THE SENATE

Senate Economics References Committee

Inquiry into international digital platforms operated by Big Tech companies

Issues Paper:

Executive Summary

Issues Paper—Executive Summary

This Executive Summary provides a short overview of the Issues Paper. For the sake of brevity, it does not include the consultative questions for submitters to address.

Mapping Big Tech

The Committee wishes to undertake a mapping exercise to map out the different types of Big Tech companies. The Committee is seeking input on how best to categorise the various tech companies. This could be used to determine what type of regulation might be required.

The topics canvassed in the paper provide an insight into some of the areas the committee is interested in examining more closely. The topics reviewed in this paper are:

1) **Market concentration**
2) **The cloud**
3) **Algorithms and transparency**
4) **Data and privacy**
5) **Children's safety**
6) **The Metaverse**
7) **International**
8) **Big Tech disinformation**

Market concentration

- The issues paper notes the high concentration of market power of the Big Tech companies and how they potentially distort market through their activities and algorithms.
- Big Tech has increasingly engaged in a practice called 'vertical integration'—i.e. companies use to control their own suppliers, distributors or retail stores in order to control their value or supply chain.
    - Vertical integration can lead to a societal loss in the form of monopolisation of markets and manipulation of prices, which would be detrimental to customers.
- Big Tech has the ability and the incentive to favour their own first-party apps at the expense of rival third-party apps—known as self-preferencing—and that such conduct may have anti-competitive effects on downstream markets.
    - Self-preferencing may entrench market power, limit consumer choice, and reduce potential for innovation in the markets in which they compete.
- The evidence about Big Tech and small business is mixed. In some cases, Big Tech is viewed as a negatively impacting small businesses through anti-competitive business practices and, in other cases, facilitating small business opportunities.

The cloud

- The cloud refers to servers that are accessed over the Internet, and the software and databases that run on those servers. Big tech companies are increasingly using cloud deployments to provide their services.
- The cloud market is dominated by a small number of large players. The top 10 cloud service providers globally in 2022 are: Amazon Web Services (AWS); Microsoft Azure; Google Cloud Platform (GCP); Alibaba Cloud; Oracle Cloud; IBM Cloud (Kyndryl); Tencent Cloud; OVHcloud; DigitalOcean; and Linode (owned by Akamai).

    - AWS, Microsoft Azure, and GCP have the largest market share, collectively capturing over 65 per cent of spending on cloud infrastructure services.
- Below is a non-exhaustive summary of the challenges for 'cloud' computing:
    - Security issues
    - Governance/Control
    - Compliance
    - Performance
- Governments are beginning to respond to the regulatory challenges.
    - For example, Ofcom, the UK regulator for the communications services, has sought input on how the market is developing and the nature of competition, particularly in cloud infrastructure services and cloud ecosystems.

Algorithm transparency

- Computer algorithms are being deployed in ever more areas of our economic, political and social lives. The decisions these algorithms make have profound effects in sectors such as healthcare, education, employment, and banking.
    - The expansion of algorithms into public decision-making processes calls for a concomitant focus on the potential pitfalls associated with the development and use of algorithms, notably the concerns around potential bias.
- The Association for Computing Machinery US Public Policy Council (USACM) advocated the following principles:
    - Awareness
    - Access and redress
    - Accountability
    - Explanation
    - Data provenance
    - Auditability and testing
    - Validation
- The United States Congress has recently seen a significant number of bills being considered to regulate algorithm use, with more than 30 bills introduced to both Houses during 2021.
- The legislative proposals have two main points in common:
    - Expanded role for the Federal Trade Commission (FTC):
        - There appears to be no equivalent role undertaken for specific regulation of this matter in Australia; and
    - Section 230 reform:
        - This provision in the *1996 Communications Decency Act* generally provides immunity for website platforms that publish information from third-party content. Legislators from both parties have called for Section 230 to be altered or overhauled.

Data and privacy

- The digital age has brought with it extraordinary advances, but it has also created new threats to consumer privacy.
    - 'Data mining' allows companies collect large amounts of data about consumers and use it to target advertisements. Many tech companies are now using sophisticated methods to track their customers, both online and offline.
        - These profiles are extremely valuable to companies, who use them to target ads, sell products and influence behaviour.
- The Australian Competition and Consumer Commission (ACCC) is looking at regulatory options. The Digital Platform Services Inquiry interim report of September 2022 examined regulator options with regard to data collection restrictions in Australia.
- The exposure of the personal data of millions of Optus and Medibank Private customers, in September 2022 and October 2022 respectively, highlighted concerns in Australia:
    - Approximately 1.2 million Optus customers had their personal information compromised through a cyber-attack; and
    - Medibank Private also acknowledged that it too had been the target of a successful cyber-attack. Hackers accessed the personal information of millions of current and former members.
- In 2021, the Morrison Government introduced laws to allow the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to access data disruption warrants. However, the ACIC does not currently have the power to have to address the issues raised by the Optus and Medibank experiences.
- As part of the European Union's (EU) efforts to keep data safe online, the General Data Protection Regulation (GDPR) was introduced which contained new data protection requirements.
    - The provisions are consistent across all twenty-eight EU member states. However, standards are quite high and require most companies to make a large investment for their implementation.
        - While the GDPR has significantly improved the privacy rights of millions inside and outside of Europe, it hasn't eliminated the worst problems.
        - Civil society groups have grown frustrated with GDPR's limitations, while some countries' regulators complain the system to handle international complaints is bloated and slows down enforcement.

Children's safety

- The risk of using computers, mobile phones and other electronic devices to access the internet and social media is that breaches of privacy may lead to fraud, identity theft and unauthorised access to personal information. Other risks include image-based abuse, cyberbullying, stalking and exposure to unreliable information or illicit materials.
- Australia's eSafety Commissioner, Ms Julie Inman Grant, stated:

> As more companies move towards encrypted messaging services and deploy features like livestreaming, the fear is that this horrific material will spread unchecked on these platforms. Child sexual exploitation material that is reported now is just the tip of the

iceberg—online child sexual abuse that isn't being detected and remediated continues to be a huge concern.[1]

The Metaverse

- Many experts consider the Metaverse a 3D model of the internet where a place exists, parallel to the physical world, where you experience a digital life through avatars. The Metaverse is new and is still being developed. It is unclear what the Metaverse will look like. It could bring content to those in ways never before imagined and, with it, legal issues and challenges never before contemplated.
- Potential emerging issues with the Metaverse are listed below. This list is indicative and not exhaustive.
    - Identity
    - Addiction and mental health
    - Privacy & data security
    - Currency and digital payments
    - Law and jurisdiction

International

- Investment from the United States (US) in Australia has, in the past, been very significant and continues to be today.
- This is also reflected in US Big Tech investments in Australia. As examples, there are five large US tech companies that have expanded into Australia:
    - Reddit
    - Google
    - Square
    - Airbnb
    - Dropbox
    - Eventbrite
- Platforms and companies from the People's Republic of China (PRC) have also come to Australia generating interest from consumers and government authorities alike—particularly TikTok.
    - There is concern over the information that TikTok may share with the Chinese Government. Once governments obtain access to data owned by companies, they could leverage this in three main ways:
        - learning more about citizens and foreigners;
        - intellectual property theft; and
        - highly targeted influence campaigns.
- These concerns are being reflected internationally:
    - US: Donald Trump signed an executive order that blocked people from downloading the app, which was followed by an order for TikTok to sell its US

[1] 'Tech platforms asked to explain how they are tackling online child sexual exploitation, *eSafety Commissioner*, 30 August 2022, https://www.esafety.gov.au/newsroom/media-releases/tech-platforms-asked-explain-how-they-are-tackling-online-child-sexual-exploitation, (accessed 12 October 2022).

business. President Biden revoked the orders and instead directed US agencies to protect the data of people in the US from foreign adversaries;

- India: where TikTok had more than 200 million users, the government in September 2020 banned the platform and dozens of other Chinese apps;
- Ireland: the data protection watchdog launched an investigation into: "transfers by TikTok of personal data to China and TikTok's compliance with the GDPR's requirements for transfers of personal data to third countries"; and
- UK: Parliament shut down its TikTok account this August after a lobbying campaign by Conservative politicians.

- The emergence of Bitcoin, Ethereum, and other so-called cryptocurrencies in the past 15 years has opened another front on the internet/Big Tech evolution. Governments and regulators are still grappling with how best to deal with it.
  - The emergence of Central Bank Digital Currencies (CBDCs) issued by states that do not share Australia's liberal-democratic values, highlights the need for consumer protections.
  - Cryptocurrencies have proven themselves to be very volatile. Bitcoin, for example, went from a peak of US$68,000 in November 2021, to US$16,000 just one year later.
  - Cryptocurrency exchanges have in some cases collapsed with shareholders and customers losing significant amounts of money.
    - The most notable of these was FTX, which collapsed in November 2022.
- Stablecoins are a digital currency that is pegged to a 'stable' reserve asset like the US dollar or gold and are designed to reduce volatility.
  - However, this has not always been the reality. For example, there is the recent collapse of the algorithmic stablecoin Terra in the United States. It is estimated that US$60 billion of wealth was destroyed in a 'digital run'.
  - Nonetheless, stablecoins could be a solution to addressing the major problem that 1.7 billion people face: they have no banking services available to them.
- One response of government is that central banks have begun examining the idea of an official digital version of the national currency—the Central Bank Digital Currency (CBDC). As part of this, regulators need to consider the privacy/big state implications. There are numerous privacy issues that could outweigh the benefits.
  - The e-Yuan from the PRC is the first CBDC to be issued by a major economy, and China's financial influence is particularly relevant in the Pacific region.
  - There is a clear link between the Chinese CBDC and Chinese financial institutions and Big Tech organisations. Chinese owned companies in Australia, such as Alipay, lets Chinese tourists use their mobile phones to pay in their own currency, while merchants receive their funds in Australian dollars.
  - Chinese state-owned banks are primary disseminators of the e-Yuan via digital wallets. If the e-Yuan was introduced into Australia, Chinese state-owned banks would be the main payment facilitators.
- Future legislation should have provisions requiring that financial services that utilise foreign CBDCs and provide for their use by Australian customers, should be made to disclose data on their use in Australia to APRA and the RBA.

Big Tech disinformation

- The tension between online free speech, hate speech and disinformation is one that has increasingly occupied the minds of policy makers.
- Disinformation, misinformation, and mal-information is widespread—especially online. Problematic information is often distributed via platforms, especially popular social media platforms such as Facebook, video sharing sites like YouTube (owned by Google), and popular messaging applications such as WhatsApp (owned by Facebook).
- Governments may, for example, pass laws that define disinformation as including, among other things, content that is critical of the government or counters government messaging.
    - Disinformation laws that are too broad and vague or pose a risk to human rights can risk curtailing legitimate speech. They can also be used selectively or indiscriminately by governments to encourage or require private companies to police speech in ways that can harm free expression and limit public debate.
- Recommendations on how disinformation issues could be handled in ways that will protect free expression and independent news media have been mooted focussing on: practical responses; legal responses; platform responses; and oversight, transparency, and due process.
- In Australia, there have been a number of reforms aimed at strengthening the online safety.
    - The Australian Code of Practice on Disinformation and Misinformation was published in February 2021 by the Digital Industry Group Inc.
    - *The Online Safety Act 2021*, assented into law in July 2021, expanded Australia's protections against online harm, to keep pace with abusive behaviour and toxic content.
    - The Morrison Government also introduced the Social Media (Anti-Trolling) Bill 2022 into the 46th Parliament. The bill, however, lapsed in April 2022.
- Big Tech companies have a corporate responsibility to ensure that their customers and their data are safe.
- US companies essentially have two options: a foreign branch; or an Australian subsidiary company.
    - Directors in local branches and subsidiaries of foreign Big-Tech companies should closely adhere to directors' duties and obligations as set out clearly in Australian law.
        - There may be a need to further clarify those duties and obligations that apply in Australia's jurisdiction so that proper enforcement is guaranteed.