Senate Standing Committee on Economics
Committee Office, Department of the Senate
Parliament House, Canberra ACT 2600

5 September 2023

Dear Secretariat

Following my appearance before the Committee on 22 August, Microsoft is pleased to provide supplementary information taken on notice during the hearing.

As we outline in our submission to the inquiry, understanding the vast variety of business models in the tech sector is critical to understanding how regulation and policy impact various products and services. Microsoft has over 200 different products and services with different types of business models. We tend to think about them in two distinct categories – our consumer based products which have a distinct connection between Microsoft and the end user – (for example Xbox, Outlook.com, Bing) and our enterprise services where Microsoft's relationship is predominantly with a business or public sector customer, and there is no direct connection between Microsoft and the end-user – for example, our cloud offerings of which more information can be found here -Azure.

Critical infrastructure legislation

In terms of the critical infrastructure legislation (Systems of Critical Infrastructure Act) Microsoft is a certified strategic provider under the Government's Hosting Certification Framework. In addition, we fall within the definition of a data processing and storage sector according to the Act and the SOCI Definitions Rules. Microsoft has met the initial requirements of the SOCI Act however we continue to engage with the Department of Home Affairs over implementation and reporting requirements going forward.

The scope of Microsoft's services captured by legislation is defined by the Act and the Asset Definition Guidelines. Under the Definitions Rules of the Systems of Critical Infrastructure Act, a data storage and processing service is deemed a critical infrastructure asset.

Microsoft Azure (Australia regions) is deemed both a critical infrastructure asset as a part of the data storage and processing sector as well as a Certified Strategic provider under the Hosting Certification

Framework. This requires Microsoft to have and maintain a risk management program for its three Australian Microsoft Azure Cloud regions, adhere to mandatory cyber security incident reporting, and an obligation to notify data service providers where applicable.

Dispute resolution processes

In terms of our dispute resolution processes for our cloud services, the Microsoft Business and Services Agreement ("MBSA") which governs commercial licensing arrangements for Microsoft Products and Professional Services offerings, as a standard position, sets out the applicable venues for which an action arising under the agreement may be brought by the commercial parties.

Many of Microsoft's commercial licensing arrangements, including where requested by commercial customers, also contain additional dispute resolution processes or steps to be adhered to between the commercial parties prior to commencing any court proceedings. This includes the disputing party notifying the other party of the details of the dispute within a set number of days, followed by senior executives of the two parties meeting to try to resolve the dispute within an agreed period. Wherein if the dispute remains unresolved, the matter is further escalated to the company's executives to meet and try to resolve within an agreed period, before proceeding on to further alternative dispute resolution processes (i.e. mediation) if the dispute is still unresolved, prior to the respective party's decision to commence court proceedings.

The Microsoft Services Agreement covers our consumer services. Due to the varied nature and scope of potential issues which may arise in relation to these products, Microsoft takes a contextual approach to the handling of consumer disputes which may arise. More information can be found here on consumer rights under Australian Consumer Law. Where a dispute or complaint arises in relation to a defective product, Microsoft makes available a direct line to contact Microsoft. Additionally, there is the ability for Australian consumers to provide feedback through a dedicated feedback form to file a complaint. Depending on the nature of the complaint or dispute, dispute resolution and escalation steps are often overseen by dedicated support teams, who work closely with other divisions within the organisation, including Microsoft's product, compliance, and legal functions.

Right to delete

With regard to the right to delete, for Microsoft's enterprise customers, Microsoft's Data Protection Addendum, which sets forth the parties' obligations with respect to the processing and security of Customer Data and Personal Data in connection with Microsoft's Online Services, clarifies that customers, at all times during the term of the customer's subscription, will have the ability to access, extract and delete customer data stored in each Online Service. Additionally, Microsoft retains Customer Data that remains stored in Online Services for 90 days after expiration or termination of a Customer's subscription so that the customer may extract their data.

For Microsoft's consumer customers, the Microsoft Service Agreement covering the use of applicable Microsoft consumer products, websites and services, makes reference to Microsoft's Privacy Statement which further describes the types of data Microsoft collects from consumers and consumer devices ("Data"), how Microsoft uses that Data, and the legal basis Microsoft has to process the consumer's data. Consumers can access and control their personal data that Microsoft has obtained either through tools Microsoft makes available to consumers, or if not available through such tools, by contacting Microsoft for assistance with access to, erasure of, and updates to their personal data as processed by Microsoft.

Revenue from sales to Government

Whilst Microsoft does not breakdown its revenue by Government as a category, our analysis of enterprise revenue for FY23 shows roughly 6% would be deemed as coming from Federal Government agencies and a further 25% from State Government.

Data residency

In terms of where Microsoft Australian customers store their data, enterprise customers can take advantage of cloud services from our Australian data centres, including Microsoft Azure, Office 365 and Dynamics 365. With the exception of a very small number of products, customers decide where their data resides. There are no default locations on Azure. A key step in every customers' use of Azure is deciding which region they want their data to reside in. If a customer wants to back it up in another region or country that is the customers decision and they have full control of this. There is different pricing based on how you purchase (pay as you go or pre-paid) and your choice of data location – which can be found here. The differences in pricing relate to the different operating costs such as power prices in different jurisdictions. You can find out more about data location here Cloud Data Integrity at its Finest | Microsoft Trust Center. The majority of Australian customers elect for their data to reside closest to their operating location which for the most part is in Australia – however some customers who operate offices or operations in other parts of the world may choose for their data to reside in those jurisdictions.

Microsoft's consumer online products and services are subject to the Microsoft Services Agreement. A full list of the covered products and services is available here. The Microsoft Privacy Statement as further referenced under the Microsoft Services Agreement further describes the types of data Microsoft collects from consumers and consumer devices, how Microsoft uses that data, and the legal bases for processing that data. Consumer Data residency location is dependent on the product or service, and a range of factors including the consumer's billing address, service performance requirements and capacity.

Human Rights Watch report

Human Rights Watch (HRW) published a report of research they had done into privacy implications of several educational applications and services that governments around the world recommended for use by students during the COVID-19 global pandemic in April 2022. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments.

The report included analysis of two Microsoft-published applications for Android devices, Minecraft: Education Edition and Microsoft Teams, and other services offered by Microsoft. The report encouraged EdTech providers, education ministries, and governments to take specified actions to protect the privacy and rights of minor children who may use the software and services provided or recommended by them.

Prior to publication of the report, HRW reached out to Microsoft with questions about some of the apps that it was reviewing for the publication. Microsoft responded, but much of the material provided in Microsoft's responses were not reflected in HRW's initial report.

The initial report published by HRW included inaccurate claims regarding Microsoft Teams and Minecraft: Education Edition. Microsoft is pleased that HRW has been willing to review information that Microsoft has provided to them prior to and since publication, and has corrected the published

report to more accurately reflect how those applications process data. Details of the corrections are provided below.

The initial publication reported the Microsoft Teams makes significant amounts of personal data from its users, including sensitive data such as precise location data, contacts list, and profile photos to third parties including to Google's Firebase Analytics. It also reported that it was unaware of any legitimate reason for Teams to request access to precise location information.

Microsoft provided information to HRW verifying that Microsoft Teams does not use Google Firebase Analytics (but does use Google Firebase Cloud Messaging to deliver push notifications, including notifications of incoming Teams calls, to Teams for Android users), and reminded HRW that it had provided information prior to publication that Microsoft Teams supports calling to telephone numbers, and as such is required by law to support emergency calling, and to provide precise location data to emergency call centers when a user makes an emergency call using Teams. HRW has published corrections regarding these errors in its initial publication.

Microsoft's approach to children's data

Microsoft is supportive of HRW's objective to encourage greater recognition of and support for the privacy rights of children when using applications for education. Microsoft provides industry-leading software and services supporting education, which include industry-leading privacy controls and protections. The terms under which Microsoft offers its software and services to educational institutions includes strong commitments with respect to privacy and data protection. When licensing Microsoft 365 cloud services, educational institutions assume the role of data controllers and Microsoft, as the service provider, acts as a data processor where our services act on the instructions of the account administrators and individual users (students) licensed to use those services through their schools. The terms of Microsoft's Data Protection Addendum, provides enterprise-grade data protection commitments to schools, districts, and ministries that use Microsoft 365 services.

Specifically

- Microsoft's services provided specifically for educational or other enterprise use do not use user data for user profiling or behavioural advertising. Products expected to be used by children for educational purposes limit the processing of user data to what is necessary to provide the services described in product documentation.

- Under Microsoft's enterprise Online Product Terms Microsoft commits that it will not share user data with third parties except those that are (a) disclosed in advance in its published list of data subprocessors and (b) bound by contracts with Microsoft to strictly limit their processing of data received from Microsoft

- As a general practice, any personal data that Microsoft receives through its educational products is handled with enhanced protections that are appropriate for handling of children's personal data, and Microsoft requires third parties to whom such personal data may be transferred to apply the same level of enhanced protections to that personal data regardless of the age of the users involved.

- In products designed for use by children, Microsoft does not collect precise location data, advertising identifiers, or similar sensitive data.

The Microsoft Privacy Statement has been written to be understood by those who are legally competent to enter into binding agreements. Additionally, to help younger audiences understand the data Microsoft collects and their rights related to that data, Microsoft provides a Privacy for young people page that provides much of the same information as the Microsoft Privacy Statement.

Information about how to access and control personal data collected by Microsoft and how to contact Microsoft with concerns about our data processing related to your personal data or your Microsoft accounts is available in the Microsoft Privacy Statement and the Privacy for young people links above.

Role of US tech companies in supporting the growth of the Australian tech ecosystem
Finally, Microsoft, LinkedIn and the Tech Council of Australia recently released some research on How Us tech workers boost the growth of Australia's tech ecosystem which we believe goes to the terms of reference of the inquiry and may be helpful to the Committee. The report can be accessed here.
Thank you for the opportunity to provide this supplementary information to support our submission and oral evidence.

Yours sincerely

Belinda Dennett
Corporate Affairs Director