21 October 2022

BSA COMMENTS ON AUSTRALIA PRODUCTIVITY COMMISSION'S SECOND INTERIM REPORT

Submitted Electronically to the Productivity Commission

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Productivity Commission (**Commission**) on the second Interim Report of its Productivity Inquiry (**Interim Report**).[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. These products and services require companies to entrust data to our members, and our members work hard to keep that trust. 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.

BSA participated in public consultations on various issues that were raised in the Interim Report, such as data sharing, critical infrastructure, cyber security, and artificial intelligence (**AI**).[3] We welcome the Commission's balanced consideration of these issues and appreciate the Interim Report's findings on the use of digital technology and data in the Australian economy, potential barriers to adopting new technologies, and key policy priorities for the Government to improve Australia's productivity.

---

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, 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] 5 Year Productivity Inquiry: Australia's Data and Digital Dividend, August 2022, https://www.pc.gov.au/inquiries/current/productivity/interim2-data-digital/productivity-interim2-data-digital.pdf.

[3] For example, see:

a) BSA Comments on Australia Cyber Security Strategy 2020, November 2019, https://www.bsa.org/files/policy-filings/11012019au2020cybersecuritystrat.pdf.

b) BSA Comments on Data Availability and Transparency Bill 2020, November 2020, https://www.bsa.org/files/policy-filings/02262021datbillcmte.pdf

c) BSA Comments on Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, January 2022, https://www.bsa.org/files/policy-filings/01312022slacip.pdf;

d) BSA Comments on Automated Decision Making and Artificial Intelligence Issues Paper, April 2022, https://www.bsa.org/files/policy-filings/04222022auaippr.pdf.

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

BSA proffers the following recommendations, which correspond to specific policy priorities highlighted in the Interim Report.

Creating new data sharing and integration opportunities:

1. Allow private and non-Australian entities to participate in the DAT Act's data sharing scheme.
2. Explore privacy enhancing technologies.

Developing digital, data and cyber security skills:

3. Improve access to STEM education and training.
4. Leverage on Skill Finder and "earn as you learn" programs to drive workforce retraining.

Balancing cyber security and growth:

5. Reaffirm commitment to risk-based policies, internationally recognised standards/approaches, and data privacy.
6. Refrain from imposing data localisation requirements and data transfer restrictions.
7. Incorporate appropriate checks and balances.

Supporting ethical use of technology and data:

8. Account for the different roles and responsibilities of stakeholders.
9. Impact Assessments for high-risk systems.

Coordinating the policy and regulatory environment:

10. Streamlining regulations and appointing a lead agency to oversee regulations/initiatives for specific areas, such as cyber security.
11. Including a "coordination impact statement" in consultation documents.

Creating new data sharing and integration opportunities

The Interim Report observed that while Australia has "some data sharing frameworks and infrastructure", including a public sector data sharing scheme under the *Data Availability and Transparency Act 2022* (**DAT Act**), there is "still significant room for improvement to generate value and productivity growth from the use of data accessible under these frameworks".[4]

BSA agrees with this observation. Government-held data is an important asset that can serve as a powerful engine for creating new jobs, promoting economic growth, driving productivity gains, and enabling innovation. To create new data sharing and integration opportunities, BSA recommends the following:

[4] Interim Report (2022), p. 44.

1. Allow private and non-Australian entities to participate in the DAT Act's data sharing scheme

The DAT Act establishes a scheme for sharing public sector data with "accredited users" for specific purposes (**Scheme**).[5] However, under the Scheme, only Australian entities are allowed to apply for accreditation. Furthermore, private entities, including "individuals, bodies corporate, partnerships, trusts and unincorporated entities" will not be able to apply for accreditation.[6] While BSA recognises that the exclusion of these entities was intended to allow the Scheme to mature, these restrictions limit the efficacy of the Scheme, and consequently, the potential of public sector data to drive economic growth and productivity.

As the Scheme will be subject to an independent review three years after its commencement,[7] BSA strongly urges the Productivity Commission to recommend expanding the Scheme to allow both private and non-Australian entities to apply for accreditation. The accreditation framework contemplated in the DAT Act already allows the Australian Government to make a risk-based decision based on the company's ability to best meet security and data-handling requirements, among other factors.[8] Whether an entity is a private or foreign one should not matter so long as it can meet the requirements in the accreditation framework, and the Australian Government retains the discretion to reject applications from entities which do not meet said requirements.

2. Explore privacy-enhancing technology

The Interim Report rightly noted that "[t]he benefits of data sharing must also be balanced against safety and privacy concerns".[9] **In this regard, BSA encourages the Productivity Commission to recommend to the Australian Government that it explores and promotes opportunities to further build value from the safe and responsible use of data with the application of privacy-enhancing technologies.** A range of emerging technologies, including homomorphic encryption, differential privacy techniques, and federated machine learning create opportunities for further sharing data while preserving individual privacy. These technologies can be used to maximise both the value and the confidentiality of sensitive information.

Developing digital, data and cyber security skills

The workforce demands of the new digital economy require preparing new generations for jobs of the future, assisting current workers as they transition to the emerging opportunities of the digital economy, and expanding opportunities to reach a bigger pool of talented workers. In this regard, the Interim Report noted that "demand for specialist digital and data workers is high across the Australian

[5] DAT Act, Section 12. Under the data sharing scheme, Commonwealth bodies are authorised to share their public sector data with accredited users, and accredited users are authorised to collect and use the data, in a controlled way. Data may be shared with an accredited user 9 directly, or through an intermediary accredited for the purpose (called an ADSP, short for accredited data service provider).

[6] Data Availability and Transparency Bill 2022 Supplementary Explanatory Memorandum, May 2022, para 6, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr6649_ems_a59313dc-0b7c-4244-8b78-c7c5e7380407%22.

[7] DAT Act, Section 142(2).

[8] DAT Act, Section 77(1). To become accredited, an entity is required to have: appropriate data management and governance policies and practices; an appropriately qualified individual in a position that has responsibility for data management and data governance; ability to minimise the risk of unauthorised access, sharing or loss of data; the necessary skills and capability to ensure the privacy, protection and appropriate use of data; and any additional criteria prescribed by the Minister.

[9] Interim Report (2022), p. 52.

economy, not just in the technology sector", and that as the Australian economy becomes increasingly digitalised, the demand for these workers is expected to grow.[10]

BSA advocates for collaborative action between the private and public sectors on the following:

3. Improve access to STEM education and training

Science, technology, engineering, and mathematics (**STEM**) education equips students with problem solving, critical thinking, and other abilities that are important for jobs in virtually every industry. It also builds interest in developing in-demand skills, which expands the available workforce for technology-related jobs.

BSA notes that in the recently concluded Job and Skills Summit, the Government committed to review STEM programs to "attract and retain more women, First Nations people, Australians in regions, those who are culturally and linguistically diverse, people with a disability and Australians from low socio-economic backgrounds into STEM careers".[11] In the immediate term, the Government will also "develop and deliver a free national virtual work experience program, which will build awareness of tech careers and support early stage-talent pathways for those who face heightened barriers to employment".[12]

BSA commends the Australian Government on its commitment to maximise opportunities in STEM, especially for underrepresented communities. BSA recommends that the Productivity Commission urge the Government to continue collaborating with the private sector on similar initiatives, including by offering scholarships and incentives such as loan forgiveness, to make STEM education more inclusive and widely available.

4. Leverage on Skill Finder and "earn as you learn" programs to drive workforce retraining

The Interim Report observed that there are "a range of reskilling and upskilling options available for workers to develop the specialist digital or data capabilities required to transition into a technical role".[13] One such option is "vendor certifications provided by companies that offer software or data services to train users of those services".[14]

In this regard, BSA notes that the Australian tech sector partnered the former Coalition Government in 2020 to launch Skill Finder – a digital skills marketplace where Australians can sign up for short courses offered by technology companies. Many of our member companies provide courses on Skill Finder, including Adobe, Atlassian, AWS, Cisco, IBM, Microsoft, Salesforce, and SAP.[15] **BSA recommends that the Productivity Commission urge the Government to continue funding and leveraging Skill Finder to drive workforce retraining, including by partnering with more technology companies and ensuring that the courses provided are constantly updated.**

However, free skills training alone may not sufficiently incentivise workers. Many adult learners simply cannot afford to participate in training if said training requires them to choose between working and

---

[10] Interim Report (2022), p. 56 – 57.

[11] Job and Skills Summit Outcomes Document, September 2022, p. 12, https://treasury.gov.au/sites/default/files/inline-files/Jobs-and-Skills-Summit-Outcomes-Document.pdf.

[12] Job and Skills Summit Outcomes Document (2022), p. 10.

[13] Interim Report (2022), p. 62.

[14] Interim Report (2022), p. 62.

[15] Skill Finder website: https://www.skillfinder.com.au/.

upskilling. BSA therefore commends the Government's plan to "deliver Digital Apprenticeships that will support workers to earn while they learn in entry level tech roles, with equity targets for those traditionally under-represented in digital and tech fields".[16] **BSA recommends expanding such "earn as you learn" programmes, including by exploring other models of offering such programmes (e.g., boot camps) to incentivise retraining and reskilling.**

Balancing cyber security and growth

Cyber security continues to grow in importance as organisations of all types continue their digital transformations. BSA agrees with many of the Interim Report's observations in this section. These include:

- Government initiatives to improve cyber resilience and response should be "light touch" where the risks are relatively low, so to minimise the potential of unnecessary costs imposed on businesses while supporting better security outcomes;[17]

- The impacts of the Government's recent critical infrastructure security regulations remain unclear but, while more time and information are required to understand whether these regulations strike an appropriate balance, there is no evaluation or review process included in the legislation;[18] and

- Incident reporting requirements should be streamlined to avoid duplication, so that businesses are not unnecessarily burdened with multiple reporting requirements when they are focused on recovering from security breaches.[19]

Building on the insights in the Interim Report, BSA further recommends the following:

5. Reaffirm commitment to risk-based policies, internationally recognised standards/approaches, and data privacy

Malicious cyber activity carries different risks for different systems and types of data. There are generally multiple approaches to defending against the same type of cyber-attack, and multiple approaches to improving data security and resiliency. Regulations and policies should prioritise approaches and policies that address different levels of risk and enable owners and operators of networks and systems to defend their data with the technologies and approaches they deem best to meet the level of security desired.

In addition, given the importance of personal and sensitive information, cyber security regulations and policies should be carefully attuned to privacy considerations. Key considerations include ensuring civilian leadership and avoiding policies that undermine the use of privacy-enhancing technologies. Privacy policies should also be aligned with leading global privacy laws, such as by incorporating the

[16] Job and Skills Summit Outcomes Document (2022), p. 12.

[17] Interim Report (2022), p. 71.

[18] Interim Report (2022), p. 73.

[19] Interim Report (2022), p. 74.

data controller/processor distinction in the review of the *Privacy Act 1988* (**"Privacy Act"**) and extending its obligations to all sectors of the economy, including small businesses. [20]

BSA urges the Productivity Commission to emphasise the importance of committing to: a) risk-based policies and practices, rather than check-box, compliance-based approaches and allow government agencies to make cybersecurity decisions based on their context and needs; and b) accounting for data privacy considerations and ensuring that privacy policies are aligned with leading global privacy laws.

6. Refrain from imposing data localisation requirements and data transfer restrictions

A growing trend of data localisation requirements present serious challenges for business of all kinds. Governments often impose these requirements under the belief that this will improve security of sensitive data.

However, requiring businesses to localise their computing facilities and data can actually undermine security by increasing risks and decreasing resilience. This can happen when localisation measures compel businesses to use local data storage providers, which limits options for businesses deciding which entities they will entrust their data to. For example, under localisation measures companies may be unable to use their business's own globally-centralised data storage center and unable to use service providers without data centers in country. But local data storage service providers may not have the same security capabilities as global counterparts, which benefit from collecting data worldwide about real-time threats and comparing malicious actors across regions and customers, which helps identify and prevent potential cyber threats. Fragmented cybersecurity systems could also expose customers in a region that relies on localised networks to new threats from other parts of the world, reducing information privacy and security for those customers. Further, requiring data to stay within a country does not allow for a company to create backups that will not be susceptible to physical or natural disaster related risks.

In this regard, we are encouraged that Australia's Digital Trade Strategy[21] expressly acknowledges the importance of facilitating cross-border data transfers and prohibiting data localisation requirements. As the Digital Trade Strategy notes, "[u]necessary restriction on the flow of data, or requirements to store data locally raises costs for businesses and significantly reduces efficiencies, impacts the ability to make decisions on business development, marketing, innovation and development of comparative advantage, and makes it difficult for businesses to enter new markets".[22] We are also fully supportive of the approach taken in Australia's Digital Economy Agreement with Singapore, which sets out binding rules prohibiting unwarranted restrictions on cross-border data transfers and requirements to localise computing facilities.

BSA urges the Productivity Commission to recommend that the Government maintain its position on facilitating cross-border data transfers and prohibiting data localisation requirements.

---

[20] This distinction is necessary in today's digital economy, where an individual may use a service from one consumer-facing entity, but that entity may rely on numerous other enterprise service providers to store, analyse, and process the data in connection with that service. Each entity that processes an individual's personal information should be subject to strong obligations to safeguard that information, but those obligations should vary according to the different roles these entities play. Other privacy regimes that have adopted this distinction include the European Union's General Data Protection Regulation, California's Consumer Privacy Act, Japan's Act on the Protection of Personal Information, and Singapore's Personal Data Protection Act

[21] Digital Trade Strategy, April 2022, https://www.dfat.gov.au/sites/default/files/digital-trade-strategy.pdf.

[22] Digital Trade Strategy (2022), p. 10.

7. Incorporate appropriate checks and balances

The Government is vested with significant powers to uphold cyber security. One such example is the Government's new powers under the amended *Security of Critical Infrastructure Act 2018* (**SOCI Act**) to intervene and assist a critical infrastructure provider in responding to a serious security incident, as identified in the Interim Report.[23] However, intrusive powers, even for the purposes of upholding cyber security, can compromise user confidence in the integrity and trustworthiness of a service provider's products and services, and should therefore be subject to appropriate checks and balances, such as independent authorisation and reviews on the exercise of such intrusive powers.

BSA urges the Productivity Commission to recommend that the Government incorporate independent authorisation requirements and reviews on the exercise of intrusive powers vested by cyber security laws. One possible check is the implementation of a mandatory review process through which panel of independent technical experts assesses the security, technical feasibility, and reasonableness of exercising said powers.

Supporting ethical use of technology and data

The Interim Report observed that emerging technologies such as AI and the Internet of Things (**IOT**) "have created ethical issues that may not relate directly to productivity, but can degrade trust in businesses and governments' use of technology and data", thus limiting adoption.[24]

BSA agrees with the above observation. To build confidence and trust in emerging technologies, organisations that develop them must do so responsibly and in a manner that accounts for the unique opportunities and risks the technology poses. Policymakers can enhance public confidence and trust by establishing a legal and regulatory environment that supports responsible innovation. In this regard, BSA recommends the following:

8. Account for the different roles and responsibilities of stakeholders

To the extent new regulations on emerging technologies are contemplated, they must account for the array of stakeholders that may play a role in various aspects of a system's design, development, and deployment.

For example, in the context of AI systems, there are at least two key stakeholders with varying degrees of responsibility for managing the risks associated with an AI system throughout its lifecycle:

- **AI Developers:** AI Developers are organisations responsible for the design and development of AI systems.

- **AI Deployers:** AI Deployers are the organisations that adopt and use AI systems — if an entity develops its own system, it is both the AI Developer and the AI Deployer.

Including this conceptual distinction would be helpful to different stakeholders as they carry out risk assessments to determine the appropriate measures to adopt for AI development, deployment, and use. In addition, it would also be useful for both AI developers and deployers to consider who the ultimate end user of the AI solution will be — in general, end-user businesses should be considered

[23] SOCI Act Part 3A and Interim Report (2022). P.72

[24] Interim Report (2022), p. 77.

more sophisticated users than end-user individuals — and this would in turn have implications on internal risk assessments and commercial viability.

9. Impact assessments for high-risk systems

An impact assessment is an accountability mechanism that promotes trust by demonstrating a system has been designed in a manner that accounts for potential risks it may pose to the public. By establishing a process for personnel to document key design choices and their underlying rationale, impact assessments enable organisations that develop or deploy high-risk systems, notably AI,[25] to identify and mitigate risks that can emerge throughout a system's lifecycle. **BSA recommends that the Productivity Commission encourage the use of impact assessments for high-risk systems and increased collaboration between the Government and industry stakeholders to outline processes for performing impact assessments.**

Coordinating on the policy and regulatory environment

The Government is progressing multiple initiatives to introduce proportionate and fit-for-purpose protections for a range of data and cyber security issues, such as the *Privacy Act 1988* review, the Hosting Certification Framework (**HCF**) and the recent amendments to the SOCI Act. However, these legislative and policy initiatives were developed and introduced for specific purposes. As such, the Interim Report rightly noted that this has resulted in "disparate regulations that target specific problems",[26] leading to a congested regulatory environment that is increasingly difficult for businesses to navigate.

To improve coordination and mitigate congestion, BSA recommends:

10. Streamlining regulations and appointing a lead agency to oversee regulations/initiatives for specific areas, such as cyber security.

Due to the proliferation of regulations and initiatives and the increasingly interlinked nature of digital and data related issues, there are significant regulatory overlaps in Australia's technology regulatory landscape. For example, multiple Government agencies – including the Department of Home Affairs, the Attorney General's Department, Digital Transformation Agency, and the Office of National Data Commissioner – oversee different legislative and policy initiatives related to data security. The Interim Report's section on streamlining incident reports similarly identifies several mandatory reporting obligations for specific types of businesses that have experienced cyber incidents.[27]

Another example of regulatory overlap is the possible expansion of the Hosting Certification Framework (**HCF**) to cover Software-as-a-Service (**SaaS**) providers. The HCF was originally conceived to address supply chain and foreign ownership risks presented by data hosting providers.[28] However, this expansion adds an unnecessary layer of certification on top of existing guidelines and mechanisms, which are already fit for purpose. For example, assessors certified under the Infosec Registered Assessor Program (**IRAP**) can provide security assessments of cloud services and ICT

[25] When AI is used in contexts that implicate civil rights or access to important life opportunities, the public should be assured that such systems have been thoroughly vetted by companies and will be continuously monitored to account for the risks associated with unintended bias. BSA recently published *Confronting Bias: BSA's Framework to Build Trust in AI* to outline a comprehensive methodology for performing impact assessments to manage these risks (see https://ai.bsa.org/confronting-bias-bsas-framework-to-build-trust-in-ai).

[26] Interim Report (2022), p. 82.

[27] Interim Report (2022), p. 74.

[28] Release of the Hosting Certification Framework, March 2021, https://www.dta.gov.au/news/release-hosting-certification-framework.

systems. To assist with the assessment of cloud services, the Cloud Security Controls Matrix (**CSCM**) can be used by IRAP assessors to capture the implementation of security controls. The CSCM also provides indicative guidance on the scoping of cloud security assessments, and inheritance for systems under a shared responsibility model. Furthermore, since the amendments to the SOCI Act, SaaS providers that work with "business critical data" are already required to be registered as critical infrastructure and will be subject to the relevant regulatory obligations, including registration of ownership.

BSA therefore agrees with the Interim Report's observation that there are many "disparate regulations that target specific problems", and that it has led to a "piecemeal regulatory environment".[29] These disparate regulations need to be streamlined to reduce business uncertainty and unnecessary costs.

In addition, the Government should consider appointing or identifying a single lead agency in areas where there are significant regulatory overlaps, such as cyber security. This lead agency would identify overlaps and oversee the cyber security regulations and initiatives of all Government agencies, ensuring consistency and coherence across all policy initiatives. This would require significant internal restructuring between agencies to ensure that that lead agency is equipped with sufficient manpower and resources to conduct this oversight function.

11. Including a "coordination impact statement" in consultation documents

As structural changes to appoint lead agencies will take significant time to implement, **BSA suggests that, in the meantime, agencies include a "coordination impact statement" in consultation documents.** Similar to a regulatory impact statement, a coordination impact statement should list the government agencies that have been engaged in internal consultations and their perspectives, as well as the implications of any policy overlaps, if any. It should also take into consideration relevant State-based laws and policies, especially when the consultation relates to proposing new national policies.

While this may lengthen the consultation process, this would compel agencies to coordinate their positions internally before proceeding with public consultations.

Conclusion

We hope that our comments will assist the Productivity Commission as it moves forward with the Interim Report. 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

[29] Interim Report (2022), p. 82