



28 February 2023

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

Re: Issues Paper: Inquiry into International Digital Platforms Operated by Big Tech Companies

Dear Sir / Madam,

Amazon Web Services Australia Pty Ltd (**AWS**) is pleased to provide comments to the Senate Standing Committee on Economics (**Committee**) on its *Inquiry into International Digital Platforms Operated by Big Tech Companies*.

Cloud services are a driving force for Australian business. Every day, our customers – including the fastest-growing startups, research institutions, health services providers, large enterprises, and government departments – safely use AWS to maximise the potential of the digital economy. We provide a powerful suite of services, from infrastructure technologies like compute, storage, and databases, to emerging technologies, such as machine learning and artificial intelligence, data lakes and analytics.

AWS is proud to play our part in building and operating the technology infrastructure and services to help Australian businesses and governments innovate, achieve greater productivity, and deliver better services. Many of our customers are owners or operators of critical infrastructure, and they choose AWS knowing that we prioritise security and resilience above all else.

Our submission aims to help the Committee better understand AWS, which will contribute to the Committee's mapping exercise of technology companies. We would like to comment on the themes covered in the Inquiry's Issues Paper and Terms of Reference, specifically where they relate to AWS and the cloud. In the sections below, we have set out the nature of our business, our contribution to the Australian economy, the secure and resilient nature of the cloud, algorithmic transparency, and the competitive cloud landscape.

AWS' investment in Australia

AWS launched in Australia in 2011 and opened its AWS Sydney Region in 2012, giving Australian enterprises, public sector organisations, start-ups, and small and medium-sized enterprises access to state-of-the-art cloud infrastructure. In the past decade, AWS has invested A\$8 billion in local infrastructure and jobs across Australia. This investment includes a workforce of more than 3,000. These workforce roles include machine learning scientists, sales and solutions architects, and data centre operators.

On 24 January 2023, AWS launched the [AWS Melbourne Region](#) – its second Australian infrastructure Region. The new Melbourne Region will offer our Australian customers additional architectural options including the ability to store backup data in geographically separated locations within Australia. As outlined in our Victorian Economic Impact Statement, we plan to invest A\$6.8 billion in the AWS Melbourne Region over the next fifteen years. This is estimated to support an annual average of over



2,500 full-time equivalent jobs at external businesses, and add A\$15.9 billion to the Australian gross domestic product by 2037. The AWS Melbourne Region will benefit businesses of all sizes, from banks, government departments and tech unicorns, to burgeoning start-ups and local small businesses.

Indeed, AWS is proud to help support the rapid growth in the wider Australian tech sector through our foundational investments in cloud infrastructure. Successful Australian tech companies such as [Atlassian](#), [Canva](#) and [Q-CTRL](#) all use AWS services to help power their businesses. In August 2022, the Tech Council of Australia reported that, in addition to significant economic contributions, large global tech companies including AWS's "global hyperscale cloud capabilities have enabled the emergence of Australian based SaaS platforms and supported Australian software companies to scale globally. This is important because tech companies are born with the intention of becoming global – operating in multiple regions and nations, having a diversified workforce and tapping into a global market of customers."¹ Further, the report found that it is crucial to maintain a supportive environment for continued investment by global tech companies in the Australian tech sector – particularly cloud and data centres – as Australia has the potential to attract a greater regional share of the cloud and data centres segment "if it can generate an abundance of cheap, renewable energy, maintain a level playing field for all companies in the tech ecosystem, and avoid protectionist policies that may deter investment."²

What is the cloud and what are the benefits of cloud computing?

Cloud computing is the on-demand delivery of IT resources via the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining their own data centres and servers, customers can acquire technology such as compute power, storage, databases and other services on an as-needed basis. It is similar to how consumers flip a switch to turn on the lights in their home, and the power company sends electricity. AWS manages and maintains the technology infrastructure in a secure environment, and businesses access these resources via the Internet to develop and run their applications.

The cloud is resilient

AWS infrastructure was specifically designed with operational resilience in mind. An AWS "Region" is a physical location where we cluster data centres. Each Region consists of a minimum of three, isolated, and physically separate "Availability Zones" within a geographic area. An Availability Zone is one or more discrete data centres with redundant power, networking, and connectivity. Availability Zones give customers the ability to operate production applications that are more highly available, fault tolerant, and scalable than would be possible from a single data centre. AWS customers are in complete control of where their data and workloads are hosted, and can choose to have their data stored and processed in one or more specific Availability Zones.

As noted above, the new AWS Melbourne Region offers our Australian customers additional flexibility, including the ability to store backup data in geographically separated locations within Australia. It also allows our Australian customers to run full primary and secondary sites onshore. This provides even greater redundancy, and improved latency by bringing key infrastructure closer to customers. Our infrastructure is connected via our redundant, high bandwidth and secure network connections, and we are proud to deliver the highest network availability of any cloud provider.

¹ The Tech Council of Australia, *Turning Australia into a Regional Tech Hub*, August 2022.

² Ibid.



The cloud is secure

Security will always be our top priority. AWS customers trust us to handle their data securely, and we honour our commitment to build and operate infrastructure that satisfies the security requirements of all organisations, from small startups to the most security-sensitive corporations and governments. To illustrate our commitment to the security and resilience of our Australian infrastructure, AWS's cloud service offering in our Australian Regions was granted Certified Strategic status under the Digital Transformation Agency's Hosting Certification Framework (HCF). In addition, over 130 of our services hosted in the Australian Regions are assessed through the Australian Signals Directorate's Information Security Registered Assessors Program (IRAP).

The rigorous security assessments we undertake with the Australian Government are also reflected globally. AWS supports 98 security standards and compliance certifications, more than any other offering, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping satisfy compliance requirements for virtually every regulatory agency around the globe. Our service offerings and associated supply chain are vetted and accepted as secure enough for top-secret workloads in the United States, which benefits all our customers globally – that is, AWS uses the same secure hardware and software to build and operate each of our Regions, putting our customers on the same confident footing around the world. This is backed by a deep set of cloud security tools, with over 300 security, compliance, and governance services and key features.

A fundamental element of our security model is the concept of shared responsibility, which is a common feature of the relationship between cloud services providers and their customers. AWS is responsible for protecting the infrastructure that runs the AWS services; this infrastructure is composed of the hardware, software, networking, and facilities that run the AWS services. AWS customers are responsible for building secure applications tailored to their needs using the tools and services available to them, but AWS is committed to supporting our customers with this. For example, our security field teams provide direct support and guidance to customers, helping them to maximise the security benefits of using AWS services. We also provide wide variety of best practices documents, encryption tools, and other guidance our customers can leverage in delivering application-level security measures. In addition, AWS partners offer hundreds of tools and features to help customers meet their security objectives, ranging from network security, configuration management, access control, and data encryption. We also encourage customers to deploy proactive services to not just detect unusual behaviour but immediately deploy mitigating actions, which are ready-to-use on AWS. Tools like Amazon GuardDuty, AWS Shield, and AWS Audit Manager enable customers to detect in real-time, mitigate, and verify their security posture.

Data Protection and Privacy

As we noted in our submission to the Senate Legal and Constitutional Affairs Committee last year on the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022*, AWS continues to support the Australian Government's objective to create comprehensive privacy laws that will protect individuals' personal information, whilst balancing an organisation's legitimate need to process that information. We look forward to engaging with the Attorney-General's Department consultation process on reforms to the *Privacy Act 1988*.

AWS has deep experience in implementing and complying with international privacy regimes. We know our customers care deeply about privacy and data security, and so we support the highest privacy standards and compliance certifications to satisfy the requirements of our customers around the world.



As we've innovated and expanded to offer the world's most capable, scalable, and reliable cloud, we've continued to prioritise making sure customers are in control and able to meet regulatory requirements anywhere they operate. What this looks like varies greatly across industries and countries.

AWS already offers a range of data protection features, accreditations, and contractual commitments that give customers control over where they locate their data, who can access it, and how it is used. We pledge to expand on these capabilities to allow customers around the world to meet their digital sovereignty requirements without compromising on the capabilities, performance, innovation, and scale of the AWS Cloud. At the same time, we will continue to work to deeply understand the evolving needs and requirements of both customers and regulators, and rapidly adapt and innovate to meet them.

We also recognise that an important objective of privacy laws is to encourage better internal data governance and improve information security hygiene-practices in organisations. As noted above, AWS is highly sensitive to the security needs of our customers and AWS is architected to be the most secure cloud computing environment available today.

Algorithmic Transparency

Artificial Intelligence (AI) applied through machine learning (ML) will be one of the most transformational technologies of our generation, tackling some of humanity's most challenging problems, augmenting human performance, and maximising productivity. Some applications of algorithms can be highly impactful on human life, while others can be trivial. In either case, the responsible use of these technologies is key to fostering continued innovation and the maintenance of trust in the systems they influence. AWS is committed to developing fair and accurate AI and ML services and providing our customers with the tools and guidance needed to build AI and ML applications responsibly.

AWS supports standards and frameworks, that raise the bar for the accuracy, fairness, safety, of AI/ML. We recognise that fairness is difficult to define and depends on the context. We also recognise that explainability remains a technical challenge and, therefore, we recommend a nuanced approach that considers the context for the deployment, and the circumstances when explainability is desirable, versus when explainability is required. We support AI governance efforts that take a risk-based approach to addressing the responsible use of AI, such as Australia's AI Ethics Principles, the OECD's AI Principles, and Singapore's AI Governance Framework. We encourage all governments considering these issues to consider aligning to such international best practices, where appropriate.

Skilling the Australian workforce

AWS strongly believes that the future of a prosperous Australia is tied to its digitally skilled workforce. Australia will greatly benefit from building and maintaining a strong population of technology professionals, and workers with digital skills across a range of job functions and industries. The entire Australian economy has been impacted by the growth in demand for digital skills. A 2021 study by AlphaBeta found that the average Australian worker will need to gain an additional seven new digital skills by 2025 to keep pace with technological change, and that Australia requires an additional 6.5 million newly-skilled and reskilled digital workers by 2025 to meet future demand for these technology skills.

AWS shares the federal government's vision of addressing the country's growing tech skills shortage by having [1.2 million people in tech jobs by 2030](#). We are committed to bridging the cloud skills gap in Australia, and have trained more than 300,000 people across Australia with cloud skills since 2017. We



offer a variety of educational, training and certification programs to help Australians develop digital skills and adopt cloud technologies, including partnering with universities such as RMIT.

Competitive landscape

Offering cloud services in Australia is highly competitive, with both global and domestic players serving a variety of customers across public and private sectors. The Inquiry's Issues Paper alone lists ten cloud providers in Australia, with many other businesses offering cloud services not mentioned. Cloud services are a small part of the global IT services market. The global IT services market is dynamic and characterised by frequent innovation and disruption from new and existing businesses, with low barriers to entry and frequent expansion and contraction of competing businesses. AWS faces intense competition from numerous providers of IT solutions with different delivery models; indeed, AWS's services represent only a small fraction of the global IT services market in which AWS competes.

Further, cloud computing technology is inherently interoperable, and customers are free to purchase multi-cloud and hybrid cloud options that best meets their needs. For each of AWS's offerings, customers have numerous alternatives, including cloud providers, on-premises hardware vendors, private data centres, hosted installations, co-located data centres, managed service providers, software providers, and hybrid solutions that combine these options. Customers can (and do) choose which service option or combination of service options would be appropriate for a given requirement based on factors such as their functionality, cost, interoperability, scalability, reliability, performance, availability, and support.

We note that the Issues Paper refers to service models of cloud computing such as "IaaS", "PaaS", "SaaS" and "FaaS". We do not recommend using these categories as frames of reference when discussing cloud services, as they do not reflect actual competitive dynamics for cloud and other IT services. First, the categorisation of cloud services into these categories does not reflect how customers generally purchase IT services. Customers do not typically evaluate products or services based on these categories. Instead, customers typically start by defining their objectives and needs, and then look at a broad set of options that might help meet them. Second, modern IT services do not fit neatly into the concepts of "IaaS", "PaaS" or "SaaS". AWS offers a variety of individual IT services that customers use to build their IT solutions. These offerings are diverse, and customers use them individually and in combination for numerous use cases. Third, the IT industry does not have a common definition for these terms, and definitions vary from company to company, and among industry groups depending on who writes them. In fact, Gartner has stopped basing its magic quadrants on IaaS and PaaS, recognizing that these categories do not adequately reflect the changing dynamics of cloud services and the ways that customers adopt them.

The Issues Paper also refers to the UK Ofcom's cloud services study, and the concept of a cloud "ecosystem". Practically, cloud services are not sold or purchased in or as an "ecosystem" – customers are free to use a wide variety of open source and proprietary technologies of their choice, and freely choose the operating system(s) they will run. They can build their entire technology application based on open standards, open source, and readily portable container technologies to enable them complete freedom to run anywhere and to reach any end user.

Finally, under AWS's standard terms, customers are free to terminate their use of AWS at any time by a simple click of a button in their online account, with no termination fees. AWS has put in place measures to facilitate migration of customers who choose to change their service providers. These measures include the provision of tools to customers to assist migration, contractual terms that enable customers to start



or stop using AWS services whenever they choose, AWS's approach to pay-as-you-go pricing, and the absence of egress fees (i.e., fees charged specifically for terminating use of AWS's services and migrating to another provider). AWS also educates its customers on building their IT solutions in a way that they can retrieve and move data from one IT environment to another.

Regulatory reforms

The cloud sector is already highly regulated. While AWS supports legislation that can better promote an Australian digital economy, Government should be mindful of the risk of unintended consequences of new regulation, including possible reduction in legal certainty and barriers to innovation and investment.

A significant number of relevant policy and regulatory reforms are already underway or were recently implemented in Australia (including reforms to the *Privacy Act 1988* (Privacy Act), the 2023-2030 Australian Cyber Security Strategy, Australia's foreign investment review framework, critical infrastructure legislation, and the Australian Government's Hosting Certification Framework). Some of these reforms have only recently commenced implementation while others are out for consultation and/or in the early stages of development. As far as possible, Government should allow time for stakeholders to properly consult on the proposed reforms and allow time for the reforms to take effect. This ensures that the effectiveness of these recent reforms can be taken into account before considering whether further new reforms are needed and then working with industry to co-design solutions to address any remaining issues.

The Issues Paper also refers to legislative proposals or reforms overseas. These developments are new and experimental, and the risks and benefits of these proposals and reforms are largely untested and unknown. These reforms are also a response to the specific legal, economic and political context of those countries, which can differ markedly to the Australian context. It would be prudent for the Committee to observe how these developments unfold first, before considering the question of whether they are suitable for the Australian context.

AWS welcomes the opportunity to work with the Committee to foster a deeper understanding of the cloud sector and the benefits AWS delivers to customers and the economy overall. AWS is also pleased to continue to work with the Government on its various existing proposed reforms. For example, AWS continues to closely engage with the Attorney-General's Department on [updates to the Privacy Act 1988](#), and looks forward to engaging through the current consultation on Australia's privacy frameworks. We also look forward to working with the Department of Home Affairs' refresh of its Cybersecurity Strategy, and will continue to work closely with the Department of Home Affairs on Australia's revamped critical infrastructure legislation. AWS also remains closely engaged with the Office of the eSafety Commissioner and its drafting of Online Safety Codes.

Thank you for the opportunity to provide our comments. We look forward to working with the Committee to help shape a safe and prosperous digital future for all Australians.

Kind regards,



Roger Somerville
Head of Public Policy, Australia and New Zealand
Amazon Web Services