15 September 2025

BSA COMMENTS ON PRODUCTIVITY COMMISSION'S HARNESSING DATA AND DIGITAL TECHNOLOGY INTERIM REPORT

Submitted Electronically to the Productivity Commission

The Business Software Alliance (**BSA**)[1] welcomes the opportunity to submit comments to the Productivity Commission on its Interim Report on Harnessing Data and Digital Technology (**Interim Report**).[2]

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

BSA commends the Productivity Commission for recognising the importance of harnessing the economic and productivity benefits of data and digital technology. The Interim Report rightly highlights that emerging technologies such as artificial intelligence (**AI**) can play a transformative role in driving growth across all sectors of the Australian economy. However, realising this potential requires a regulatory landscape that encourages innovation while providing clear guidance for businesses. We are encouraged that the Interim Report's findings and recommendations underscore the need for clear and outcomes-focused reform options which minimise unnecessary regulations, thereby enabling Australian businesses to adopt and leverage technology with confidence.

Summary of BSA's Recommendations

Our recommendations correspond to the specific policy areas highlighted in the Interim Report, as follows:

<u>Artificial Intelligence</u>

1. Focus on identifying high-risk use cases of AI
2. Recognise and define the different roles and responsibilities of entities in the AI supply chain

[1] BSA's members include: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

[2] Harnessing Data and Digital Technology – Interim Report, August 2025, https://www.pc.gov.au/inquiries/current/data-digital/interim/data-digital-interim.pdf

3. Officially designate a non-regulatory central coordinating body for AI policy
4. Introduce a clear copyright exception for AI training

Data Access

5. Allow private and non-Australian entities to participate in the Data Availability and Transparency Act 2022 (**DAT Act**) data sharing scheme
6. Explore privacy-enhancing technologies

Privacy

7. Implement a controller-processor distinction

Artificial Intelligence

The broad adoption of enterprise AI by Australian businesses and organisations must be a strategic priority for the Government. The economic opportunities presented by AI extend beyond the development of more powerful tools – they also lie in enabling these tools to make every sector of the economy more efficient and productive. Countries that promote AI adoption across both the private and public sectors will be best placed to capture the greatest economic benefits and deliver substantial gains across industries. overly prescriptive or premature regulation risks discouraging businesses from adopting AI tools.

In this regard, BSA agrees with the Interim Report's findings and recommendations that:

- The Government plays a key role in promoting investment in digital technology, including AI, by providing a stable regulatory environment.[3]
- Any regulatory response to potential harms from using AI must be proportionate, risk-based, outcomes-based and technology neutral where possible.[4]
- The Government should undertake a comprehensive set of "gap analyses" to understand the risks stemming from AI and whether these risks can be dealt with under existing regulatory frameworks.[5]
- Until these gap analyses are completed, the Government should pause consideration on economy-wide AI-specific regulations, including potential mandatory guardrails for AI in high-risk settings, to avoid regulatory duplication and imposing unnecessary compliance burdens.[6]
- Economy-wide AI-specific regulations should only be considered as a last resort for the use cases of AI that meet two criteria, namely: a) where existing regulatory frameworks cannot be sufficiently adapted to handle the issue; and b) where technology-neutral regulations are not feasible.[7]

[3] Interim Report (2025), p. 19.

[4] Interim Report (2025), p. 19.

[5] Interim Report (2025), p. 17. BSA further notes that in 2022, the Australian Government conducted a similar consultation on whether Australia's laws and regulations are fit for purpose and able to respond to emerging technologies, such as AI. While this consultation was conducted before the generative AI "boom", the Government can leverage the groundwork and insights gleaned from this exercise. **See:** Consultation launched to position Australia as a leader in Digital Economy Regulation, March 2022, https://www.pmc.gov.au/news/consultation-launched-position-australia-leader-digital-economy-regulation.

[6] Interim Report (2025), p. 18.

[7] Interim Report (2025), p. 20.

- Mandatory guardrails for AI in high-risk settings are only appropriate in circumstances where the gap analyses determined that existing regulatory frameworks or new technology-neutral regulations cannot adequately mitigate the risk of harm.[8]

These findings and recommendations present a solid set of principles on which the Government can build its approach to AI policymaking. BSA proffers the following recommendations to operationalise these principles and ensure that Australia's AI framework both promotes responsible innovation and maximises the productivity and competitiveness benefits of AI adoption.

Focus on identifying high-risk use cases of AI

We support the risk-based approach recommended in the Interim Report. The risks of AI are inherently use-case specific. Many AI systems pose extremely low, or even no, risk to individuals or society, while creating potentially significant benefits like helping to organise digital files, auto-populate common forms for subsequent human review, or improve a company's ability to forecast supply chain issues.

Generally, AI governance efforts should focus on addressing high-risk AI use cases based on potential harm. This approach assesses risk based on the AI system's application and intended use case, rather than the sector in which it is used or deployed. In this regard, BSA has encouraged policymakers to focus on AI systems specifically developed to make consequential decisions, which are determinations that have a material legal or similarly significant effect on a consumer's eligibility for and result in the provision or denial of housing, employment, credit, education, access to physical places of public accommodation, healthcare, or insurance. This prevents low-risk AI systems from being automatically classified as high-risk simply because they are used in a particular sector (e.g., healthcare).

Recommendation: In line with a risk-based approach, the Productivity Commission should make clear that the focus of the gap analyses is to identify high-risk AI use cases. This will ensure that any subsequent regulatory efforts are targeted at a set of specific use cases.

Recognise and define the different roles and responsibilities of entities in the AI supply chain

It is critical for the Government to clearly recognise and define the different roles and responsibilities of various actors in the AI supply chain. This is because AI systems are often developed, integrated and deployed by different organisations, each of which has access to different information and the ability to address different risks. Without clear role differentiation, regulatory obligations risk being either duplicative or misaligned, placing unrealistic compliance burdens on some actors while leaving actual risks unaddressed. In short, all actors in the AI supply chain should act responsibly, but legal requirements and best practices should be tailored to each actor's role.

- Several actors may comprise the AI supply chain. Important roles include:**Developer of High-Risk AI System:** An entity that: (1) designs an AI system specifically intended to be used as a high-risk system; (2) substantially modifies a high-risk AI system, or (3)

[8] Interim Report (2025), p. 21

substantially modifies a non-high-risk AI system so that it becomes a high-risk AI system. Consequently, an AI developer is well-placed to provide details on the intended purpose of the AI system, the capabilities of the AI system, known limitations, and risks of the AI system at the time of development, the data used to train the AI system, and how the AI system was evaluated prior to sale.

- **Deployer of High-Risk AI systems:** An entity that uses a high-risk AI system. Consequently, an AI deployer is well-placed to provide details on the purpose for which the AI system is deployed, transparency measures relating to affected individuals or end users (e.g., disclosures of how the deployer plans to use a customer's personal information), post-deployment monitoring, user safeguards, and measures taken to mitigate potential risks arising from the AI system's deployment. AI deployers may also have more insight into the data inputs during the system's use and the resulting outputs and other real-world factors affecting the system's performance.
- **Integrator:** Outside of developers and deployers of high-risk AI systems, the widespread use of General Purpose AI (**GPAI**) models to power applications and products has highlighted another important actor in the AI supply chain – integrators. Integrators are entities that: (1) connect their customers to third-party general purpose AI models using their own software or platforms; or (2) otherwise integrate GPAI models into products or services for use by third parties without substantially modifying the GPAI models. Consequently, integrators are well-placed to share relevant, non-sensitive information about the changes they make to the model to the next company in the supply chain so that it can understand the AI's capabilities and limitations once it is used in the real world.

Recommendation: The Productivity Commission should recognise these distinct roles and urge agencies to consider the differences among them when assessing appropriate responsibilities.

Officially designate a non-regulatory central coordinating body for AI policy

To ensure regulatory coherence and avoid duplication, the Productivity Commission should recommend that the Government designate a lead non-regulatory body with responsibility to coordinate AI governance and policymaking across sectors. Given the cross-cutting nature of AI, responsibilities can be fragmented across different agencies and regulators. The Interim Report acknowledged that "[t]he range of commonly-cited AI risks spans several Australian Government portfolios including health, consumer protection, criminal law, national defence, financial regulation, media regulation and intellectual property".[9]

While sectoral regulators will remain best placed to address risks in their respective domains, a central coordinating body is needed to ensure consistency in policy direction and avoid overlapping or conflicting requirements. Importantly, the coordinating body's function is not to draft regulations on behalf of agencies or sectoral regulators – rather, it should be setting the overarching policy direction, working closely with various Government stakeholders to coordinate regulatory approaches, and ensuring that AI governance across portfolios remains risk-based and proportionate.

[9] Interim Report (2025), p. 17.

Recommendation: The Productivity Commission should urge the Government to officially designate a lead agency or non-regulatory central coordinating body to oversee AI policy coordination, with a focus on preventing internal regulatory fragmentation and duplication.

Introduce a clear copyright exception for AI training

The Interim Report explores whether "current Australian copyright law is a barrier to building and training AI models"[10] and considers if "there is a case for a new fair dealing exception that explicitly covers text and data mining".[11] BSA supports the development of statutory exceptions, including a text and data mining exception (**TDM exception**), that permit AI training on lawfully accessed content.

AI training entails a process of teaching an AI system to make decisions or predictions by exposing it to large amounts of data. "Raw data" sources may include everything from machine-to-machine data (e.g., satellite transmission data) and international trade statistics to published materials, blog posts, website comments, and chat room logs. Because much of the content on the Internet is subject to copyright protection (which arises automatically upon creation of an original work), some raw data may include material covered by copyright.

"Raw data" must typically be subjected to a transformative data preparation process that disaggregates and converts data into a form that can be semantically understood by a computer. As part of this process, an AI development team semantically and structurally transforms the data through "tokenization," which involves breaking down a piece of text or data into smaller units (or "tokens") for purposes of computational analysis. At the end of this process, training data will often ultimately appear as a sequence of tokens that stretches across the entire AI corpus.

This training process does not infringe on copyright because it consists of computational analysis of mathematical correlations, patterns, and trends across tokenised variables. These mathematical relationships are not copyrightable, and the training process is not a consumptive use of expressive content. Rather, it is a functional process aimed at enabling machines to detect and model statistical relationships. In this sense, AI training is distinct from expressive uses of copyrighted works.

To provide greater legal certainty for copyright holders and AI developers alike, we urge the Productivity Commission to recommend introducing a clear copyright exception which can be applied for both commercial and non-commercial activities, like those in Japan and Singapore and under consideration in Hong Kong. Introducing the consequent legal certainty will facilitate investments in AI development and deployment in Australia while clarifying appropriate protections for copyright holders.[12] As the Government of Singapore explained when it introduced its "computational data analysis" exception (i.e., Singapore's equivalent of a TDM exception):

> *A specific exception for such activities is preferred to relying on the general open-ended fair dealing defence, as it promotes certainty and allows calibration of specific safeguards*

[10] Interim Report (2025), p. 24

[11] Interim Report (2025), p. 27.

[12] BSA recognises that some content owners want more say in how their content is used in or with AI. One way to reflect and respect those wishes is through "opt-out" tools. The development and use of such opt-out tools, and the standards governing them, are best handled through voluntary conversations between creators and AI developers and deployers, who collectively are better positioned to develop effective, consensus-driven technical mechanisms than the Government.

> *and conditions to address the concerns raised by [various stakeholders]. These include conditions to preserve and protect rights-holders' commercial interests and freedom to conduct business based on licensing and subscription models. For example, the exception will be limited to acts of copying and a user must have lawful access to the works and other subject matter that are copied. If certain material can only be accessed through a paid subscription, the user must pay for the subscription before using the material for text and data mining. The user also cannot distribute the material to anyone without such lawful access. The exception will also not prevent rights-holders from taking reasonable measures to maintain the security and stability of their computer system or network.*[13]

In sum, a well-crafted exception would: a) promote AI development and wider economic growth; b) facilitate research; c) allow Australia to maintain its competitiveness on the global stage and sustain its position as a hub for growth and investment; d) afford legal certainty to users; and e) strike an appropriate balance between copyright protection and reasonable use of copyright works.

Recommendation: The Productivity Commission should recommend that the Government introduce a clear statutory exception that applies to both commercial and non-commercial AI training conducted on lawfully accessed materials. Such an exception would provide businesses with the certainty to invest in AI development, strengthen Australia's competitiveness, and ensure that copyright holders' interests are preserved through lawful access safeguards.

Data Access and Sharing

BSA agrees with the Interim Report's observation that "the benefits of data sharing remain somewhat untapped in Australia".[14] The Interim Report also noted that, as part of efforts to give individuals and consumers better access to data that relates to them, governments around the world are developing new regulatory pathways to facilitate data portability and interoperability.[15] Indeed, 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:

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**).[16] However, under the Scheme, only Australian entities are allowed to apply for accreditation. Furthermore, private entities, including "individuals, bodies corporate,

[13] Singapore Copyright Review Report, January 2019, https://www.mlaw.gov.sg/files/news/public-consultations/2021/copyrightbill/Annex_A-Copyright_Report2019.pdf

[14] Interim Report (2025), p. 29

[15] Interim Report (2025), p. 37.

[16] 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).

partnerships, trusts and unincorporated entities" will not be able to apply for accreditation.[17] 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.

BSA notes that the Government has commenced a statutory review of the DAT Act, which considers the effectiveness of the DAT Act and whether its operations support improvements in public sector data availability, sharing and transparency.[18] This is a good opportunity for the 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.[19] 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.

Recommendation: The Productivity Commission should recommend expanding the DAT Act accreditation framework to allow applications from both private and non-Australian entities, provided they can demonstrate compliance with Australia's security, privacy, and data-handling requirements. This would increase the utility of the Scheme, maximise the value of public sector data.

Explore privacy-enhancing technologies

The benefits of data sharing must also be balanced against safety and privacy concerns. In this regard, BSA encourages the Productivity Commission to recommend that the Government explore the application of privacy-enhancing technologies and promote opportunities to further build value from the safe and responsible use of data. 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.

Recommendation: The Productivity Commission should recommend that the Government explore and support the adoption of privacy-enhancing technologies to supplement efforts to improve data access.

[17] 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.

[18] Statutory Review of the Data Availability and Transparency Act, August 2025, https://www.finance.gov.au/government/public-data/public-data-policy/statutory-review-data-availability-and-transparency-act-2022.

[19] 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.

Privacy

BSA has participated in multiple consultations on the review of the Privacy Act.[20] As currently formulated, the Privacy Act falls short of striking the right balance between protecting an individual's privacy and supporting beneficial, responsible data use. Importantly, we note the Interim Report's findings that "businesses may have not fully comprehended what their regulatory obligations were", which led to unnecessary "compliance" that impose additional costs on businesses without improving privacy outcomes.[21]

Such issues stem from the lack of an important distinction between data controllers and data processors, which is a foundational element of modern privacy laws globally.

Implement a controller-processor distinction

In brief, "data controllers" refer to entities which determine the purposes and means of processing personal data, whereas "data processors" are entities that handle personal data on behalf of controllers pursuant to their instructions. In its Response to the Privacy Act Review Report (**Response**),[22] the Government agreed-in-principle to the proposal to implement a clear distinction between controllers and processors in the Privacy Act. Indeed, the Government recognised that a key focus area of the Privacy Act review was to "increase clarity and simplicity for entities and individuals", and that introducing the controller-processor distinction would "bring Australia into line with other jurisdictions, reflect the operational reality of modern business relationships, and reduce the compliance burden for entities acting as processors".[23]

BSA strongly agrees with the Government's observations in the Response. The introduction of a controller-processor distinction is the most important proposal to emerge from the Privacy Act review. There are significant benefits to implementing this distinction under the Privacy Act:

- Adopting a distinction between controllers and processors will align the Privacy Act with privacy laws globally, including, but not limited to the European Union's General Data Protection Regulation (**GDPR**), California's Consumer Privacy Act (**CCPA**), and Singapore's Personal Data Protection Act (**PDPA**). This alignment will help Australian entities understand how their obligations under the Privacy Act map to their obligations under data protection laws in other major markets. It will also help entities streamline data protection and transfer practices across markets.
- Clearly distinguishing between the roles of controllers and processors also improves consumer protection and enhances regulatory certainty for businesses. As noted in the Attorney General Department's Privacy Act Review Report 2022 (**AGD Report**),[24]

[20] See: BSA Comments on Privacy Amendment Bill 2024, October 2024, https://www.bsa.org/policy-filings/australia-bsa-comments-on-privacy-amendment-bill-2024; BSA Comments on Australia Privacy Act Review Report 2022, April 2023, https://www.bsa.org/policy-filings/australia-bsa-comments-on-australia-privacy-act-review-report-2022; BSA Comments on Privacy Legislation Amendment Bill, November 2022, https://www.bsa.org/policy-filings/australia-bsa-comments-on-privacy-legislation-amendment-bill; BSA Comments on Review of Australia Privacy Act 1988, January 2022, https://www.bsa.org/policy-filings/australia-bsa-comments-on-review-of-australia-privacy-act-1988

[21] Interim Report (2025), p. 55.

[22] Government Response to the Privacy Act Review Report, September 2023, https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report

[23] Response (2023), p. 15

[24] Privacy Act Review Report 2022, February 2023, https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf

distinguishing between controllers and processors will "clarify consent obligations and assist with clarifying obligations in relation to any new individual rights (such as a right to erasure) that may be introduced following this review", and "help entities more effectively respond to data breaches".[25]

In the absence of a controller-processor distinction, both consumers and businesses face increased uncertainty. Consumers lack clarity about which entities are responsible for safeguarding their data and how to exercise their rights, while businesses lack clear guidance on their obligations, leading to potential gaps in accountability and compliance. Australia's Privacy Act will also remain an outlier among major jurisdictions. This means that both Australian businesses expanding into new markets and businesses looking to invest in Australia will need to navigate inconsistent privacy frameworks across multiple regions, which increases compliance costs and complexity.

In the context of implementing the controller-processor distinction, we further recommend the following:

1. Adopt definitions of controllers and processors that align with other important privacy laws. Under the GDPR, for example, a data controller is defined as an entity that "alone, or jointly with others, determines the purposes and means of processing personal data", whereas a data processor is defined as an entity that "processes personal data on behalf of the controller". The language provides a clear distinction between entities that decide how and why to collect an individual's personal data and entities that act on behalf of others to process personal information.

2. Clearly recognise that determining whether an entity is acting as a controller or processor is fact-based and context specific. A single company may act as a controller for some of its products and services (i.e., consumer-facing products) and as a processor for others (i.e., business-to-business services). Such a company should be subject to obligations the Privacy Act places on controllers when it acts as a controller and subject to obligations the Privacy Act places on processors when it acts as a processor.

3. Ensure that obligations for controllers and processors are appropriately tailored according to their roles. Controllers and processors should be subject to distinct obligations under the Privacy Act. Importantly, consumer-facing responsibilities, such as obtaining consent from individuals and responding to consumer rights requests, should be assigned to controllers rather than processors. This reflects the fact controllers are entities that decide how and why to collect a consumer's personal information. Processors should be subject to other obligations, such as requirements to safeguard personal information and to process personal information only on behalf of the controller and pursuant to its instructions. This allocation of responsibilities is also consistent with global norms.

Recommendation: The Productivity Commission should urge the Government to prioritise implementing the controller-processor distinction in the next tranche of Privacy Act amendments. This will involve: (1) adopting definitions of controllers and processors that align with other

[25] AGD Report (2023), p. 231

leading privacy laws; (2) clearly recognise that determining whether an entity is acting as a controller or processor is fact-based and context specific; and (3) ensure that obligations and controllers are appropriately tailored according to their roles. This will modernise Australia's privacy regime and provide more legal certainty for businesses and consumers. In this context,

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.

Yours sincerely,

Tham Shen Hong
Senior Manager, Policy – APAC