28 February 2023

BSA COMMENTS ON INQUIRY INTO INTERNATIONAL DIGITAL PLATFORMS OPERATED BY BIG TECH COMPANIES

Submitted Electronically to the Senate Economics References Committee

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Senate Economics References Committee (**Committee**) on its inquiry into international digital platforms operated by Big Tech companies (**Inquiry**) and its associated Issues Paper.[2]

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members create the technology products and services that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. Our members have made significant investments in Australia, and we are proud that many Australian entities and consumers continue to rely on our members' products and services to do business and support Australia's economy.

In this context, BSA participated in public consultations on various matters that are raised in the Issues Paper, including privacy, data security, and online safety.[3] Given the many streams of ongoing work in the technology regulatory space, we encourage the Committee to be cautious of overlap in what is already a complex matrix of regulations, legislation, and guiding codes.

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Inquiry into international digital platforms operated by Big Tech companies, December 2022, https://www.aph.gov.au/-/media/Committees/economics_ctte/IssuesPaper/221206_FINAL_Issues_Paper.pdf?la=en&hash=AE4F8DA7564C4109FCC4BD6066BC65CB7EC3C120.

[3] For example, see:

a) BSA Comments on Basic Online Safety Expectations, November 2021, https://www.bsa.org/files/policy-filings/11122021bosecmts.pdf.

b) BSA Comments on Review of Australia Privacy Act 1988, January 2022 https://www.bsa.org/files/policy-filings/04222022auaippr.pdf.

c) BSA Comments on National Data Security Action Plan, June 2022, https://www.bsa.org/files/policy-filings/06062022aunatdatasec.pdf.

d) BSA Comments on Privacy Legislation Amendment Bill, November 2022, https://www.bsa.org/files/policy-filings/11072022aupriv.pdf.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

Summary of BSA's Recommendations

1. Foster a more coordinated regulatory landscape by avoiding regulatory duplication and overlap.

2. Explore how the Government can further collaborate with software and IT companies to drive digital transformation, education, and reskilling efforts.

3. Focus on strengthening public-private partnerships and adopt collaborative approaches to address the identified concerns in the Issues Paper, and improve coordination between regulators, policymakers, and the private sector.

Building a more coordinated regulatory landscape

The Inquiry considers "the adequacy and effectiveness of recent attempts in Australia and internationally, to regulate the activities of such international digital platforms" and highlights that there are "legitimate community expectations of explicit regulation of Big Tech in Australia".[4]

These community expectations have been met with a proliferation of regulations and initiatives. Due to the increasingly interlinked nature of digital and data related issues, this has created significant regulatory overlaps in Australia's technology regulatory landscape. For example, while there is currently no universal requirement for Australian businesses to report cyber security incidents, there are several mandatory reporting obligations for specific types of businesses that are spread across multiple pieces of legislation.[5] The proliferation and overlap of regulations often result from taking a reactionary approach to addressing specific issues.[6] This reactionary approach introduces unintended consequences, especially where legislation intended to address a specific issue has a broader impact due to the interlinked nature of digital and data activities, resulting in a piecemeal regulatory environment that is difficult for both public and private stakeholders to navigate.

The Committee should also note that there are already multiple ongoing initiatives and efforts that seek to (or already) address the concerns raised in the Issues Paper, such as data privacy and children safety.[7] Many such initiatives are efforts which will span multiple years and it is crucial that they run their course without any parallel approaches or initiatives being taken, so as to reduce regulatory confusion and overlap. Examples include the following:

---

[4] Issues Paper (2022), p.3 -4.

[5] Examples of prevailing reporting requirements include:

a) Under the Security of Critical Infrastructure Act 2018, and subsequent amendments, critical infrastructure asset owners and operators must report critical incidents (with a "significant impact" on their asset) within 12 hours of becoming aware of the incident, and other security incidents (with a "relevant impact" on their asset) within 72 hours.

b) The Privacy Amendment (Notifiable Data Breaches) Act 2017 amended the Privacy Act 1988 to require organisations to "notify affected individuals and the [Office of the Australian Information Commissioner] when a data breach is likely to result in serious harm to an individual whose personal information is involved". The scheme applies to all organisations covered by the Privacy Act, which includes Australian Government agencies and businesses with annual turnover of more than $3 million AUD. The Attorney General's Office is currently undertaking a substantial review of the Privacy Act.

c) In the financial services sector, the Prudential Standard CPS 234 on Information Security requires entities regulated by the Australian Prudential Regulation Authority (**APRA**) — including banks, insurers, and superannuation funds — to notify the regulator of material information security incidents within 72 hours. Entities must also notify APRA of material information security control weaknesses within 10 business days.

[6] As observed in 5 Year Productivity Inquiry: Australia's Data and Digital Dividend, August 2022, p. 82, https://www.pc.gov.au/inquiries/current/productivity/interim2-data-digital/productivity-interim2-data-digital.pdf.

[7] Issues Paper (2022), p. 28-.29.

- The ongoing review of the *Privacy Act 1988* (**Privacy Act**), which commenced in October 2020. The Attorney-General's Department (**AGD**) just released the comprehensive Privacy Act Review Report,[8] which considers many of the privacy issues which were raised in the Issues Paper.[9] The recently passed *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (**Privacy Enforcement Act**) also increased the maximum penalties that can be applied under the Privacy Act, increased the powers of the Australian Information Commissioner, strengthened the Notifiable Data Breaches scheme, and equipped the Australian Information Commissioner and the Australian Communications and Media Authority with greater information sharing powers. Given that only a few months have passed since the Privacy Enforcement Act entered into force, it is premature for the Inquiry to consider whether "stronger penalties" and "further changes to privacy laws" are required.[10]

- Similarly, pursuant to the *Online Safety Act 2021*, the industry is presently engaging with the eSafety Commissioner to develop a set of Industry Codes of Practice for the Online Industry aimed at regulating certain types of harmful online material[11] (e.g., material promoting child sexual abuse). This process has been ongoing since July 2021. The Issues Paper asks how "effective is the current legislative framework in protecting children" and "what more can be done to enhance online safety for child protection", but it is again premature to consider these questions when there is work being undertaken to specifically address these issues.

To avoid duplicating efforts and further complicating the regulatory landscape, BSA recommends that the Committee take stock of the ongoing initiatives and efforts that seek to (or already) address the questions and concerns raised in the Issues Paper, and to undertake a review for their effectiveness later, rather than seek to introduce additional legislative efforts at this point. We also recommend that the Committee consider the broader issue of how to reduce regulatory overlap, including by promoting improved coordination between regulators, policymakers, and the private sector (see Point 3).

Work with software and IT companies to drive digital transformation, education and reskilling efforts

While the Issues Paper considered the "very significant" investments by large, multinational software and IT companies in Australia,[12] these investments only form part of the contributions that such companies have made to Australia's economy.

Digital Transformation

One important contribution overlooked by the Issues Paper is the capacity for IT and software companies to drive digital transformation. BSA member companies develop the software-enabled

[8] Privacy Act Review Report 2022, February 2023, https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

[9] For example, the Privacy Act Review Report considers in detail the issue of whether to establish a statutory tort for serious invasions of privacy. See Issues Paper (2022) at p. 28 and the Privacy Act Review Report (2023) at Chapter 27 (A statutory tort for serious invasions of privacy).

[10] Issues Paper (2022), p. 28.

[11] Consolidated Industry Codes of Practice for the Online Industry, Phase 1, accessed February 2023, https://onlinesafety.org.au/codes/.

[12] Issues Paper (2022), p. 31 – 33.

tools that allow both businesses and governments to maximize productivity and grow their operations. Examples of the potential for digital transformation are as wide-ranging as its potential:[13]

- **Retail**: Software solutions will transform the shopping experience for both online and brick-and-mortar operations. In-store shoppers can expect Augmented Reality (**AR**) and Virtual Reality (**VR**) offerings that create a more engaging and interactive environment, and other tools will provide more convenient customer service operations. Online, new tools will create seamless customer experiences tailored to specific customers.

- **Healthcare:** Healthcare providers will use various digital solutions to create patient-centric and value-based outcomes that both improve care and reduce costs. Virtual doctor visits and networked electronic medical records are just two modes of digitalisation that are transforming healthcare. Pharmaceutical and healthcare companies such as Abbott and Amgen will use digital tools to quickly develop new therapies and to deliver new services to patients.

- **Manufacturing:** The Industrial Internet of Things helps companies improved production by reducing downtime and wasting less materials while still ensuring high-quality goods. Predictive maintenance and other process upgrades will improve worker efficiency and increase profits. AR solutions can enable advance training and allow for collaboration across widespread operations.

- **Smart Cities:** Mixing physical infrastructure like roads, bridges, and buildings with cutting-edge digital technologies will ensure safer communities and improve citizens' quality of life. From utility monitoring to public safety to environmental sustainability, technologies such as sensors, AI, and video analytics are helping the public sector transform the way it provides essential services to achieve greater efficiency, lower costs, and a higher level of citizen engagement.

COVID-19 highlighted further the importance of digital transformation and enablement, as both businesses and governments leveraged on software tools to supplement their response to the pandemic. For example, in Australia, Lifeline needed to quickly facilitate a remote contact centre for Crisis Supporters to speak with supervisors, as well as two-way short messages for supporter-to-help-seeker connection. Using Twilio, Lifeline deployed a 100% cloud contact centre in less than a week to support Australians in need.

Education and Reskilling

Another increasingly important contribution from large IT and software companies is their provision of substantial education and reskilling opportunities for students and workers to develop digital capabilities to meet the demands of a rapidly digitalising economy.

Many software and IT companies are partnering with Australian educational institutions to strengthen science, technology, engineering, and mathematics education for students enrolled in traditional educational programs:

- Alteryx provides access to a holistic data analytics curriculum called SparkED - including education software, learning pathways, certification preparation, and a vibrant online community for support and career networking – free of charge to university educators. More

[13] Digital Transformation: A Look at Where We Are and the Promise of What's to come, February 2022, https://www.dxnetwork.org/downloads/dtnprimer.pdf.

than a dozen Australian universities and student societies are already benefitting from Alteryx's SparkED program, with educators using these resources to support students in fields ranging from business analytics to supply chain and accounting.[14]

- Cisco's Networking Academy has been in Australia for 25 years. It is an internationally-recognised IT skills and career-building program that is free of charge. Cisco partners with colleges, universities, vocational schools, public sector, and nonprofits in Australia, and ensures opportunities are evenly dispersed based on age, gender, and economic diversity, plus, open to those with disabilities. Cisco has supported the training of almost 240,000 students through more than 100 partnerships with learning institutions in Australia. 94% of students in Australia completing a Cisco Certified course report that the program has assisted them to gain a new Job or a better educational opportunity.[15]

Notably, large IT and software companies also provide alternatives to a formal, full-length undergraduate or postgraduate degree. Such alternatives are crucial for incentivising workers to transition into technology roles, as they enable workers to obtain targeted skills or knowledge within a shorter timeframe and at a reduced cost relative to traditional tertiary education.

- Vendor certifications are provided by companies that offer software or data services to train users of those services. For example, AWS, through its Skill Builder initiative, offers over 500 courses ranging from foundation AWS cloud knowledge through to specialty domains in machine learning, advanced networking, and databases.[16] Salesforce's Trailhead initiative is a free online learning platform that provides wide range of courses and skills training, including data management, platform development, and Customer Relationship Management basics.[17] Microsoft Learn empowers individuals by providing free access to over 3500 modules of learning from fundamentals to expert level.[18] This includes content for individuals seeking professional development, educators looking to modernise their curriculum,[19] students wishing to demonstrate their technical capability through free certifications,[20] and to a range of commercial and non-profit organisations looking to reskill the nation.[21]

A recent example of public-private partnership in this regard is how the Australian IT sector partnered with the Government in 2020 to launch Skill Finder — a digital skills marketplace where Australians can sign up for short courses offered by technology companies. Many BSA member companies provide courses on Skill Finder, including Adobe, Atlassian, AWS, Cisco, IBM, Microsoft, Salesforce, and SAP.[22]

BSA recommends that the Committee explore how the Government can do more to tap into software and IT companies' resources and expertise to drive digital transformation, education, and reskilling efforts. One possible collaboration between Government and industry in this

---

[14] Alteryx SparkED, accessed February 2023, https://www.alteryx.com/sparked.

[15] Cisco Networking Academy, accessed February 2023, https://www.netacad.com/.

[16] AWS Skill Builder, accessed February 2023, https://aws.amazon.com/training/digital/.

[17] Salesforce Trailhead, accessed February 2023, http://trailhead.salesforce.com/.

[18] Microsoft Learn: accessed February 2023, https://learn.microsoft.com/en-us/training/.

[19] Microsoft Learn for Educators program: accessed February 2023, https://learn.microsoft.com/en-us/training/educator-center/programs/msle/.

[20] Microsoft Certification, accessed February 2023, https://msftstudentcert.cloudreadyskills.com/.

[21] Microsoft Professional Certificates, accessed February 2023, https://opportunity.linkedin.com/skills-for-in-demand-jobs.

[22] Skill Finder, accessed February 2023, https://www.skillfinder.com.au/.

regard is exploring mechanisms to better adopt and recognise vendor training within accredited training and formal education.[23]

Strengthen public-private partnerships

Communication and collaboration between the public and private sectors are cornerstones of a vibrant digital economy. Healthy public-private partnerships allow all stakeholders to reap the substantial benefits of digitalisation, while overcoming the ever-evolving risks and challenges presented by new technologies.

In this regard, the Committee should note that many of the matters that are raised in the Issues Paper, including privacy, data security, and online safety, often involve shared responsibilities across both public and private sectors. For example, in the context of data security, although governments often hold critical security tools and information, the private sector owns and operates significant elements of the critical infrastructure and the technology platforms that are targeted by malicious cyber activity, as well as many of the cyber security tools and services necessary to defend against such threats. To better address these concerns, it is imperative for the public and private sectors to work together.

At the outset, the Issues Paper characterised the Inquiry as an assessment of "the extent to which [Big Tech] exert power and influence over markets to the detriment of Australian consumers".[24] Framing the relationship between technology service providers and Australian consumers in this way is counterproductive. It undermines the trust and collaborative relationships that the public and private sectors have built up over many years and the considerable potential for future growth in the Australian digital economy.[25] Instead, the Committee should focus on strengthening public-private partnerships and finding ways to approach the identified risks and concerns (e.g., security and governance issues related to cloud computing,[26] data privacy concerns[27]) in a collaborative manner.

A recent initiative by the Department of Home Affairs — the Trusted Information Sharing Network (**TISN**) — serves as a positive example of an effective and innovative public-private partnership mechanism. The TISN provides a platform for critical infrastructure owners and operators to share information on threats and vulnerabilities and collaborate on appropriate measures to mitigate risk and boost resilience. The TISN is comprised of representatives from different critical infrastructure sectors, and each sector is supported by an Australian Government agency — usually the agency that has regulatory responsibility for that sector. Under the TISN Data Sector Group, data storage and processing service providers, which include cloud service providers, work together with government agencies to: a) identify and manage risks to critical infrastructure; b) address security gaps within sectors and implement mitigation strategies; c) inform future policy and programs to further support

[23] The current process for integrating industry content into nationally accredited qualifications requires a complex mapping of industry training material and curriculum with Units of Competency, which can become out-of-date quickly due to rapid changes in technology. Further, without better recognising the adoption of this industry-relevant content in the training leveraged for traineeship and apprenticeship programs, it creates a lack of incentives in the system for young people to do industry-relevant training and for businesses in the development of entry-level pathways.

[24] Issues Paper (2022), p.3.

[25] The Australian tech sector has become a critical part of the economy, contributing $167bn to Australia's GDP in 2021, equivalent to 8.5%, and employing 861,000 Australians. The Australian tech sector could contribute $244bn annually to GDP by 2031. See: The economic contribution of Australia's tech sector, August 2021, https://techcouncil.com.au/wp-content/uploads/2021/08/TCA-Tech-sectors-economic-contribution-full-res.pdf.

[26] Issues Paper (2022), p. 18.

[27] Issues Paper (2022), p. 24-25.

critical infrastructure resilience; and d) achieve the objectives of the Critical Infrastructure Resilience Strategy.[28]

BSA recommends the Committee consider similar collaborative approaches to address the identified concerns in the Issues Paper, but just as importantly, to improve coordination between regulators, policymakers, and the private sector (see Point 1).

In this regard, BSA notes that the Digital Platform Regulators Forum (**DP-REG**) was established in March 2022 to improve coordination on digital platform regulation,[29] focusing on "how competition, consumer protection, privacy, online safety and data intersect in issues that the various regulators consider".[30] Unfortunately, the DP-REG is comprised only of regulators — absent from the conversation are both policymakers and industry representatives.

In light of the above, BSA further recommends the Committee assess the viability of adopting the Australia National University Tech Policy Design Centre's proposed Tech Policy and Regulation Coordination (TPRC) Model.[31] The TPRC model was developed following extensive consultations with Australian regulators, the Australian Government, industry and civil society, and a study of tech regulators in 14 jurisdictions.[32] The TPRC model contemplates setting up a Tech Policy and Regulation Expert Forum (**TPREF**) and a standing Tech Policy and Regulation Expert Advisory Panel (**TPREAP**), both which facilitate meaningful participation by industry.[33] The increased involvement of industry representatives will provide the government with access to independent technical expertise and a regular platform for consultations. More importantly, it will discourage taking a reactionary approach when addressing emerging concerns and ultimately will pave the way for a more certain regulatory environment.

Conclusion

We hope that our comments will assist the Committee as it moves forward with the Inquiry. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Tham Shen Hong

Tham Shen Hong
Manager, Policy – APAC

---

[28] Trusted Information Sharing Network – Overview, accessed February 2023, https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/tisn-overview.pdf.

[29] The DP-REG consists of the Australia Competition and Consumer Commission (**ACCC**), Australia Communications and Media Authority (**ACMA**), Office of Australia Information Commissioner (**OAIC**) and Office of the eSafety Commissioner.

[30] DP-REG Terms of Reference, March 2022, https://www.oaic.gov.au/__data/assets/pdf_file/0019/16732/DP-REG-Terms-of-Reference.pdf.

[31] Tending the Tech-Ecosystem: who should be the tech-regulator(s)?, February 2023, https://techpolicydesign.au/wp-content/uploads/2022/11/Web_TPDC_Publication_NO.1_2022-3.pdf.

[32] Tending the Tech-Ecosystem (2023), p. 7.

[33] The TPREF would comprise of 25 core industry, civil society and consumer representatives appointed for 2-year terms, whereas the TPREAP is a database of experts drawn from industry, academia, or civil society, but serving in their independent personal capacity.