5th April 2023

Australian Competition and Consumer Commission (ACCC)
23 Marcus Clarke Street Canberra ACT
GPO Box 3131 Canberra ACT 2601
Email: digitalmonitoring@accc.gov.au

Subject: Expanding Ecosystems Of Digital Platform Service Providers

Dear Digital Platforms Committee,

We are writing in response to the Issues Paper published on 8th March 2023 regarding the expanding ecosystems of digital platform service providers as part of the five-year Digital Platform Services Inquiry. As an Australian technology company, Vault has vast amounts of experience dealing with the issues raised in the Issues Paper and providing detailed responses based on the available information. Therefore, we are pleased to share our expertise on this issue with the Australian Competition and Consumer Commission.

We understand that the ACCC's main job is to watch over competition, manage industries, and defend and support consumer rights. As more digital services and connected products from big foreign tech companies (known as 'Big Tech') become common in our country, we think the Government needs stronger control and rules. This will help deal with issues related to money, competition, privacy and control over data, and safety for Australian customers/businesses.

Interoperability

With the exception of Google, Big Tech has intentionally limited their use of Open Source Open Standards for Interoperability in order to increase their market dominance and increase customer “stickiness”.

Once having called Open Source a “cancer”, Microsoft is improving in some parts of their business but their cloud platform Azure is fundamentally a proprietary platform with significant lock-in. In recent times Mirosoft has acquired a company called OpenAI (known for ChatGPT). OpenAI was a company that built open, interoperable AI platforms for the benefit of society. Since Microsoft's acquisition, the platform is no longer open and has been made proprietary.

Amazon’s cloud platform, AWS, does at first seem to have some services that are based on open or interoperable systems, however it has been Vault’s experience that AWS has “forked” open and interoperable components resulting in more vendor lock-in.

We submit that lack of regulation in this area has resulted in vendor lock-in that has no benefit to the consumer. Additionally and adversely, this results in an ability for these organisations to rent seek.

Systemic Advantage

Incubance provides an insurmountable advantage for Big Tech to launch an inferior product successfully. Big Tech regularly subsidises new products into a market until the existing competition is either acquired or extinguished. Big Tech has even gone further to either bundle or extort their way to dominance. For example:

- On 14th July 2021, Microsoft announced that it would only provide support and security updates to Windows Server 2012 if hosted on Azure. There are no technical reasons for this, however it results in any customers of other cloud providers needing to move some of their workloads to Azure. Such a direct abuse of market power has gone without regulatory action. This example alone has caused material consumer and competitive damage to the Australian market.
- Microsoft's Service Provider Licensing Agreement (SPLA) has recently settled a discriminatory pricing complaint with the European Commission's (EC) antitrust arm. Again, we are seeing no regulatory action from the ACCC in the Australian market.
- Amazon's AWS released systematic programs that subsidise deals at early stages which are followed by rent seeking through lock-in. This includes subsidies in the $5,000 to $100,000 range for startups (AWS Activate) through multimillion dollar subsidies to buy large chunks of business (AWS Data Centre Migration). Big Tech can be found openly breaching anti competitive rules without consequence from the ACCC.

Economic Impacts

The ACCC should examine the impact of the concentration of market power by Big Tech companies on Australia's sovereign capability in the technology sector. It should investigate how the dominance of these companies may impact local technology companies and limit their ability to compete in the market. It should also consider how this concentration of market power may impact Australia's ability to develop and stimulate innovation in key areas, such as artificial intelligence, cyber security, and data analytics, which can create new industries and increase competitiveness in global markets.

Furthermore, the ACCC should consider how Australia can build and maintain its own sovereign capability in the technology sector. This could include exploring opportunities for local companies to innovate and compete in the market, investing in research and development, and promoting the development of local technology ecosystems.

Data Sovereignty, Control and Jurisdiction

Data sovereignty is an important concept that should be investigated by the ACCC on the nature and extent of international digital platforms operated by large overseas-based multinational technology companies, 'Big Tech'.

The issue of data sovereignty is particularly relevant to the ACCC because the collection and processing of data by Big Tech companies often involves the transfer of personal data across borders, which can have significant implications for privacy, security, and national sovereignty.

Data sovereignty is vital for building the public's trust in the Government and commercial markets. To access vital services and benefits, personal information must be divulged and recorded. Often, there is little to no choice in what personal information is stored by the Government. The public, therefore, has a higher standard for Government when it comes to the management of personal data. When people provide personal data to the Government, there is an expectation that this data will be stored and managed within Australia.

Data sovereignty is a growing concern for Australians. The Federal Government Information Commissioner's Australian Community Attitudes to Privacy Survey 2020 states that 74% of Australians consider it to be "a misuse of personal information" if their data has foreign processing access — an increase from 68% in the 2013 survey.

Further, the same report shows, many Australians see loss of data sovereignty being the single biggest issue with 41% of people believing sending data to foreign companies or countries is the biggest risk to privacy today. 92% of Australians have some concerns about the sovereignty of their personal data.

Data sovereignty refers to the concept that data is subject to the laws and governance of the country in which the data originated. In order of importance, the main sub constructs of data sovereignty are:

- Legal - the data is subject solely to the laws of the country of data origin. Generally, this means that the custodian must be owned and operated within the country.
- Operational - data, metadata, monitoring and remote access are managed solely within the country of the data's origin.
- Physical - the data at rest and in transit remains within the originating country.

When in-country data is stored on services, which are subject to foreign laws, an organisation retains substantial legal obligations concerning that data's protection. However, the information may no longer be under their control and could be impacted by the laws and actions of a foreign country. This includes the future (as yet unwritten) laws of a foreign country. While the privacy laws of foreign countries may align to Australia's today, there is no certainty that they will do so in the future. At present, some countries have sectoral coverage, while others have omnibus law, with at least one national data protection law in addition to sectoral regulations. In Europe, under GDPR a citizen must be informed if their data is subject of foreign law and have the right to opt-out of non-sovereign services.

Protecting Australian Citizens:

The ACCC should examine the impact of Big Tech companies on the safety of Australian citizens and consider the potential risks posed by the integration of multiple services, products, and hardware within Big Tech companies' own ecosystem, particularly in the context of the collection and processing of personal data, the integration of multiple services, and the use of algorithms.

The ACCC should examine whether the algorithms used by these platforms lack transparency and contribute to greater concentrations of market power, which may pose significant risks to the safety

of Australian citizens. The ACCC should investigate how regulating this behaviour could lead to better outcomes in the public interest and promote the safety of citizens.

It is crucial to ensure that the regulatory framework is sufficient to address these risks and to promote the safety of citizens.

Australian Democracy

The inquiry should examine the impact of Big Tech companies on Australia's democratic processes, particularly in the context of the increasing power and influence of these companies over public debate and the dissemination of information. The market shares of these international digital platforms across the provision of hardware and software services may have significant implications for the plurality of voices in public debate, with potential negative impacts on the quality of democratic discourse.

ACCC's Digital Platforms Branch, should also consider whether regulatory frameworks are adequate and effective in addressing the concentration of market power and potential threats to democracy. Ultimately, the inquiry should provide recommendations for how Australia can protect its democratic processes and promote a fair and diverse marketplace of ideas.

Government Influence

Our experience has been that Big Tech has a disproportionate influence on Government officials and regulators. Below are a few examples in recent years.

- Under Minister Robert, the DTA has successfully lobbied to change the Hosting Certification Framework (HCF) to remove Sovereignty requirements despite the purpose of the HCF to provide a transparent assurance framework to ensure Sovereignty after an Australian strategic asset was purchased by Chinese buyers.
- Taxation loopholes have been created, such as transfer pricing, which resulted in Big Tech paying negligible Australian tax. This creates a persistent pricing advantage for Big Tech.
- The DTA established Whole of Government Agreements that explicitly favour Big Tech and directly disadvantage local providers (100% of Whole of Government Agreements are still with multinationals).
- The Australian Signals Directorate awarded several Big Tech providers "CCSL" certifications while explicitly, in documented form, not meeting requirements while requiring non-Big Tech providers to meet these same requirements.
- Foreign interference reports about Big Tech go uninvestigated.

Regulatory Inadequacy

It is also important to consider the adequacy and effectiveness of recent attempts, in Australia and internationally, to regulate the activities of these international digital platforms. The ACCC should examine whether the current regulatory frameworks are sufficient to address the growing concentration of market power and potential threats to democratic processes.

Based on the historical track record, if the ACCC were to take action against Big Tech we would expect the outcome to be nothing more than an inconsequential slap on the wrist. We ask, how does the ACCC propose to remediate the actual harm caused? To level the playing field, the ACCC would need to consider penalties greater than 50% of global market capitalisation of the offender or issue compensation to the companies that lost out at several times their current market capitalisation.

We believe that the ACCC's historical performance indicates that it may not possess the necessary leadership, resolve, and political support to effectively tackle the widespread and systemic issues arising from the global multi-trillion-dollar market abuses.

In conclusion, it is our view that the expansion of the digital platform ecosystems operated by large overseas-based multinational Big Tech companies exerting power and influence over markets and public debate, to the detriment of Australian democracy and users, could have far-reaching implications for the Australian economy and society. It is therefore essential that the ACCC Digital Platforms Branch examines all relevant issues and potential solutions. We hope that the ACCC finds this response helpful in shaping the scope and focus of the inquiry.

Yours Sincerely,

Rupert Taylor-Price
CEO