI in Australia? What are the costs, benefits and risks of a text and data mining exception likely to be?**
- **How should the exception be implemented in the Copyright Act – for example, should it be through a broad text and data mining exception or one that covers non-commercial uses only?**
- **Is there a need for legislative criteria or regulatory guidance to help provide clarity about what types of uses are fair?**

We do not support a fair dealing exception covering text and data mining for the development and use of AI in Australia. In addition, we do not support a broad text and data mining exception, whether it is for non-commercial use or otherwise.

We note that the PC compares Australia's fair dealing exemption regime to the United States 'fair use' doctrine.[4] In our view, the introduction of a 'fair use' doctrine in Australia could erode copyright holders' protections and create uncertainty for IP holders and AI developers. In the US, there are differing views on the extent that the 'fair use' doctrine applies when training AI models. The extent of reliance on the fair use doctrine is far from settled, see: *Thomson Reuters Enterprise v Ross Intelligence Inc* 11 February 2025 No1:20-cv-613-SB;[5] *Bartz v. Anthropic PBC,* No. 24-cv-05417 (N.D. Cal. June 23, 2025).[6] Given this, in our view, there should be no adoption of a US-style fair use doctrine in Australian copyright laws.

In our view, barriers to entry to the AI market are inherent for later deployers of AI, because of the early 'land grab' by big AI deployers already. The US has less protected datasets than Australia. We suggest that the PC provides more evidence of the actual risks or barriers of copyright or privacy to AI innovation in Australia to enable a more informed understanding of the current barriers to tailoring AI content to the Australian context.

[4] Productivity Commission, *Harnessing data and digital technology* (2025) 26: https://www.pc.gov.au/inquiries/current/data-digital/interim/data-digital-interim.pdf.
[5] https://www.ded.uscourts.gov/sites/ded/files/opinions/20-613_5.pdf.
[6] https://www.govinfo.gov/app/details/USCOURTS-cand-3_24-cv-05417.

Instead, we support the alternative option of increased licensing of works for the training of AI. As noted by the PC by quoting the Copyright Agency's submission, licenses for data use in training AI models is increasingly prevalent.[7] An international example includes the New England Journal of Medicine (**NEJM**) entering into an agreement with Open Evidence in February 2025 to allow it to integrate 30 years of NEJM content into its AI models for clinical use.[8] Most other academic publishers, news and book publishers and media groups have licensed their works to AI developers. In the US, the Copyright Clearance Center now enables publishers to include AI training in their licensing arrangements (usually for internal use).[9]

In our view, there is no reason why the existing licensing system, which is an established framework that has worked well and adapted from print to digital and capable of adapting to other changes, cannot be used for licencing copyrighted works for AI training. In Australia, existing copyright licensing and collection agencies such as Australasian Performing Right Association Limited, Australasian Mechanical Copyright Owners Society, and the Phonographic Performance Company of Australia, act on behalf to copyright holders to ensure that they are compensated for the use of their works. Users can obtain a licence to use of the works across various platforms. Blanket licenses are available to enable businesses and organisations to use works from the agencies' catalogue without negotiating individual agreements. In our view, this system could be readily adapted for use in the context of AI. Licencing also provides an avenue for lawful access to works, rather than AI developers using 'shadow libraries' of pirated works, which is an increasing problem in the United States.[10]

Supporting safe data access and use through outcomes-based privacy regulation

Draft recommendation 3.1: An alternative compliance pathway for privacy.

The Australian Government should amend the *Privacy Act 1988* (Cth) to provide an alternative compliance pathway that enables regulated entities to fulfil their privacy obligations by meeting criteria that are targeted at outcomes, rather than controls-based rules.

In our view, this recommendation appears to characterise privacy as an economic hindrance rather than emphasising the economic advantages that stem from protecting personal information. We are concerned that there has been insufficient reference to the significant evidence and research contained in the Privacy Act Review,[11] which undertook comprehensive analysis of many key issues of privacy regulation (including the impact on small businesses) and carefully considered the opinions of both businesses and individuals.

[7] Productivity Commission, *Harnessing data and digital technology* (2025) 25.
[8] Open Evidence Australia, 'OpenEvidence and NEJM Group, publisher of the New England Journal of Medicine, sign content agreement' (19 February 2025): https://www.openevidence.com/announcements/openevidence-and-nejm.
[9] Copyright Clearance Center, Press Release, 'CCC Announces AI Systems Training License for the External Use of Copyrighted Works Coming Soon' (4 March 2025): https://www.copyright.com/media-press-releases/ccc-announces-ai-systems-training-license-for-the-external-use-of-copyrighted-works-coming-soon/.
[10] See: Forbes Australia, 'Anthropic will pay $1.5 billion to settle copyright lawsuit from book authors' (8 September 2025): https://www.forbes.com.au/news/innovation/anthropic-will-pay-1-5-billion-to-settle-copyright-lawsuit-from-book-authors/.
[11] Attorney-General's Department, *Privacy Act Review Report* (2022): https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.

We contend that it is only with effective privacy regulation that individuals have the confidence to share personal information with organisations. Protecting data builds trust and encourages stronger participation in our digital economy, which will contribute to productivity. In our view, there will be a cost to national productivity if individuals are not confident to share information with others, given the basis of effective data flow is an individual's consent to having their personal information collected in the first place. We have already witnessed how data breaches threaten to erode trust in the digital environment.

While we acknowledge that other privacy models deserve further consideration, and an outcomes-based regime has positive aspects, we query what the spectrum of outcomes of this alternative compliance pathway is intended to be. Privacy law in Australia is already difficult to navigate for many businesses, and the recommendations in this Interim Report might further delay 'tranche 2' privacy reforms. To have a dual track is likely to be confusing, and potentially increase compliance costs, particularly for small businesses – both those already captured by the Privacy Act (e.g. small health practices) and other small businesses brought under the Privacy Act in future reforms.

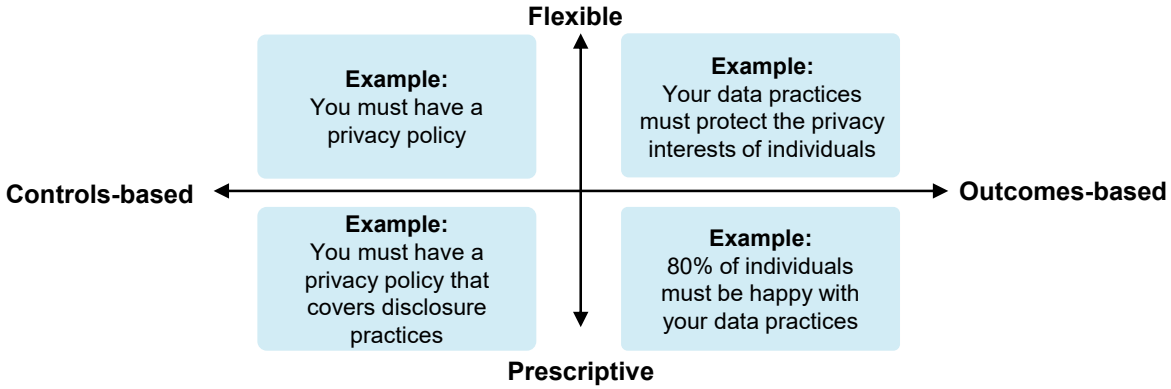
We suggest it would assist for the PC to provide practical examples of how the alternate outcomes-based models would operate, along with a comparison of the results – including the difference in compliance costs, with the application of the current law.

In addition, privacy law is closely intertwined with cybersecurity legislation, often resulting in areas of overlap. Organisations must comply with the notifiable data breach scheme outlined in the Privacy Act, and some organisations must also comply with the notification requirements under the *Security of Critical Infrastructure Act 2018* (Cth) and ransomware reporting obligations mandated by the *Cyber Security Act 2024* (Cth). We suggest that any proposed changes to privacy frameworks should be evaluated with consideration of these regulatory intersections, with an aim to harmonise legal requirements and support organisational compliance.

We also suggest that an outcomes-based approach should align with human rights. The PC's recommendation appears to emphasise the impact of the privacy regime on large corporations, which, given the productivity focus, is appropriate. However, privacy must be considered more broadly, and balance in regulatory approach is required, with appropriate consideration of impacts on a range of actors, from individuals, very small not-for-profits, to large charities and corporations. We reiterate that strong privacy protections will encourage stronger participation in our digital economy, which will contribute to productivity.

We note Box 3.4 of the Interim Report taxonomises regulation based on the criteria of flexible vs prescriptive, outcomes-based vs controls-based. If the criteria were applied to the Australian Privacy Principles (**APPs**), the APPs would be scattered across the quadrants based on their characteristics. APPs such as APPs 1.3, 1.4, and 5[12] will likely fall into the bottom left quadrant of 'prescriptive and controls-based', while APPs 1.2, 3.5, 6, 7.1, 10 and 11[13] will likely be characterised as outcomes-based. However, we query the practical utility of this taxonomic exercise, when, in our view, an effective system of balanced privacy regulation needs a mix of flexible and prescriptive, and of outcomes-based or controls-based requirements.

[12] https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles.
[13] Ibid.



Box 3.4 of the Interim Report[14]

Options for framing requirements for the alternative pathway

We acknowledge that the current notice and consent model for privacy is inadequate. In our view, there needs to be a greater emphasis on organisational accountability as an overlay to notice and consent requirements.

The Interim Report proposes three options: a best interest obligation, an obligation for regulated entities to have regard to the best interest of an individual, or a duty of care.[15] These options depart from the Privacy Act Review's recommendation of a 'fair and reasonable' test to be applied by entities in the collection, use and disclosure of personal information.[16]

In our view, it is not clear why a best interest obligation should be considered more certain and less onerous than the more objectively assessed test of reasonableness. We also suggest that a cost-benefit analysis of the 'best interests' track is necessary to provide evidence that the alternative pathway will lead to reduced compliance costs and burden. In our view, at a preliminary level, compliance costs associated with a 'best interests' model would include the cost categories of evaluating whether a particular practice is in the best interests of the affected individuals; documenting the outcome of the evaluation; as well as opportunity costs and the costs of maintaining data governance that would prevent data leakage.[17] It is not clear to us, without evidence, that a best interest obligation would lead to reduced compliance costs.

We suggest the PC considers the option of implementing a duty of care to require regulated entities to take steps to prevent reasonably foreseeable harm to an individual's privacy. This is consistent with the duty of care for digital platforms recommended by the independent statutory review of the *Online Safety Act 2021*

[14] Productivity Commission, *Harnessing data and digital technology* (2025) 56: https://www.pc.gov.au/inquiries/current/data-digital/interim/data-digital-interim.pdf.
[15] Ibid 61.
[16] Attorney-General's Department, *Privacy Act Review Report* (2022) 3: https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.
[17] Peter Leonard, 'Data privacy regulation under review: the Productivity Commission's "Pillar 3" interim report' (2025) 5.

(Cth).[18] The duty of care would shift the onus and responsibility onto regulated entities, consistent with the principle of organisational accountability.

If you have any queries about the items above, or would like further information, please contact Mimi Lee, Policy Lawyer, on 02 9926 0174 or mimi.lee@lawsociety.com.au.

Yours sincerely

Jennifer Ball

Jennifer Ball
President

[18] Delia Rickard PSM, *Report of the Statutory Review of the Online Safety Act 2021* (October 2024): https://www.infrastructure.gov.au/sites/default/files/documents/report-of-the-statutory-review-of-the-online-safety-act-2021-february-2025.pdf.