Australian Institute of Company Directors

18 Jamison Street,
Sydney NSW 2000

t: 1300 739 119
e: contact@aicd.com.au
aicd.com.au

ABN 11 008 484 197

28 February 2023

Senate Standing Committee on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Committee Secretary

Inquiry into the Influence of international digital platforms

Thank you for the opportunity to provide comments to the Senate Economics Legislation Committee (the **Committee**) inquiry into the Influence of international digital platforms (the **Inquiry**).

The Australian Institute of Company Directors' (**AICD**) mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. The AICD's membership of nearly 50,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits (**NFPs**), large and small businesses and the government sector.

The AICD welcomes the Inquiry as an opportunity to comprehensively assess the role and impact of international digital platforms (**Big Tech**) on the Australian economy and society.

The AICD's policy positions in this submission have been informed by consultation with AICD members, industry experts, industry bodies and representatives of Big Tech companies.

1. Executive Summary

The AICD recommends the Inquiry adopt a nuanced and balanced approach to assessing the dynamic, multi-faceted role of Big Tech and be cautious in making recommendations that may curtail innovation. This balance would reflect that Big Tech companies are key participants in the Australian economy through offering vital products and services that underpin an innovative global facing economy and separately make significant investments in digital infrastructure and employ highly skilled cyber and digital workers. However, we also recognise this should be weighed against the legitimate community and public policy concerns that exist with some Big Tech products and services.

We encourage the Inquiry to establish a clear evidence base for any recommendations proposing wholesale legislative and regulatory reforms, as well as consider the recommendations of parallel Government reviews being advanced in areas relevant to the Inquiry. The AICD has been concerned that recent legislative reforms focused on cyber security, privacy laws and data management as well as the digital economy have occurred in a truncated manner without a comprehensive understanding of the costs and benefits of change. This has often exacerbated complexity in these policy areas and contributed to a patchwork of existing regulatory obligations.

Our key points in this submission are as follows:

1. Cyber security governance is a key priority for Australian directors. Cyber risk management in the rapidly evolving threat landscape continues to prove challenging for organisations of all sizes,

particularly in light of the complex and fragmented regulatory obligations that apply to varying degrees across industries. There is an opportunity for Government to develop a genuine partnership with industry to drive a coordinated approach to building national cyber resilience. Big Tech companies have the potential to enhance this partnership model through their resourcing, knowledge and experience in combatting cyber risks at the global level;

2. Large scale data breaches in Australia have in recent months led to the strengthening of penalties that organisations may face for serious and repeated privacy breaches, while an extensive and ongoing review of the *Privacy Act 1988* (**Privacy Act Review**) has made significant recommendations for changes to Australia's privacy laws. It is critical that wholesale privacy law reforms are considered in detail, are subject to comprehensive consultation and a thorough analysis of the cost benefit trade-off of policy options;

3. The Australian Competition and Consumer Commission's (**ACCC**) Digital Platforms Inquiry is the appropriate avenue for the Government to assess the necessity for any changes to Australia's existing competition laws to address concerns about the degree of market power and vertical integration. Concern over Big Tech market power is not unique to Australia, and we caution against reforms that may lead to a bespoke competition framework that is internationally inconsistent and disadvantages Australia's access to Big Tech products and skills; and

4. It is unclear what concerns (if any) there are with the governance of Big Tech subsidiary companies in Australia, including any identified issues with directors of Australian subsidiaries failing to meet their fiduciary and statutory directors' duties and corporate responsibilities. Australia's long-established directors' duties framework sets out clear obligations on individual directors with respect to the entities they govern, including for subsidiaries of a foreign parent company. Should these duties not be met by directors of Big Tech Australian subsidiaries, this can be addressed through Australia's existing legislative framework and appropriate enforcement action by the Australian Securities and Investment Commission (**ASIC**).

2. Cyber security obligations

AICD members are highly engaged on the governance of cyber security and data protection and are motivated to build the cyber resilience of their organisations. Cyber-crime and data security is consistently cited as the number one issue keeping directors awake at night in the AICD's biannual Director Sentiment Index.[1]

To support AICD members in governing cyber risk we published the Cyber Security Governance Principles (the **Principles**) in partnership with the Cyber Security Cooperative Research Centre (**CSCRC**), in October 2022.[2] The Principles have filled an identified gap in practical guidance available to Australian directors of all sizes of organisations to effectively oversee and engage with management on this rapidly evolving risk. The Principles received the endorsement from the Minister for Home Affairs and Cyber Security both in an accompanying foreword. To date the Principles and the supporting resources have received over 15,000 unique downloads reflecting the appetite of directors to improve their knowledge of cyber security risk and build organisational-wide cyber resilience.

In developing the Principles, and through engagement on earlier Government reform proposals, AICD members have consistently expressed concern with the often-uncoordinated Government approach to

[1] AICD Director Sentiment Index, Second Half 2022, available here.
[2] AICD CSCRC Cyber Security Principles, October 2022, available here.

cyber security regulatory reforms. An example of this is the requirement for notification of cyber incidents and data breaches where, in addition to the Notifiable Data Breaches Scheme (**NDB Scheme**), there are separate Government reporting requirements that differ by industry and whether the organisation is subject to the *Security of Critical Infrastructure Act 2018* (**SOCI Act**). Senior directors have provided feedback that the complex, and fragmented regulatory landscape, is often a barrier to an organisation effectively responding to significant cyber incidents and ensuring appropriate communication channels exist with government.

A Government – industry partnership model

The success of the Principles reflects the opportunities that exist for industry to be a genuine partner with Government in driving a 'team Australia' agenda to build cyber resilience. The speed at which the cyber security threat landscape has been evolving, consistent with changes in technology and personal behaviour with digital products, makes a policy focus solely on strengthening the 'stick', or compliance elements of regulatory regimes, counterproductive.

A partnership between Government and industry would recognise the dynamic threat environment and the private sector, including Big Tech companies, will have the knowledge and expertise to contribute to combatting the threat. Informed by member feedback, our view is that a partnership model would have the following key components:

- greater coordination across relevant agencies on future cyber security reforms, including aligning the Privacy Act Review recommendations with other future regulatory proposals, such as the development of the Government's *Cyber Strategy 2023 - 2030*;
- clarity on regulator responsibilities when undertaking investigations and enforcement activity on cyber security and data breaches. Senior directors, who have experienced a significant cyber incident, have shared with the AICD their frustration at how overlapping and unclear regulator roles have impeded an effective and timely response by an organisation to a significant incident;
- a safe harbour or protected information mechanism where an organisation can share information of a significant cyber incident with a regulator(s) to assist in response and recovery without concern that the information will subsequently be used in enforcement action;
- consideration of how existing reporting and notification obligations (e.g. SOCI Act obligations, Notifiable Data Breaches Scheme) can be harmonised or streamlined with the goal that an organisation only needs to report or notify to the Government once;
- targeted support for SMEs and NFPs to build cyber security resilience and improve data management practices, education, information sharing and guidance in the event of experiencing and recovering from a cyber security incident;
- addressing urgent skills shortages in technology and cyber security specialties, including support via Australia's immigration programs; and
- proactive threat and intelligence sharing by key Government agencies (e.g. Australian Cyber Security Centre, Office of the Australian Information Commissioner) with industry.

The AICD urges the Inquiry to consider how a partnership model, of the type outlined above, represents a an opportunity for a coordinated and collaborative approach to building national cyber resilience rather than a narrow focus on finding opportunities to impose new regulatory obligations.

3. Data governance and privacy laws

This section responds to the data and privacy section of the Issues Paper.

The Issues Paper raises a number of questions about how to strengthen the protection of personal information of Australians, including options for individuals to pursue compensation for privacy breaches. As noted in the Issues Paper, there have been a number of significant data breaches in Australia in the past year resulting from malicious cyber security attacks.

The AICD recognises the significant public concern with recent large scale data breaches and the impact it has had on affected individuals and appreciate the momentum this has provided for regulatory reform. However, we are concerned that reactive policy making in this area could hamper a more considered response to legitimate public concerns.

By way of example, amendments to the penalty provisions of the Privacy Act passed by Parliament in November 2022 were subject to very limited consultation (specifically, a brief Senate inquiry). Despite widespread industry concern, including from the AICD, with the drafting and the incentive structures that the provisions would create, they were passed without amendment.[3] This is a salient example of how policy-making in cyber and privacy policy areas can proceed with such speed that there is little time to appropriately assess the potential for unintended consequences and understand the costs and benefits of changes.

While recognising that there is room to strengthen the regulatory framework, we strongly encourage the Inquiry to recommend that legislative proposals in these key policy areas be subject to comprehensive consultation and a thorough analysis of the cost benefit trade-off of policy options.

Privacy Act Review

The Attorney General's Department has recently published the Final Report of the Privacy Act Review containing over 100 recommendations. Taken together, the recommendations if acted upon by the Government would represent a fundamental rebuild of the Privacy Act and elevate it as a priority legislative framework for businesses. The changes would significantly increase the level of prescription of key obligations, require significant resourcing and changes to business processes for organisations of all sizes, and bring Australia's privacy law regime into alignment with the European Union's (**EU**) General Data Protection Regime (**GDPR**).

Consistent with our submission to the Privacy Act Review in January 2022, we support reforms that modernise the Privacy Act to ensure it reflects a modern digital economy where individuals and businesses are engaging, and providing personal information, in new and innovative ways.[4] However, we are concerned that many of the proposed reforms are being advanced by a perception that Australia's privacy laws are weak and poorly performing, therefore warranting existing elements to be strengthened and made more prescriptive. Such a significant policy case needs to be comprehensively tested from a cost benefit perspective to ensure that the likely benefits will outweigh costs, for instance to innovation and business competitiveness with global counterparts.

For example, the recommended removal of the existing small business exemption under the Privacy Act requires very close analysis. This would be a significant change that would impose sweeping obligations

---

[3] AICD submission to Senate Legal and Constitutional Affairs Committee, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, November 2022, available here.
[4] AICD submission, Privacy Act Review, January 2022, available here.

on millions of small businesses and would come with material compliance costs at both an individual and aggregate business level. Our understanding is that under the proposed reforms the full suite of Privacy Act obligations will be imposed on small businesses, including for example the requirement to have a nominated senior manager be accountable for privacy. This approach, on first reading, appears disproportionate to the risk posed by many small businesses in mishandling personal information and will involve extensive compliance costs for potentially limited public benefit. Rather we would recommend that the Government focus on how such small businesses can be best supported, including in terms of building their cyber resilience and data management practices.

More generally, we understand that research conducted into the GDPR in the EU has identified legitimate questions about its effectiveness in improving privacy and has had potential detrimental impacts on innovation.[5] These studies point to the clear need for the Government to comprehensively consider the appropriateness of broadly adopting the GDPR model in Australia.

The AICD intends to engage comprehensively with directors to inform our submissions to the current consultation on the Privacy Act Review and future rounds on proposed legislation. We recommend this Inquiry urge the Government to closely assess the recommendations of the Privacy Act Review and undertake a thorough analysis of the effectiveness of the core components of the GDPR.

Data localisation

The Issues Paper notes that there is some level of concern with the cloud computing offering of Big Tech companies covering both cyber security, governance of data, compliance and the level of market concentration. As reflected in the Issues Paper, the concept of the 'cloud' is extremely broad and covers multiple different products or markets, from Infrastructure-as-a-Service to Software-as-a-Service.

AICD members have provided feedback that there is often a strong business case for utilising cloud platforms in some form, including those of Big Tech cloud providers (e.g. AWS, Azure). A cloud product or service is in most cases a more secure environment to store and manage data than the business itself storing data on local infrastructure. Further, it provides the business with a more innovative and evolving product, with greater computing power and is often not something that could be readily replicated by the customer. Directors have noted though that Australian businesses often have no or very limited bargaining power with Big Tech cloud providers, including limited scope to negotiate terms and conditions and price.

The AICD's view is that caution should be taken in proposing any widespread data localisation requirements for specific types of data or mandating that data is not stored offshore with the large Big Tech cloud providers. We are not satisfied that such regulatory intervention would result in improvements in cyber resilience or improve the level of competition in these markets. In particular, requiring Australian organisations to find domestic alternatives to Big Tech providers, is likely to be highly complex and costly and may deprive organisations of cost effective, secure and innovative data management solutions. Perversely, such intervention may reduce Australia's level of cyber resilience through limiting the use of more cyber secure providers overseas.

Lastly, we are unaware of clear evidence that there are currently significant management or misuse issues with Australian data being stored overseas, or that regulators or law enforcement agencies are

[5] National Bureau of Economic Research, *GDPR and the Lost Generation of Innovative Apps*, May 2022, available here; Social Science Research Network, *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR*, January 2020, available here.

unable to access this data in a timely manner. Again, we would encourage an evidence-based approach to policy making in this complex area.

4. Market concentration and vertical integration

This section responds to the market concentration section of the Issues Paper.

We recognise there are significant concerns with the market power, unfair contract terms and the degree of vertical integration of Big Tech firms in certain product and service markets in Australia. For instance, some directors have provided feedback that there is limited or no ability for even large Australian companies to negotiate on terms or price with large cloud providers owned by Big Tech companies.

However, we strongly encourage the Inquiry to proceed with caution with any recommendations that are intended to promote competition or curb any identified market power issues outside of the ACCC's Digital Platforms Inquiry (**DPI**). Since commencing the DPI the ACCC has built up extensive expertise and insight into the operation of digital platforms and Big Tech in Australia. Our view is that the DPI and its accompanying findings and recommendations is the appropriate avenue for the Government to assess the necessity for any changes to the existing competition laws, including the potential for a customised approach for digital platforms.

In particular, we note that the ACCC has proposed in its 5th Report, a new power under the *Competition and Consumer Act 2010* to make mandated codes of conduct for designated digital platforms. In addition to addressing competition and consumer conduct concerns by digital platforms, a code framework may also be an appropriate policy response to concerns about corporate responsibility of Big Tech subsidiaries and foreign branches, which we discuss below.

The Treasury recently concluded consultation on the ACCC's recommendations. The AICD did not participate in that consultation process and considers that key stakeholders with expertise in competition law and economics are better placed to reflect on the ACCC's recommendations. However, we note that Australia is a relatively small market globally for Big Tech companies and there appears to be clear advantages in Australia leveraging and aligning with international regulatory approaches as they are developed.

5. Corporate responsibility

This section addresses the issues raised on pages 42-43 of the Issues Paper in respect of the use of foreign branches and how directors of Australian subsidiaries of Big Tech companies meet their fiduciary and statutory director duties under sections 180-184 of the *Corporations Act 2001* (Cth) (**Corporations Act**).

The AICD interprets this section of the Issues Paper as raising concerns that the existing regulatory frameworks that apply to foreign branches and/or subsidiaries may be insufficient to ensure corporate responsibility at Big Tech companies. This includes that directors of subsidiaries of Big Tech companies are not meeting their directors' duties, particularly as it relates to understanding the activities, and acting in the interest, of the subsidiaries they govern. The suggestion appears to be that this in turn may have had a detrimental impact on the corporate responsibility of Big Tech companies in Australia, including exacerbating disinformation on digital platforms.

The AICD is not aware of any concerns or identified issues with directors of Australian subsidiaries failing to meet their directors' duties under the Corporations Act, including any regulatory action. We are also not

aware of issues with the use of foreign branches and understand that generally Big Tech companies have utilised the subsidiary model in Australia.

As reflected in the Issues Paper, directors of Australian companies have the same duties regardless of ownership of the company, including whether it is a foreign subsidiary. There is long-established judicial authority in Australia that directors of a subsidiary in a corporate group, including a foreign subsidiary, owe duties to, and must act in the interests of, that entity and that entity alone. In the case of directors of a wholly-owned subsidiary, section 187 of the Corporations Act expressly permits the director of a subsidiary to consider the interests of the corporate group in limited circumstances.[6] The test for whether a director acted in good faith in the best interests of the holding company is an objective test, meaning directors must act "reasonably". This consistent legislative framework has significant advantages in clearly setting out the obligations on individual directors and providing the regulator, ASIC, with a clear set of uniform duties under which to investigate and enforce potential breaches.

The AICD considers that the existing directors' duties framework, and the regulatory enforcement toolkit it provides to ASIC to pursue any breach of these obligations, is fit for purpose. Any proposals to amend this existing directors' duties framework to specifically address issues with Big Tech corporate responsibility would be a blunt and counterproductive policy response that could have widespread ramifications for directors of all organisations.

We also urge caution with any proposal to amend the foreign branch framework. It is not apparent there are deficiencies currently with this company model and any change to the framework would likely have implications for many other businesses and companies that operate in Australia and are not Big Tech.

The AICD's strong view is that where there are isolated concerns with the governance of Big Tech subsidiaries, this can be addressed through the existing legislative framework and enforcement tools.

6. Next Steps

We hope our submission will be of assistance. If you would like to discuss any aspects further, please contact Simon Mitchell, Senior Policy Adviser at smitchell@aicd.com.au or Laura Bacon, Senior Policy Adviser at lbacon@aicd.com.au.

Yours sincerely,

Louise Petschler GAICD
General Manager, Education & Policy Leadership

[6] Notably, section 187 only applies to wholly-owned subsidiaries and in circumstances where solvency is not an issue. The company constitution must also expressly authorise the directors to act in the best interests of the holding company for section 187 of the Act to apply.