THE SENATE

Senate Economics References Committee

Inquiry into international digital platforms operated by Big Tech companies

Issues Paper

Table of Contents

Introduction

On 26 September 2022, the Senate referred an inquiry into international digital platforms operated by large overseas-based multinational technology companies – so called 'Big Tech' companies – and the nature and extent to which they exert power and influence over markets to the detriment of Australian consumers, to the Senate Economics References Committee (the committee), with particular reference to:

a) the market shares of such international digital platforms across the provision of hardware and software services;

b) vertical integration, or linking of multiple services, products and/or hardware, within such international digital platforms and resultant outcomes on users' ability to exercise choice;

c) whether algorithms used by such international digital platforms lack transparency, manipulate users and user responses, and contribute to greater concentrations of market power and how regulating this behaviour could lead to better outcomes in the public interest;

d) the collection and processing of children's data, particularly for the purposes of profiling, behavioural advertising, or other uses;

e) the adequacy and effectiveness of recent attempts, in Australia and internationally, to regulate the activities of such international digital platforms;

f) broader impacts of concentration of market power on consumers, competition and macro-economic performance, and potential solutions; and

g) any other related matters.

Background

Technology companies include companies that provide hardware, software, platforms and consumer services, many of which provide multiple services. In the United States (US), so-called 'Big Tech' is often understood to include the 'Big Five' tech companies, also known as GAFAM, which operate digital platforms used around the world. These are:

- Google (Alphabet);
- Apple;
- Facebook (Meta);
- Amazon; and
- Microsoft.

Together, these five companies have a joint market capitalisation of around US$4.5 trillion.[1] These companies in many instances have acquired other popular platforms—Google, for example, owns YouTube, while Meta owns Instagram and Whatsapp. Big Tech can also refer to other major tech companies which vary in their market concentrations across different parts of the globe but predominate globally in their particular segment of the market.

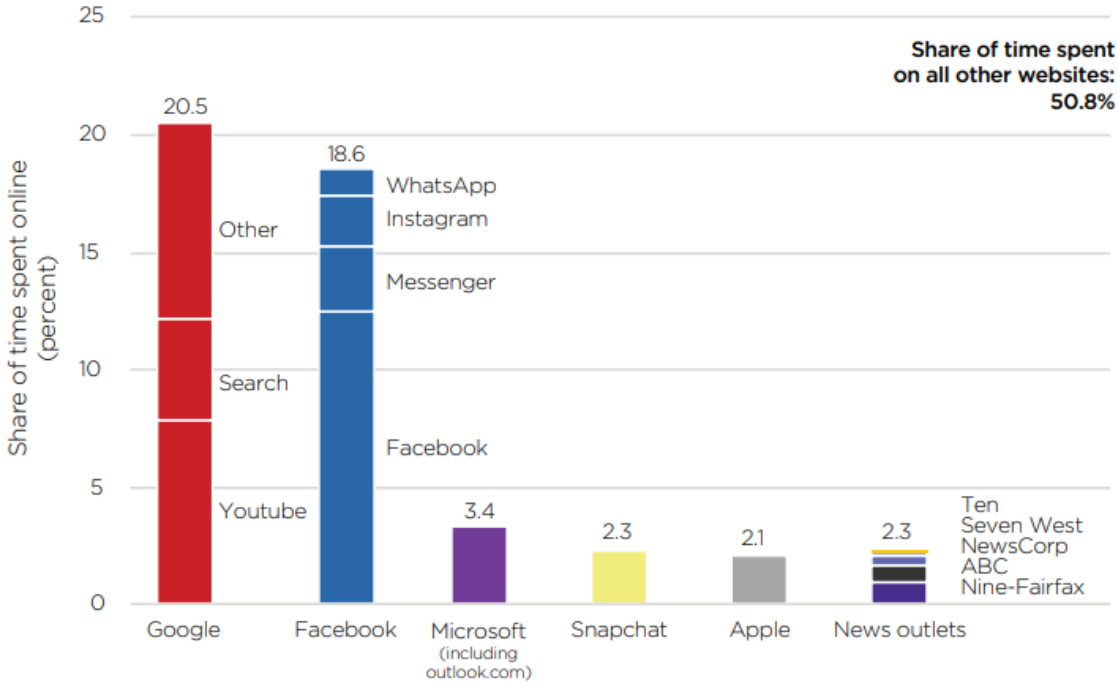
---

1 Cory Mitchel, 'GAFAM stocks', 7 October 2020, https://www.investopedia.com/terms/g/gafam-stocks.asp (accessed 2 September 2022).

The website 'Techtarget' provides a useful definition of 'Big Tech: "Big Tech is a term that refers to the most dominant and largest technology companies in their respective sectors. Their products and services are used globally and have become heavily relied upon by businesses and individuals alike, bringing up privacy, safety and Antitrust concerns about their influence and operations and whether strict regulations should be considered." https://www.techtarget.com/whatis/definition/Big-Tech, (accessed 12 October 2022).

An analysis of the time Australians spend on particular apps and websites reveals the market share that Google, Apple, Meta and Microsoft command in Australia, with Australians spending the most time on Google (including YouTube and search engines) and Meta-owned platforms (Facebook, Messenger, Instagram and Whatsapp) (see Figure 1).

Figure 1: Apps and websites Australians spent the most time on, as of 2019, by platform



Source: ACCC, Digital Platforms Inquiry – Final Report, July 2019, p. 6, citing Nielsen Digital Panel, February 2019.

According to an article published by the Australian Institute of Policy and Science, there 'are now legitimate community expectations of explicit regulation of Big Tech in Australia'.[2] A Lowy Institute poll which found that 90 per cent of Australians surveyed consider that the influence of social media companies is an important or critical threat to the vital interests of Australia. A poll by the *Australian Financial Review* in late 2020 found that 77 per cent of Australians surveyed felt that Big Tech companies should face stronger government regulation.[3]

In other jurisdictions, policymakers and legislators across the political spectrum are pushing for reforms to Big Tech companies, focusing on issues such as market dominance, unfair contract terms, misinformation, privacy, freedom of speech, and the impact of platforms on businesses and individuals.

Concern has focused particularly on alleged monopolistic practices, data localisation, the regulation of 'fake news' distributed via online platforms, data harvesting, harmful and illegal content, and the impact of algorithms on users (for example, on the mental health of young people using social media). However, the primary concern is the market power of Big Tech companies, which is generating increasing unease for governments around the world.[4]

---

2 Rys Farthing & Dhakshayini Sooriyakumaran, 'Why the era of big tech self-regulation must end', *Australian Quarterly*, Oct–Dec 2021, pp. 7–8.

3 Paul Smith, 'Big tech on the nose as Aussies demand accountability and tougher laws', *Australian Financial Review*, 2 November 2020, https://www.afr.com/technology/big-tech-on-the-nose-as-aussies-demand-accountability-and-tougher-laws-20201030-p56a93, (accessed 28 October 2022).

4 Thomas A. Lambert, 'What's behind the war on Big Tech?', *Regulation*, vol. 44, no. 3, 2021, p. 30.

Issues Paper—overview

This issues paper provides an overview, as of November 2022, of current key issues arising in the regulation of Big Tech.

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 the views of submitters on how best to categorise the various tech companies and this mapping process could be used to determine what type of regulation might be required.

The topics canvassed here 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**

Responding to the Issues Paper

The discussion below is not authoritative nor exhaustive and is intended as a starting point only. A further reading list is also included at the end of this paper.

At the end of each section are open questions seeking views on these policy issues and whether people agree with the focus of the Issues Paper and general contention.

Questions included within this paper are a guide for submitters. The committee does not expect or require submissions to respond to every question included in this Issues Paper. Wherever possible, please provide reasons for your views and any evidence available to support your views.

Through submissions to the inquiry, the committee welcomes further insights from subject matter experts and interested stakeholders. Information as to how to lodge a submission can be found on the committee's website.

It is recommended that comments stay focussed on the terms of reference. Documents that don't address the terms of reference and diverge onto extraneous issues are unlikely to be accepted as submissions. Further guidance on making a submission can be found on the Senate's Making a Submission website.

Market concentration

The economic consequences of Big Tech

The impact of Big Tech companies on the general economy and thus small business is beyond question. Harvard Business School's Dr. John Deighton observed:

> the… internet "has shaped US economic development on a scale comparable to, and likely exceeding, the introduction of electrification in the last quarter of the 19th century." No other

> technology has done more to spur innovation and competition, level the playing field for small businesses, and create communities of shared values and interests, online and off.
>
> More than 17 million US jobs depend on the commercial internet, which contributed nearly $12.45 trillion to the country's economy in 2020, a 22 per cent growth rate over four years. The US economy grew between 2 per cent and 3 per cent during the same period. IAB's [Interactive Advertising Bureau] study also shows that small businesses and self-employed individuals account for the largest share of internet jobs.[5]

The website *Thryv* noted that, with regard, to the power of Big Tech:

> The truth is massive technology conglomerates from Apple to Amazon hold a ton of power. One small change in an algorithm can cause waves in how small businesses communicate with customers or do business…
>
> Small operations heavily rely on these Big Tech giants to do business. And why not? For many, advertising on Facebook and Instagram has worked so well that some small businesses bypass having their own websites.[6]

Vertical Integration

One aspect of Big Tech dominance is 'vertical integration'. As tech companies have grown to become the largest firms in the world, they have increasingly engaged in a practice called 'vertical integration'. It is a strategy that companies use to control their own suppliers, distributors or retail stores in order to control their value or supply chain. Companies can integrate vertically through mergers and acquisitions or research and development; giving them the opportunity to have full control of the processes related to their operations.[7]

Despite the competition between Big Tech companies, most of them rely on each other for a particular product or service. For example, Google pays Apple around US$7 billion annually to be the default search engine for Safari. At the same time, Netflix uses Amazon Web Services for its computing and storage needs and IBM recently chose Slack as the organisational communication tool. However, tech giants are starting to work towards creating a full solution suite for their customers. The desire to completely own this full solution suite has led Big Tech to engage in more vertical integration activities.[8]

Some recent examples of vertical integration in Big Tech are:

- Amazon launched its own delivery service in Los Angeles to compete with FedEx and UPS and purchased Whole Foods the year prior; [9]

---

5 Cited in 'How the politics of "Big Tech" is threatening US small business' *WARC*, 4 May 2022, https://www.warc.com/newsandopinion/opinion/how-the-politics-of-big-tech-is-threatening-us-small-business/en-gb/5667, (accessed 6 October 2022).

6 'Welcome to the Metaverse— How Big Tech impacts small business', *Thryv,* 12 February 2021, https://www.thryv.com.au/blog/big-tech-impact-small-business/, (accessed 6 October 2022).

7 'Apple Silicon: Why tech giants engage in vertical integration', *Common Sense,* https://www.tcsnetwork.co.uk/apple-silicon-why-tech-giants-engage-in-vertical-integration/, (accessed 7 October 2022).

8 'Apple Silicon: Why tech giants engage in vertical integration', *Common Sense,* (accessed 7 October 2022).

9 'Amazon is launching its own delivery service to compete with UPS and FedEx', *Business Insider,* https://www.businessinsider.com/amazon-launching-own-delivery-service-compete-ups-fedex-2018-2, (accessed 7 October 2022).

- Samsung purchased Harman for US$8 billion and absorbs Harman Kardon, Infinity, JBL, and Mark Levinson brands;[10] and
- Microsoft purchased LinkedIn taking Microsoft a step closer to a vertically connected ecosystem.[11]

A further and more recent example of vertical integration is the launch by Apple of its Apple Card savings account in partnership with Goldman Sachs. On 13 October 2022, Apple issued a press release describing their product:

> In the coming months, Apple Card users will be able to open the new high-yield Savings account and have their Daily Cash automatically deposited into it — with no fees, no minimum deposits, and no minimum balance requirements. Soon, users can spend, send, and save Daily Cash directly from Wallet.[12]

The Apple Card was launched in August 2019 and, according to Apple, is a credit card where:

> Your information lives on your iPhone, beautifully laid out and easy to understand. We eliminated fees and built tools to help you pay less interest, and you can apply in minutes to see if you are approved with no impact to your credit score. Advanced technologies like Face ID, Touch ID, and Apple Pay give you a new level of privacy and security.[13]

Ron Shevlin, Chief Research Officer at Cornerstone Advisors, examined Apple's financial initiatives in an article in *Forbes* magazine.[14] He observed:

> …Apple is signalling to the market its intentions to compete with commerce platforms like Square, PayPal, Google, and Klarna.
>
> Apple's penetration and control in the consumer market is incredibly strong, but until recently, it's had little presence on the merchant side. Apple realizes that it needs to pursue a platform business model to protect and grow its market position.[15]

He concluded:

> Varying payment terms—for example, spreading payments for a purchase over a period of time—or providing credit before or during the shopping process, marketers can influence consumers' likelihood to buy.
>
> Personalizing payment terms is another way for merchants to influence consumers' choice of products and providers—and it's the commerce platforms who have the data, analytical capabilities, and connectivity to make this happen.

---

10 'Samsung to buy car tech company Harman for $8 billion ', *Reuters*, https://www.reuters.com/article/us-harman-intl-ind-samsung-elec-idUSKBN1390O9, (accessed 7 October 2022).

11 'An ecosystem perspective on Microsoft's acquisition of LinkedIn', *LinkedIn*, https://www.linkedin.com/pulse/ecosystem-perspective-microsofts-acquisition-linkedin-jay-van-zyl, (accessed 7 October 2022).

12 'Apple Card will soon let users grow Daily Cash rewards while saving for the future', *Apple* website, https://www.apple.com/newsroom/2022/10/apple-card-will-let-users-grow-daily-cash-rewards-while-saving-for-the-future/, (accessed 31 October 2022).

13 'Apple Card', *Apple* website, https://www.apple.com/apple-card/, (accessed 31 October 2022).

14 ''Breakout': Apple's Plan To Pump Up Apple Card And Apple Pay And Win The Payments War, *Forbes,* 10 April 2022, https://www.forbes.com/sites/ronshevlin/2022/04/10/breakout-apples-plan-to-pump-up-apple-card-and-apple-pay-and-win-the-payments-war/, (accessed 31 October 2022).

15 ''Breakout': Apple's Plan To Pump Up Apple Card And Apple Pay And Win The Payments War, *Forbes,* 10 April 2022, (accessed 31 October 2022).

> Apple, Square, Klarna, and Shopify know that reducing friction and cost in the payment process influences purchase behavior. As a result, having a superior payments experience is critical to building the commerce platform for the 2020s.[16]

Through vertical integration and other measures, Big Tech companies are starting to outgrow their partners. This means that they can cut ties with their partners and create the service or product that those partners were offering themselves. If complementary assets are in place, Big Tech companies will usually wait until they can create a superior product at a cheaper price.[17]

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. This wave of Big Tech vertical integration looks like it could become a self-reinforcing cycle; i.e. a Big Tech company will vertically integrate because it wants to grow, however, as it grows there is further incentive to vertically integrate.[18]

App–marketplaces

The Australian Competition and Consumer Commission (ACCC) is conducting an inquiry into Digital Platform Services.[19] As part of this inquiry, the ACCC is examining the use of computer applications (Apps) by Big Tech in furthering their business.

In their March 2021 Interim report, the ACCC noted that Apple and Google each offer their own apps (first-party apps), which compete directly with apps developed by third parties (third-party apps) reliant on Apple and Google's app marketplaces.

The ACCC expressed concern that, given their market power and their related activities, Apple and Google each have 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.

A number of Apple and Google's own apps clearly benefit from being pre-installed or set as defaults and/or having superior integration with the relevant operating system. Pre-installation and defaults may entrench market power, limit consumer choice, and reduce potential for innovation in the downstream markets in which they compete.[20]

Multiple solutions have been identified internationally to address this issue of self-preferencing. These include structural separation of vertically integrated platforms, and the introduction of a per-se prohibition which would effectively ban or restrict a platform with particular characteristics self-preferencing its services and products over those of third parties.[21]

The ACCC identified that there is a potential need for information collected by Apple and Google in their capacity as app marketplace operators to be ring-fenced from their other operations and business decisions. This would minimise the risk of this information being used to provide

---

16 ''Breakout': Apple's Plan To Pump Up Apple Card And Apple Pay And Win The Payments War, *Forbes,* 10 April 2022, (accessed 31 October 2022).

17 'Apple Silicon: Why tech giants engage in vertical integration', *Common Sense,* (accessed 7 October 2022).

18 'Apple Silicon: Why tech giants engage in vertical integration', *Common Sense,* (accessed 7 October 2022).

19 'Digital platform services inquiry 2020-2025', *ACCC* webpage, https://www.accc.gov.au/publications/serial-publications/digital-platform-services-inquiry-2020-2025, (accessed 25 November 2022).

20 'Digital platform services inquiry 2020-2025 – March 2021 interim report', *ACCC* webpage, https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20March%202021%20interim%20report.pdf, p. 6., (accessed 25 November 2022).

21 'Digital platform services inquiry 2020-2025 – March 2021 interim report', *ACCC* webpage, pp. 7–8., (accessed 25 November 2022).

Apple and Google with an unfair competitive advantage over third-party app developers in downstream markets for apps.[22]

The ACCC also reviewed concerns about commission rates charged by Apple and Google on payments made for digital goods through apps (inapp payments) and the associated terms. The ACCC observed that both Apple and Google require that certain in-app payments must be processed through their respective in-app payment systems. Apple and Google both impose a commission of 30 per cent on these payments, although there are circumstances where the rate is 15 per cent. Both Apple and Google recently expanded the circumstances in which only 15 per cent is required to be paid. Both app marketplaces provide that an app is not permitted to contain information that directs users to an off-app payment option.[23]

The ACCC concluded:

> Tying of app store services to in-app payment systems leads to a loss of consumer choice as consumers are unable to use (and developers are unable to offer) any other payment option when making payments in apps. This could negatively impact the quality and functionality of the apps and services that app developers wish to provide their users, such as by limiting their ability to issue refunds or cancel subscriptions. It could also affect:
>
> - app developers' ability to make changes to the prices of in-app purchases
> - competition between apps that are subject to the requirement and apps that are not
> - the choice of business model for app developers.
>
> Some stakeholders, including the Coalition for App Fairness, Epic Games and Match Group, submit that the requirement to use Apple and Google's in-app payment systems has resulted in higher prices for consumers.[24]

Gilbert & Tobin provide a further useful summary from a similar report done by the Competition and Markets Authority (CMA) in the United Kingdom. They also observed:

> The main way in which both Apple and Google monetise their app stores directly is through requirements on certain developers to use their proprietary payment systems to process in-app purchases made by users, such as paid for aps, features or content within an app, or subscriptions… Under these arrangements, Apple and Google collect a commission of up to 30 per cent on in-app purchases.[25]

Spotify, in its response to the CMA's Digital Markets Taskforce Call for Information, stated:

> App stores are in a position not only to set app approval terms unilaterally, but also to give themselves the discretion unilaterally to amend app approval rules (or their interpretation), leaving developers no option but to adapt their own commercial conduct, even when materially disadvantageous to them.[26]

---

22 'Digital platform services inquiry 2020-2025 – March 2021 interim report', *ACCC* webpage, p. 9, (accessed 25 November 2022).

23 'Digital platform services inquiry 2020-2025 – March 2021 interim report', *ACCC* webpage, p. 9, (accessed 25 November 2022).

24 'Digital platform services inquiry 2020-2025 – September 2022 interim report', *ACCC* webpage, p. 133, (accessed 25 November 2022).

25 'Mobile ecosystems: Role of Google and Apple in competition between app developers', *Lexology,* webpage, https://www.lexology.com/library/detail.aspx?g=764cfe15-215b-4fdc-8236-a881373ff565, (accessed 25 November 2022).

26 Spotify, 'Response to the CMA's Digital Markets Taskforce Call for Information', 8 December 2020, p 4, cited in 'Digital platform services inquiry 2020-2025 – March 2021 interim report', *ACCC* webpage, p. 46, (accessed 25 November 2022).

Epic Games, regarding their attempt to introduce its own in-app payment system, and subsequent litigation with Apple, commented in their submission to the ACCC enquiry:

> Developers are barred from reaching billions of iOS and Android users unless they go through the Apple and Google app stores and submit to whatever terms they impose. Opening mobile devices to alternate means of downloading applications and software is foundational to the creation of a more open ecosystem, whether it be alternative app stores or direct downloading of applications from the web. These solutions already exist and are regularly and safely used by consumers every day when they use their laptop or desktop computers, including PCs, macs and Chromebooks. It is only when consumers shift from the computer on their desk to the computer in their pocket that they are limited to software installation through the App Store and Play Store. These limits are the product of commercial decisions by Apple and Google – not of safety or technical necessity.[27]

Parallel to this, the Australian Government has introduced a Digital Games Tax Offset (DGTO). The DGTO will allow Australian games developers access to a 30 per cent rebate on projects costing up to $500,000.

Originally introduced by the Morrison Government, the measure has now been reintroduced by the Albanese Government through the Treasury Laws Amendment (2022 Measures No. 4) Bill 2022 that has now been introduced to Parliament and will be reviewed by this Committee.[28] The states are also introducing similar measures:

> …spurred by further state elections, governments around the country have begun introducing bigger and better incentive packages over the last year. In April, Queensland introduced one of the nation's most attractive packages, continuing several years of positive expansion in the sector. New South Wales began introducing new games funding initiatives last year to compete with those on offer in Victoria. Not to be outdone, and facing a state election of its own, Victoria's Andrews government announced a new set of Vicscreen initiatives at PAX Aus in October.[29]

Such support may very well be needed in response to Big Tech's increasing market share. For example, in January of this year, Microsoft spent $US75 billion (A$112 billion) purchasing games publisher Activision Blizzard. The *Australian Financial Review* noted:

> Video games have come to be seen as one path towards these more immersive online worlds. The biggest tech companies have powerful incentives to take the next step and develop full gaming operations, says Michael Wolf, a media consultant. "Every one of these [tech] companies knows gaming is going to be a growth area, and it ties into their metaverse ambitions more broadly."[30]

Indie developers find it difficult to break into the market given the platform fees. GamesHub provided this useful summary:

> The industry standard platform fee hovers around 30 per cent, which includes the likes of Steam, PlayStation, and Nintendo. In an attempt to disrupt the market, the Epic Games Store only takes

---

27 Epic Games, Submission to the ACCC Digital Platform Services Inquiry, p. 7, https://www.accc.gov.au/system/files/Epic%20Games.pdf, (accessed 25 November 2022).

28 'Australian Digital Games Tax Offset Has Been Introduced To Parliament, Inching It Closer To Law', *Kotaku,* 23 November 2022, https://www.kotaku.com.au/2022/11/australian-digital-games-tax-offset-introduced-to-parliament/, (accessed 28 November 2022).

29 'Australian Digital Games Tax Offset Has Been Introduced To Parliament, Inching It Closer To Law', *Kotaku,* 23 November 2022, https://www.kotaku.com.au/2022/11/australian-digital-games-tax-offset-introduced-to-parliament/, (accessed 28 November 2022).

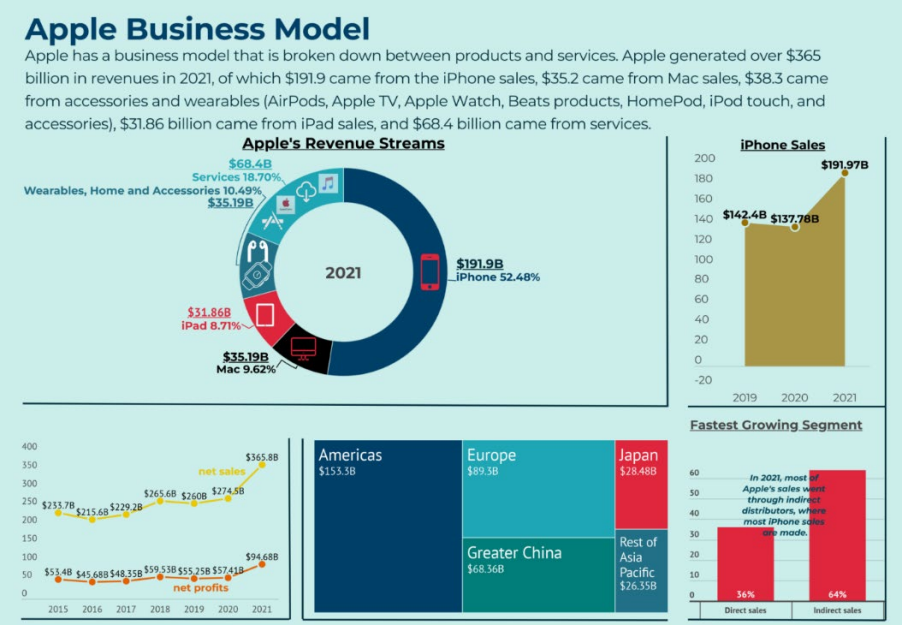
30 'Why gaming is the new big tech battleground', *Australian Financial Review,* 24 January 2022, https://www.afr.com/technology/why-gaming-is-the-new-big-tech-battleground-20220124-p59qok, (accessed 28 November 2022).

12 per cent, and independent platform itch.io allows developers to set their own split, with a default cut of 10 per cent. Microsoft takes 30 per cent of sales made through the Xbox console's digital store, while its PC marketplace recently changed to 12 per cent in line with Epic. Many game developers believe the standard 30 per cent platform cut is too high. According to figures from the Game Developers Conference 2021 State of the Game Industry survey, 71 per cent of over 3,000 respondents believed digital storefronts should only receive 20 per cent or less of each sale.[31]

Big Tech Business Models

Apple

Apple's business model is based on product sales. Apple has made over US$365.8 billion in revenues in 2021, of which over US$191.9 billion or over 52 per cent of its total revenues came from the iPhone. Yet, the iPhone isn't just a hardware product; it's a business platform that combines hardware (iPhone), operating system (iOS), and a marketplace (the App Store). Thus, the company still makes most of its money around a single product which powers up an entrepreneurial ecosystem.[32]



Source: Gennaro Cuofano, 'How Do Tech Companies Make Money? Visualizing Tech Giants Business Models In 2022', FourWeekMBA, 26 August 2022.

Microsoft

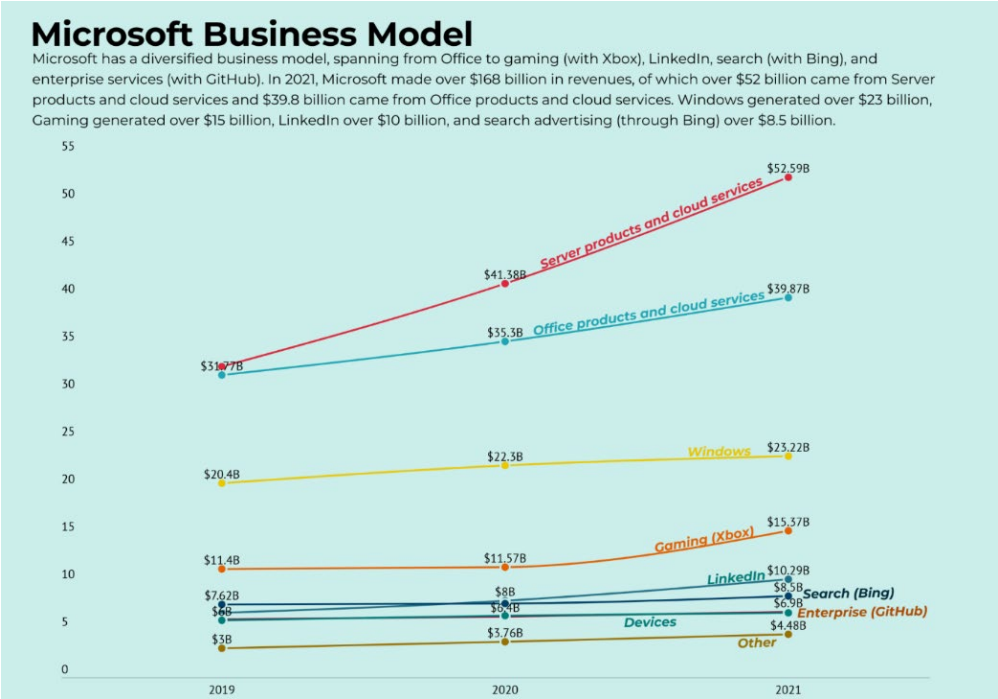
Founded in 1975, Microsoft is still one of the most valued companies, with a market capitalization of over seven hundred billion dollars. That is also because the company has been able to use the excess cash it generated in the last decades to acquire new ventures.

---

31 'How digital distribution and game prices are costing developers', *GamesHub* webpage, 24 May 2022, https://www.gameshub.com/news/features/how-game-prices-digital-distribution-and-xbox-game-pass-affects-developers-10912/, (accessed 25 November 2022).

32 Gennaro Cuofano, 'How Do Tech Companies Make Money? Visualizing Tech Giants Business Models In 2022', *FourWeekMBA*, 26 August 2022, https://fourweekmba.com/tech-giants-business-models/, (accessed 20 October 2022).

Microsoft has been able to use its lucrative cash source, the Microsoft Office System, to diversify its business model significantly. In 2021, Microsoft generated over US$168 billion in revenues, with server products and cloud services passing for the first-time office products.[33]



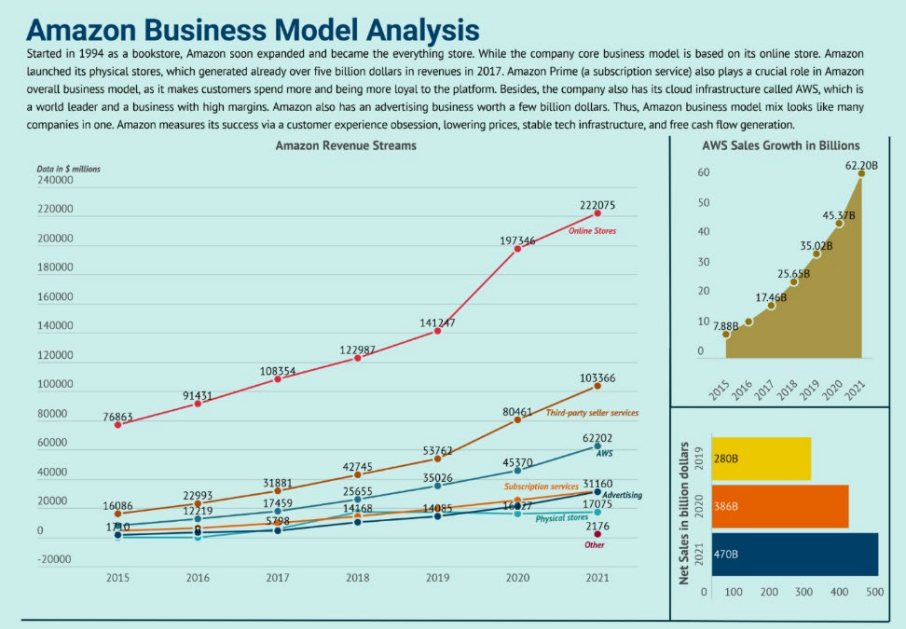
Source: Gennaro Cuofano, 'How Do Tech Companies Make Money? Visualizing Tech Giants Business Models In 2022', FourWeekMBA, 26 August 2022.

Amazon

Amazon has a diversified business model. In 2021, Amazon posted over US$469 billion in revenues and over US$33 billion in net profits. Online stores contributed to over 47 per cent of Amazon revenues. Amazon has a diversified business model as there is a growing part of the business that relies on seller services, subscription services (Prime), and cloud-based services (AWS). It is highly probable that the part of the business related to seller services, subscriptions, and cloud-based services will become the most critical part of the company from the revenue generation standpoint.[34]

33 Gennaro Cuofano, 'How Do Tech Companies Make Money? Visualizing Tech Giants Business Models In 2022', *FourWeekMBA*, 26 August 2022.

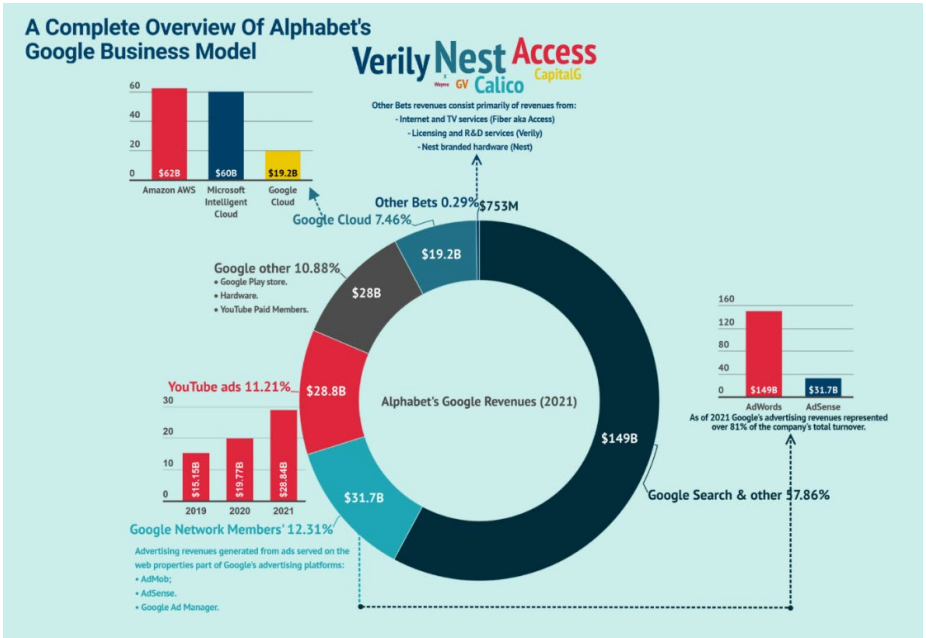
34 Gennaro Cuofano, 'How Do Tech Companies Make Money? Visualizing Tech Giants Business Models In 2022', *FourWeekMBA*, 26 August 2022.



Source: Gennaro Cuofano, 'How Do Tech Companies Make Money? Visualizing Tech Giants Business Models In 2022', FourWeekMBA, 26 August 2022.

Google

Google (now Alphabet) primarily makes money through advertising. The Google search engine, while free, is monetized with paid advertising. In 2021, Google's advertising generated over US$209 billion compared to US$257 billion in net sales. Advertising represented over 81 per cent of net sales, followed by Google cloud (US$19 billion) and Google's other revenue streams (Google Play, Pixel phones, and YouTube Premium). However, the company is growing other revenue streams too such as Apps, Google cloud, and Hardware).[35]

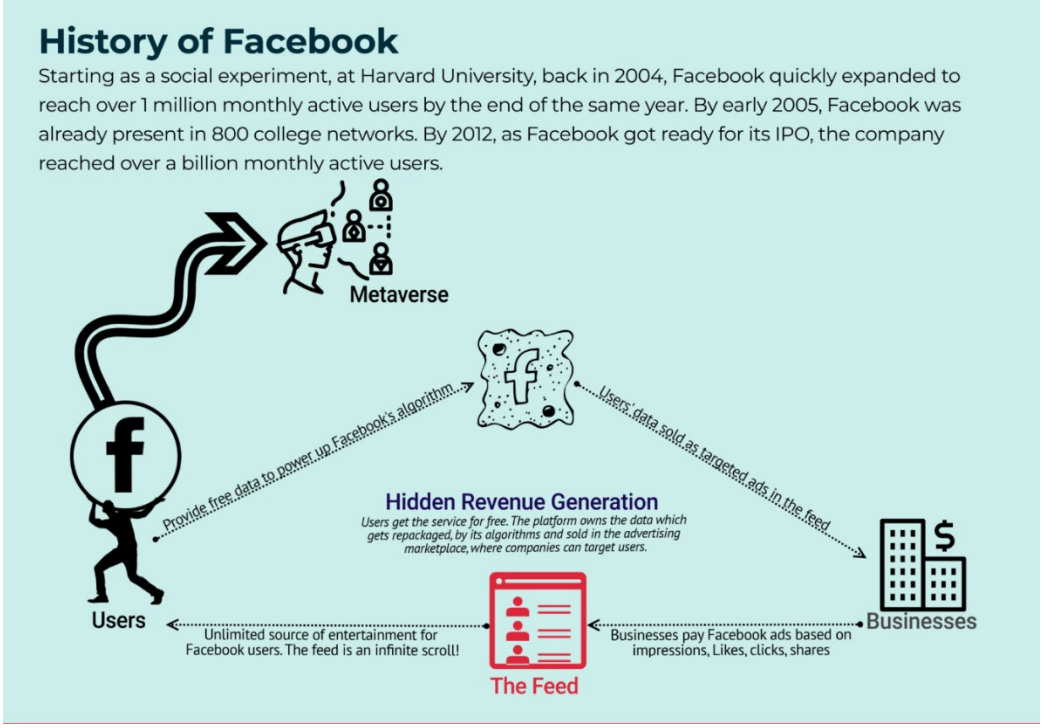


Source: Gennaro Cuofano, 'How Do Tech Companies Make Money? Visualizing Tech Giants Business Models In 2022', FourWeekMBA, 26 August 2022.

35 Gennaro Cuofano, 'How Do Tech Companies Make Money? Visualizing Tech Giants Business Models In 2022', *FourWeekMBA*, 26 August 2022.

Facebook

Facebook's business model is based on advertising as it is able to tap into the value of its billions of users. As of 2021, over 97 per cent of its revenues came from advertising. Facebook's algorithms condense the attention of the over 2.91 billion monthly active users who use the platform (as measured in June 2021). Meta generated US$117.9 billion in revenues, in 2021, of which US$114.9 billion was from advertising (97.4 per cent of the total revenues) and over US$2.2 billion from Reality Labs (the augmented and virtual reality products arm).[36]



Source: Gennaro Cuofano, 'How Do Tech Companies Make Money? Visualizing Tech Giants Business Models In 2022', FourWeekMBA, 26 August 2022.

Impact on small business

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.

On 30 March 2022, Small Business Majority (SBM) in the United States released a scientific opinion poll that revealed most small business owners seek a more equitable playing field with larger competitors, particularly on digital platforms and in the area of contracts and agreements.

The poll revealed that, even before the pandemic, large corporations maintained a stranglehold across all markets and industries. When many small businesses pivoted to online platforms during the pandemic to keep their businesses afloat, they were exposed to further competitive inequities. The SBM report outlined some of those unfair practices:

36 Gennaro Cuofano, 'How Does Facebook [Meta] Make Money? Facebook Business Model Analysis 2022', *FourWeekMBA*, https://fourweekmba.com/how-does-facebook-make-money/, 26 August 2022, (accessed 2 November 2022).

- Small businesses want a more equitable playing field with their larger competitors: 83 per cent said larger companies have the resources to drown small businesses out with their market power;
- Small businesses increasingly rely on online platforms for their businesses: 30 per cent use Facebook's marketplace as part of their marketing strategy;
- Standard big business practices are hurting smaller firms: 35 per cent said they had been affected by self-preferencing, while 55 per cent believe that it's an issue; 34 per cent said they had been negatively affected by predatory pricing, while 55 per cent believe that it's an issue; and
- Small businesses are impacted by unfair agreements and terms with large companies: 41 per cent said they had been negatively affected by differential pricing based on their size.

One small business owner was quoted as saying:

> I've had to overcome barriers on my journey to attain the American dream and build generational wealth, mostly from large technology platforms that practice unapologetic monopolization. Big tech companies like Amazon have the resources to test different marketing strategies and stand by calmly as their revenue fluctuates. Us small guys don't have that luxury. We have to pay to win. But we have no chance of winning if the competition isn't playing fair.[37]

Potential benefits for small business

The argument has also been made that Big Tech, in fact, facilitates small business success:

> Digital platforms, tools, and marketplaces help small businesses start, grow, and succeed. Digital advertising and online marketing help small companies find new customers — cost-efficiently. The digital cloud helps small businesses reduce paperwork, reduce their environmental footprint, and be more flexible in where and how they work. Digital marketplaces help small businesses sell more products in the next county, a neighbouring state, and around the world.
>
> It seems policymakers only talk about Facebook, Apple, Google, and Amazon, but there are many digital platforms that support small businesses. QuickBooks, Pinterest, Houzz, and Etsy, or less well-known tech platforms like John Deere, whose Precision Agriculture solutions work wonders for small farmers. All of these companies collect, aggregate, and analyze vast quantities of data — safely, securely, and inexpensively. They deliver the power of data science to small businesses that could not do this any other way.
>
> It is indisputable that large digital platforms, services, and marketplaces provide small businesses with affordable, scalable, and secure business solutions. They have opened up new markets and allowed small businesses to compete globally and in ways that were unimaginable a few decades ago.[38]

---

37 'New Scientific Opinion Poll: Small business owners experience unlevel playing field with large companies and Big Tech', *Small Business Majority*, 30 March 2022, https://smallbusinessmajority.org/press-release/new-scientific-opinion-poll-small-business-owners-experience-unlevel-playing-field-large-companies-and-big-tech, (accessed 6 October 2022).

38 'Digital Big Tech drives small business success', *The Hill*, 19 November 2019, https://thehill.com/opinion/technology/471005-digital-big-tech-drives-small-business-success/, (accessed 6 October 2022).

Consultation questions:

Question 1: What impact does the market power of big tech companies have on the economy, society and small businesses?

Question 2: What regulatory measures could be put in place to address the adverse impact of big tech companies? What other non-regulatory interventions could governments take to reduce the market power of big tech companies?

Question 3: Do Big Tech companies have any special dispensations from the rules that govern all other companies? If so, should these be removed, and why?

The cloud

The cloud market is, like many aspects of Big Tech, 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).[39]

AWS, Microsoft Azure, and GCP are the cloud service providers with the largest market share, collectively capturing over 65 per cent of spending on cloud infrastructure services. The breakdown is:

- AWS has 34 per cent market share,
- Microsoft Azure has 22 per cent market share, and
- GCP has 9.5 per cent market share.[40]

In terms of how the cloud itself functions, the webpage *Cloudfare* has provided a good summary.

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 and cloud servers are located in data centres all over the world. By using cloud computing, users and companies do not have to manage physical servers themselves or run software applications on their own machines.[41]

The cloud enables users to access the same files and applications from almost any device, as computing and storage takes place on servers in a data centre, instead of on the user device. Thus, a user can log in to their Instagram account on a new phone after their old phone breaks and still find their old account in place, with all their photos, videos, and conversation history.[42]

---

39 Mary Zhang, 'Top 10 Cloud Service Providers Globally in 2022, *DgtlInfra,* 22 June 2022, https://dgtlinfra.com/top-10-cloud-service-providers-2022/, (accessed 11 November 2022).

40 Mary Zhang, 'Top 10 Cloud Service Providers Globally in 2022, *DgtlInfra,* 22 June 2022, (accessed 11 November 2022).

41 'What is the cloud?', *Cloudflare*, https://www.cloudflare.com/en-gb/learning/cloud/what-is-the-cloud/, (accessed 29 September 2022).

42 'What is the cloud?', *Cloudflare,* (accessed 29 September 2022).

Main service models of 'cloud' computing

- **Software-as-a-Service (SaaS):** Instead of users installing an application on their device, SaaS applications are hosted on cloud servers, and users access them over the Internet. Examples of SaaS applications include Salesforce, MailChimp, and Slack.
- **Platform-as-a-Service (PaaS):** In this model, companies don't pay for hosted applications; instead they pay for the things they need to build their own applications. PaaS vendors offer everything necessary for building an application, including development tools, infrastructure, and operating systems, over the Internet. PaaS examples include Heroku and Microsoft Azure.
- **Infrastructure-as-a-Service (IaaS):** In this model, a company rents the servers and storage they need from a cloud provider. They then use that cloud infrastructure to build their applications. IaaS providers include DigitalOcean, Google Compute Engine, and OpenStack.

  Formerly, SaaS, PaaS, and IaaS were the three main models of cloud computing, and essentially all cloud services fit into one of these categories. However, in recent years a fourth model has emerged:

- **Function-as-a-Service (FaaS):** FaaS, also known as serverless computing, breaks cloud applications down into even smaller components that only run when they are needed. FaaS or still run on servers, as do all these models of cloud computing. But they are called 'serverless' because they do not run on dedicated machines, and the companies building the applications do not have to manage any servers.

Most common 'cloud' deployments:

- **Private cloud**: is a server, data centre, or distributed network wholly dedicated to one organisation.
- **Public cloud**: is a service run by an external vendor that may include servers in one or multiple data centres. Unlike a private cloud, public clouds are shared by multiple organizations. Using virtual machines, individual servers may be shared by different companies, a situation that is called 'multitenancy' because multiple tenants are renting server space within the same server.
- **Hybrid cloud**: hybrid cloud deployments combine public and private clouds, and may even include on-premises legacy servers. An organization may use their private cloud for some services and their public cloud for others, or they may use the public cloud as backup for their private cloud.
- **Multi-cloud**: is a type of cloud deployment that involves using multiple public clouds. In other words, an organization with a multi-cloud deployment rents virtual servers and services from several external vendors—to continue the analogy used above, this is like leasing several adjacent plots of land from different landlords. Multi-cloud deployments can also be hybrid cloud, and vice versa.[43]

[43] 'What is the cloud?', *Cloudflare,* (accessed 29 September 2022).

Problems and issues with 'cloud' computing

The webpage *Datapine* provided a useful summary of the challenges for 'cloud' computing.[44] The following list is a summary of the relevant issues to this inquiry and not exhaustive:

- *Security issues*

  Like many other branches of technology, security is a pressing concern in the world of cloud-based computing, as you are unable to see the exact location where your data is stored or being processed. This increases the risks that can arise during the implementation or management process.

  Currently, 93 per cent of leading companies across sectors are highly concerned about experiencing a significant data breach within their cloud-centric ecosystems.

  The main concerns surrounding cyber threats across the board are:

  - compromised credentials;
  - broken authentication;
  - human error;
  - mass sensitive data breaches;
  - hacked interfaces and application programming interface (APIs); and
  - account hijacking.

- *Governance/Control*

  Proper Information Technology (IT) governance should ensure IT assets are implemented and used according to agreed-upon policies and procedures; ensure that these assets are properly controlled and maintained and ensure that these assets are supporting your organisation's strategy and goals.

  In today's cloud-based world, IT does not always have full control over the provisioning, de-provisioning, and operations of infrastructure. This has increased the difficulty for IT to provide the governance, compliance, risks, and data quality management required. To mitigate the various risks and uncertainties in transitioning to the cloud, IT must adapt its traditional IT control processes to include the cloud.

- *Compliance*

  Every time a company moves data from the internal storage to a cloud, it is faced with being compliant with official regulations and laws. For example, healthcare organizations in the United States have to comply with HIPAA (*Health Insurance Portability and Accountability Act of 1996*).

  This is one of the many challenges facing cloud computing, and although the procedure can take a certain amount of time, the data must be properly stored.

- *Performance*

  When an organization moves to the cloud it becomes dependent on the service providers. The performance of the organisation's business intelligence (BI) and other cloud-based systems is also tied to the performance of the provider when it falters—i.e. when your

---

44 '12 cloud Computing Risks & Challenges Businesses Are Facing In These Days', *The datapine Blog*, 1 June 2022, https://www.datapine.com/blog/cloud-computing-risks-and-challenges/ (accessed 29 September 2022).

provider is down, you are also down. This isn't uncommon, over the past couple of years all the big players have experienced outages.

For the data-driven decision-making process, real-time data for organizations is imperative and with an inherent lack of control that comes with cloud computing, companies may run into real-time monitoring problems.

International regulation

Around the world, governments are beginning to respond to the regulatory challenges. For example, the UK is seeking to better regulate the cloud and its services.

Ofcom, the UK regulator for the communications services, published on 6 October 2022 a 'cloud services market study; Call for inputs' paper. Ofcom is seeking stakeholders' input on how the market is developing and the nature of competition, particularly in cloud infrastructure services and cloud ecosystems.[45]

Ofcom's study will explore whether any feature of the markets for cloud services, or the behaviour of providers, could dampen competition and harm consumers through higher prices, lower quality products or less innovation. Ofcom will be considering two themes in depth:

- **cloud infrastructure services**, which include services that provide access to raw computing resources, i.e. basic compute, storage and networking (often referred to as infrastructure as a service, or IaaS), as well as services that can be used to develop, test, run and manage applications in the cloud (platform as a service, or PaaS). These are the foundational elements of the cloud stack on which other cloud services are built.
- **cloud ecosystems**, which are the portfolios of services that the hyperscalers [e.g. – AWS, Microsoft and Google] and some other vertically integrated cloud providers supply across the cloud value chain (i.e. also including software as a service, or SaaS). These include cloud marketplaces, which offer access not just to the marketplace owners' services but to those of other cloud providers.[46]

Ofcom's paper also provided a brief overview of cloud regulation in:

- The European Union;
- France;
- Netherlands; and
- Japan.[47]

Ofcom is aiming to complete its study in one year and expect to publish a consultation on their interim findings in March/April 2023.[48]

---

45 ''Cloud services market study; Call for inputs', Ofcom webpage, https://www.ofcom.org.uk/__data/assets/pdf_file/0025/244825/call-for-inputs-cloud-market-study.pdf, (accessed 31 October 2022).

46 ''Cloud services market study; Call for inputs', Ofcom webpage, (accessed 31 October 2022), p. 1.

47 ''Cloud services market study; Call for inputs', Ofcom webpage, (accessed 31 October 2022), pp. 10–12.

48 ''Cloud services market study; Call for inputs', Ofcom webpage, (accessed 31 October 2022), p. 2.

Consultation questions:

Question 1: With respect to the cloud, what regulation that currently exists in other countries that could be of benefit to Australia?

Question 2: Should new assessments and oversight protocols for cloud computing products be implemented to bolster security of the cloud? If yes, how should cloud computing products be regulated?

Question 3: Would government regulation increase confidence in cloud services and provide greater clarity on accountability and have an impact on the benefits this technology?

Question 4: What regulatory challenges are associated with the use of cloud services, particularly where data and information is stored in other jurisdictions? How might these regulatory challenges be addressed to ensure that consumers using cloud services are protected?

Question 5: What can be done to promote competition in the cloud space rather than attempt some form of protection in this market?

Algorithm transparency

Transparency International New Zealand (TINZ) published an article in 2021 which provides a useful summary of the importance of algorithm transparency.[49]

TINZ noted that 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. This issue is made even more urgent by the accumulating evidence that algorithmic systems can produce outputs that are flawed or discriminatory in nature. The two main sources of bias that can distort the accuracy of algorithms are the developers themselves and the input data with which the algorithms are provided.

Moreover, the analytical processes that algorithms rely on to produce their outputs are often too complex and opaque for humans to comprehend, which can make it extremely difficult to detect erroneous outputs. The Association for Computing Machinery points to three potential causes of opacity in algorithmic decision-making processes.[50] First, there are technical factors that can mean that the algorithm's outcomes may not lend themselves to human explanation, a problem particularly acute in machine-learning systems that can resemble a 'black box.' Second, economic factors such as commercial secrets and other costs associated with disclosing

---

49 Niklas Kossow, Svea Windwehr and Matthew Jenkins, *Algorithmic transparency and accountability*, Transparency International New Zealand, 05 February 2021, https://knowledgehub.transparency.org/assets/uploads/kproducts/Algorithmic-Transparency_2021.pdf, (accessed 4 October 2022).

50 Association for Computing Machinery. 2017. "Principles for Algorithmic Transparency and Accountability." https://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf, cited in Niklas Kossow, Svea Windwehr and Matthew Jenkins, *Algorithmic transparency and accountability*, Transparency International New Zealand, 05 February 2021, (accessed 4 October 2022).

information can inhibit algorithmic transparency. Finally, socio-political challenges, such as data privacy legislation may complicate efforts to disclose information, particularly with regards to the training data used.

TINZ argued that, given the potential for automated decision-making to result in discriminatory outcomes, the use of algorithms in public administration needs to come with certain standards. What these safeguards look like will vary in different contexts but should be built into each stage of adopting algorithmic systems.

TINZ argued that ultimately, institutions that use algorithms as part of automated decision-making processes need to be held to the same standards as institutions in which humans make these decisions. Developers must ensure that the algorithmic systems they design are able to comply with the demands of impartial and accountable administration, such as accountability, redress and auditability.[51]

The Association for Computing Machinery US Public Policy Council (USACM) issued a *Statement on Algorithmic Transparency and Accountability* which advocated the following principles:

1. **Awareness**: Owners, designers, builders, users, and other stakeholders of analytic systems should be aware of the possible biases involved in their design, implementation, and use and the potential harm that biases can cause to individuals and society.
2. **Access and redress**: Regulators should encourage the adoption of mechanisms that enable questioning and redress for individuals and groups that are adversely affected by algorithmically informed decisions.
3. **Accountability:** Institutions should be held responsible for decisions made by the algorithms that they use, even if it is not feasible to explain in detail how the algorithms produce their results.
4. **Explanation**: Systems and institutions that use algorithmic decision-making are encouraged to produce explanations regarding both the procedures followed by the algorithm and the specific decisions that are made. This is particularly important in public policy contexts.
5. **Data provenance**: A description of the way in which the training data was collected should be maintained by the builders of the algorithms, accompanied by an exploration of the potential biases induced by the human or algorithmic data-gathering process. Public scrutiny of the data provides maximum opportunity for corrections. However, concerns over privacy, protecting trade secrets, or revelation of analytics that might allow malicious actors to game the system can justify restricting access to qualified and authorized individuals.
6. **Auditability**: Models, algorithms, data, and decisions should be recorded so that they can be audited in cases where harm is suspected.
7. **Validation and testing**: Institutions should use rigorous methods to validate their models and document those methods and results. In particular, they should routinely perform tests to assess and determine whether the model generates discriminatory harm. Institutions are encouraged to make the results of such tests public.[52]

---

51 Niklas Kossow, Svea Windwehr and Matthew Jenkins, Algorithmic transparency and accountability, Transparency International New Zealand, 05 February 2021, (accessed 4 October 2022).

52 'Statement on Algorithmic Transparency and Accountability', *Association for Computing Machinery & US Public Policy Council (USACM),* 12 January 2017, https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf (accessed 4 October 2022).

US legislative reforms

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 in 2021.[53]

The legislative proposals have two main points in common as outlined below. Noting the role of the Federal Trade Commission (FTC) and its caved-out role as regulator in this area, there appears to be no equivalent role undertaken for specific regulation of this matter in Australia.

- **Expanded role for the Federal Trade Commission (FTC).** In the preponderance of proposals, the Federal Trade Commission (FTC) is responsible for enforcement and regulation activities within the legislation.[54] For example:
    - Under the proposed Platform Accountability and Transparency Act (PATA), the FTC would be responsible for enforcing instances of non-compliance with the Act whereby social media companies would be required to provide vetted independent researchers and the public with access to certain platform data. Consequences for a failure to comply would apply.[55]
    - The FTC would have the authority to require that platforms proactively make certain information available to researchers or the public on an ongoing basis, for example, on user targeting and engagement.[56]
    - Through its appointees, policy changes and legislative proposals, the Biden Administration is positioning the FTC as a check on technology companies, whereby congress is calling on the FTC to flex its existing investigative, regulatory and enforcement muscles to promote stronger algorithmic accountability.[57]
- **Section 230 reform**. The aforementioned provision in the 1996 Communications Decency Act generally provides immunity for website platforms that publish information from third-party content. While coming from different ideological perspectives, Legislators from both parties have called for Section 230 to be altered or overhauled in response to recent events.[58]
    - Republicans have argued that major platforms have applied bias in restricting conservative content. Former President Trump vetoed the fiscal year 2021 National Defense Authorization Act because it did not "terminate" Section 230. In 2020, he signed an executive order targeting this legal shield that Internet companies rely on to protect them from liability for user-created content.[59]

In addition to the bills cited above, a few of the proposals that are currently pending in the House and Senate are outlined below.

---

53 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, https://www.dlapiper.com/en/us/insights/publications/2022/1/us-congress-tries-to-decode-algorithms/, (accessed 11 November 2022). This doesn't include additional references to algorithms, AI, machine learning and automated decision-making embedded in a wide range of appropriations and authorization bills, a reflection of the prevalence of these technologies in so many domains.

54 The agency has responsibilities over consumer protection and promotion of competition.

55 A failure to comply may also equate to the potential loss of immunity under section 230 of the *Communications Decency Act*.

56 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

57 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

58 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

59 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

- *The Algorithmic Justice and Online Platform Transparency Act (HR 3611 and S 1896):* The legislation would prohibit algorithmic processes on online platforms that discriminate on the basis of race, age, gender, ability and other protected characteristics; establish a safety and effectiveness standard for algorithms; require online platforms to describe to users in plain language the types of algorithmic processes they employ and the information they collect to power them; and, require online platforms to maintain detailed records describing their algorithmic process for review by the FTC, in compliance with key privacy and data de-identification standards.[60]
- *The Filter Bubble Transparency Act (S 2024 and HR 5921):* would establish requirements for large online platforms that use algorithms applying AI or machine learning to user-specific data to determine the way content is displayed to users. Platforms must notify users that the platform uses such data and make a version of the platform available that uses only user-specific data that has been expressly provided by the user and which enables users to switch between the two platforms.[61]
- *The Justice in Forensic Algorithms Act of 2021 (HR 2438):* some lawmakers are concerned about algorithms' applications in law enforcement, such as the use of facial recognition technology. This bill establishes a federal framework to govern the use of computational forensic software that relies on an automated computational process to assess evidence in a criminal investigation. [62]
- *The PACT Act (S 797):* The bipartisan Platform Accountability and Consumer Transparency (PACT) Act[63] would update Section 230 to require that large online platforms remove court-determined illegal content and activity within four days and would exempt the enforcement of federal civil laws from Section 230.[64]
- *The Protecting Americans from Dangerous Algorithms Act (S 3029 and HR 2154)***:** If social media companies promote extremist content on their platforms that leads to offline violence, such as interference with civil rights or acts of international terrorism, their immunity from liability would be limited by this bill.[65]
- *The Social Media DATA Act (HR 3451)***:** Similar to the PATA outlined above, the Social Media Disclosure And Transparency of Advertisements (DATA) Act of 2021 would require the FTC regulate the accessible data made available by large digital advertising platforms, including specific information that must be made available. The FTC would also be required to undertake a consultation process to provide a set of best practices for social media research.[66]
- *The Algorithmic Accountability Act of 2019***:** introduced in the previous session of Congress in both houses, was one of the most extensive regulatory approaches to AI ever introduced at the federal level. The proposal required specified commercial entities

60 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

61 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

62 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

63 The bill was introduced in previous sessions of Congress but did not advance.

64 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

65 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

66 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

to conduct assessments of high-risk systems that involve personal information or make automated critical decisions, such as systems that use AI or machine learning.[67]

Consultation questions:

Question 1: Akin to the Federal Trade Commission in the US, should an oversight body be established in Australia to undertake similar regulatory activities?

Question 2: Are there useful ideas in the proposed US legislation that are applicable in Australia?

Question 3: Similarly, are there other jurisdictions, such as the UK, EU and Japan, that also have applicable concepts that could be usefully incorporated into Australian law?

Data and privacy

The digital age has brought with it extraordinary advances, but it has also created new threats to consumer privacy. One of the biggest concerns comes from the way that Big Tech companies collect and use customer data.[68]

Most people are now familiar with the term 'data mining'—the process by which companies collect large amounts of data about consumers online activity and use it to target advertisements and sell products. But data mining is just one aspect. Many tech companies are now using sophisticated methods to track their customers every move, both online and offline.[69]

This tracking is made possible by the proliferation of devices that are connected to the internet. These devices collect a wealth of data about our whereabouts, our behaviours and even our physiology. This data is then used to create detailed profiles of each individual user.[70]

These profiles are extremely valuable to companies, who use them to target ads, sell products and influence our behaviour. In other words, companies use their customers personal information to pursue profit.[71]

Internationally, policymakers and legislators across the political spectrum have begun pushing for reforms to Big Tech companies, focusing on issues such as market dominance, unfair contract terms, misinformation, privacy, freedom of speech, and the impact of platforms on businesses and individuals. Concern has focused particularly on alleged monopolistic practices, data localisation, the regulation of 'fake news' distributed via online platforms, data harvesting, harmful and illegal content.

Fortune Magazine observed:

> All along, companies insisted they had policies to respect privacy and empower people to make their own choices. Facebook, at its launch, even sought to distinguish itself from MySpace by

67 'US Congress tries to decode algorithms', *DLA Piper*, 27 January 2022, (accessed 11 November 2022).

68 'Big tech vs. data privacy: It wasn't meant to be this way', *Venturebeat*, 21 May 2022, https://venturebeat.com/datadecisionmakers/big-tech-vs-data-privacy-it-wasnt-meant-to-be-this-way/ (accessed 4 October 2022).

69 'Big tech vs. data privacy: It wasn't meant to be this way', *Venturebeat*, 21 May 2022, (accessed 4 October 2022).

70 'Big tech vs. data privacy: It wasn't meant to be this way', *Venturebeat*, 21 May 2022, (accessed 4 October 2022).

71 'Big tech vs. data privacy: It wasn't meant to be this way', *Venturebeat*, 21 May 2022, (accessed 4 October 2022).

> emphasizing that it would put privacy first. It didn't. After all, no Facebook policies were breached when, in 2016, it facilitated Cambridge Analytica's harvesting of privacy data from more than 87 million Facebook users. And Facebook was not alone; an endless number of companies skim our data without our knowledge or consent.
>
> On the regulatory side, government has been slow and clumsy. Efforts like the European Union's *General Data Protection Regulation*, or GDPR, and California's *Privacy Rights Act*, or CPRA, have attempted to define new rules of the road. The problem is that tech firms move faster than governments and often operate in spaces where they have a significant information advantage over regulators. As a result, even as awareness of data dignity builds, Big Tech remains free to track our movements, gather information about us, and sell those insights as they wish.[72]

In terms of data regulation, the 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.[73]

Data breaches in Australia

The exposure of the personal data of millions of *Optus* and *Medibank Private* customers in September 2022 and October 2022 respectively highlighted this issue here in Australia.

As of 5 October 2022, it appears that 1.2 million *Optus* customers had at least one number from a current and valid form of identification, and personal information, compromised. These included Medicare details and passport numbers.[74]

On Thursday 13 October 2022, healthcare insurer, *Medibank Private*, acknowledged that it too had been the target of a successful cyber-attack. Although initially stating that: "it had not found any customer data that had been compromised",[75] it became apparent within two weeks that: "the company confirmed that hackers accessed personal information on all 4 million of its customers and an unknown number of former members…"[76]

Other recent cyber-attacks have involved the 2.2 million customers of Woolworths' *MyDeal* online marketplace arm whose data was accessed using "compromised" credentials, also during October 2022,[77] and in the breach of ProctorU—a database of 444,000 student records with email addresses belonging to Australian university students.[78]

---

72 Toward data dignity: How we lost our privacy to Big Tech, *Fortune*, 28 January 2022, https://fortune.com/2022/01/28/big-tech-data-privacy-ethicaltech/ (accessed 5 October 2022).

73 'Digital platform services inquiry 2020-2025 – September 2022 interim report', *ACCC* webpage, p. 133, (accessed 25 November 2022).

74 'Deloitte brought in to examine Optus data breach, *ITNews*, 3 October 2022, https://www.itnews.com.au/news/deloitte-brought-in-to-examine-optus-data-breach-585966, (accessed 5 October 2022).

75 'Medibank doesn't know if your data is private after 'incident', *Australian Financial Review*, 13 October 2022, https://www.afr.com/companies/financial-services/medibank-private-hit-by-cyberattack-20221013-p5bpi6, (accessed 28 October 2022).

76 'Display accountability': Customers vent fury as Medibank suffers $1.7b hit', *Sydney Morning Herald*, 26 October 2022, https://www.smh.com.au/business/companies/medibank-confirms-that-every-customer-s-personal-data-was-accessed-in-hack-20221026-p5bsy7.html, (accessed 28 October 2022).

77 'Woolworths says 2.2m MyDeal customers' data hacked', *Australian Financial Review*, 15 October 2022, https://www.afr.com/technology/woolworths-says-2-2m-mydeal-customers-data-hacked-20221015-p5bpzo, (accessed 28 October 2022).

78 For this and further examples of successful hacks on Australian organisations, see: '11 Biggest Data Breaches in Australia (Includes 2022 Attacks)', *Upguard* webpage, https://www.upguard.com/blog/biggest-data-breaches-australia, (accessed 28 October 2022).

The Office of the Australian Information Commissioner (OAIC) periodically publishes statistical information about notifications received under the Notifiable Data Breaches (NDB) scheme. The most recent report, published in February 2022, identified that not all data breaches were malicious, rather many were committed through human error.[79]

The breakdown of cyber incidents was:

- phishing (compromised credentials)—32 per cent;
- compromised or stolen credentials (method unknown)—28 per cent;
- ransomware—23 per cent;
- hacking—8 per cent; and
- brute-force attack (compromised credentials)—5 per cent.[80]

The OAIC report identified the following top causes of human error breaches:

- personal information emailed to the wrong recipient—43 per cent;
- unintended release or publication—21 per cent; and
- loss of paperwork or data storage device—8 per cent.[81]

Human error or not, such breaches should not be taken lightly. The Australian Institute of Criminology noted:

> In 2018–19, the estimated direct and indirect cost of identity crime in Australia was $3.1billion. In 2019 alone, the total losses reported by Australian Institute of Criminology (AIC) online survey respondents was $3.6million. Identity crimes are also notoriously under-reported as a result of inhibiting factors such as victim blaming and the complexity of reporting. The emotional, physiological, and socio-economic impacts faced by victims are often overlooked but can be extreme and prolonged.[82]

In 2021, the former Coalition Government introduced laws to allow the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to access data disruption warrants, which allow them to launch cyberattacks to prevent serious crimes.[83] However, at this stage the ACIC does not have the power to have to address the issues raised with regard to the hacking experienced by Optus and Medibank.

A particular international example

In August 2022, the United Nations (UN) High Commissioner for Human Rights published its report *The Right to Privacy in the Digital Age*.[84] The report focused on: the abuse of intrusive

---

79 A copy of the report can be found at the Office of the Australian Information Commissioner webpage: 'Notifiable data breaches statistics', https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics, (accessed 28 October 2022).

80 'Human error a major factor in data breaches', *MyBusiness*, 24 February 2022, https://www.mybusiness.com.au/resources/news/human-error-a-major-factor-in-data-breaches, (accessed 28 October 2022).

81 'Human error a major factor in data breaches', *MyBusiness*, 24 February 2022, (accessed 28 October 2022).

82 Australian Institute of Criminology, *Statistical Bulletin 37*, 14 December 2021, https://www.aic.gov.au/publications/sb/sb37, and https://www.aic.gov.au/sites/default/files/2021-12/sb37_identity_crime_and_misuse_in_australia_results_2021_survey.pdf, (accessed 5 October 2022).

83 Surveillance Legislation Amendment (Identity and Disrupt) Bill 2021. A copy can be found here: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6623 (accessed 17 November 2022).

84 *The Right to Privacy in the Digital Age*, Report of the Office of the United Nations High Commissioner for Human Rights,https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf, (accessed 5 October 2022).

hacking tools; the key role of encryption in ensuring the enjoyment of the right to privacy and other rights; and the wide-spread monitoring of public spaces.

Part of the UN analysis focussed on the misuse of the of the Pegasus spyware. Designed as a tool for intelligence gathering and counter-terrorism by government, the spyware was also being used by governments to target human rights defenders, dissidents, journalists, activists and politicians.[85]

The UN observed:

> The capabilities of spyware tools and services offered on the global market are formidable. Pegasus, for example, once installed, grants complete and unrestricted access to all sensors and information on infected devices, effectively turning most smartphones into 24-hour surveillance devices, accessing the camera and microphone, geolocation data, emails, messages, photos and videos, as well as all applications. It allows the intruder to obtain a detailed picture of the life of its victims, their thoughts, preferences, professional activities, political thinking, health, financial situation and social and intimate lives. While many hacking tools require some action on the part of the victim, such as clicking on a link or opening an attachment to a message, Pegasus is installed by stealth, through a so-called 'zero-click attack'. The software makes it almost impossible for victims to avoid infection once they have been targeted.[86]

The EU and the General Data Protection Regulation (GDPR)

As part of the European Union's (EU) efforts to keep data safe online, the EU introduced the General Data Protection Regulation (GDPR) which contained new data protection requirements that applied from 25 May 2018.

The European Parliament adopted the GDPR in April 2016, replacing an outdated data protection directive from 1995. It carries provisions that require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The GDPR also regulates the exportation of personal data outside the EU.[87]

The provisions are consistent across all twenty-eight EU member states, which means that companies have just one standard to meet within the EU. However, that standard is quite high and requires most companies to make a large investment to meet and to administer.[88]

While the GDPR has significantly improved the privacy rights of millions inside and outside of Europe, it hasn't stamped out the worst problems. For example, data brokers are still stockpiling information and selling it, and the online advertising industry remains beset with potential abuses.[89]

Wired reported that since the GDPR came into effect, data regulators tasked with enforcing the law have struggled to act quickly on complaints against Big Tech firms and the shadowy online advertising industry, with scores of cases still outstanding. Furthermore, civil society groups

---

85 *The Right to Privacy in the Digital Age*, Report of the Office of the United Nations High Commissioner for Human Rights, (accessed 5 October 2022), p. 3.

86 *The Right to Privacy in the Digital Age*, Report of the Office of the United Nations High Commissioner for Human Rights, (accessed 5 October 2022), p. 3.

87 'General Data Protection Regulation (GDPR): What you need to know to stay compliant', *CSO,* 12 June 2020, https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html, (accessed 17 November 2022).

88 'General Data Protection Regulation (GDPR): What you need to know to stay compliant', *CSO,* 12 June 2020, (accessed 17 November 2022).

89 'How GDPR is failing', *Wired,* 23 May 2022, https://www.wired.co.uk/article/gdpr-2022, (accessed 17 November 2022).

have grown frustrated with GDPR's limitations, while some countries' regulators complain the system to handle international complaints is bloated and slows down enforcement.[90]

As of 2022, there are increasing discussion underway as to how the GDPR can be improved.[91]

Consultation questions:

Question 1: What benefits would arise from introducing a legal mechanism to allow people to seek compensation for privacy breaches in Australia (e.g. establishment of a statutory tort for serious invasion of privacy)?

Question 2: Would stronger penalties levied by government regulation act as an effective disincentive to prevent data leaks and hacks in the future? What should be the scope and size of any such penalties?

Question 3: Do further changes to privacy laws in Australia need to be made to better protect Australians and change corporate attitudes regarding data collection and management?

Children's safety

As described by the Australian Institute of Family Studies, online safety is often used interchangeably with terms such as internet safety, cyber-safety, internet security, online security and cyber security, although these terms can relate to different aspects of online engagement.

For example, 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.[92]

Online safety has been of concern to the Australian Government and society generally. On 30 August 2022, legal notices were sent by Australia's eSafety Commissioner to Apple, Meta, Microsoft, Snap and Omegle, requiring them to explain what they are doing to prevent the use of their platforms for child sexual exploitation, requiring them to respond within 28 days and saying they will face penalties of up to A$555,000 a day if they fail to do so.[93]

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.

---

90 'How GDPR is failing', *Wired,* 23 May 2022, (accessed 17 November 2022).

91 For example, see: '10 years after: The EU's 'crunch time' on GDPR enforcement', *International Association of Privacy Professionals*, 28 June 2022, https://iapp.org/news/a/10-years-after-the-eus-crunch-moment-on-gdpr-enforcement/; 'GDPR Turns Four: Experts Lay Down the Challenges That Lie Ahead', *Spiceworks*, 25 May 2022, https://www.spiceworks.com/it-security/data-security/articles/gdpr-turns-four-challenges-remain/, and '3 Years Later: An Analysis of GDPR Enforcement', Center for Strategic and International Studies, 13 September 2021, https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement, (all accessed 17 November 2022).

92 'Online Safety', Australian Institute of Family Studies, https://aifs.gov.au/resources/resource-sheets/online-safety, (accessed 7 October 2022).

93 'Australian Regulator Asks Big Tech to Detail Online Safety Practices', *PYMNTS*, 30 August 2022, https://www.pymnts.com/big-tech/2022/australian-regulator-asks-big-tech-to-detail-online-safety-practices/, (accessed 12 October 2022).

> 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.[94]

The notices were issued under Australia's Basic Online Safety Expectations, which is part of the *Online Safety Act 2021,* and outlines the minimum online safety requirements expected of tech companies that operate in the country.[95]

Consultation questions:

Question 1: How effective is the current legislative framework in protecting children and preventing online harm from occurring?

Question 2: What more can be done to enhance online safety for child protection in Australia?

The Metaverse

Oxford Languages defines the Metaverse as: "a virtual-reality space in which users can interact with a computer-generated environment and other users".[96] 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 the interaction of avatars. In other words, the concept of a metaverse refers to the migration of various parts of the human experience from the physical world to an increasingly immersive virtual world. It is an embodiment of numerous virtual words, where technology has the opportunity to bring content to those in ways never before imagined and, with it, legal issues and challenges never before contemplated.[97]

Nonetheless, the concept of the Metaverse is new, and still being developed, so it is unclear what the Metaverse will look like. Website *Vice* made the following observation:

> Talking about the metaverse feels a lot like talking about the internet back in the 70s and the 80s. As the building blocks of the new form of communication were being laid down, it sparked speculation around what it would look like and how people would use it. Everyone was talking about it but few knew what it really meant or how it would work. Looking back, it didn't turn out exactly as some people imagined.[98]

Issues with the Metaverse

Potential emerging issues are described below. This list is indicative and not exhaustive.

---

94 '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).

95 'Australian Regulator Asks Big Tech to Detail Online Safety Practices', *PYMNTS*, 30 August 2022, (accessed 12 October 2022).

96 '7 Challenges of The Metaverse', *Lucid Reality*, 4 July 2022, https://lucidrealitylabs.com/blog/7-challenges-of-the-metaverse, (accessed 29 September 2022).

97 'Exploring the metaverse: What laws will apply?' *DLA Piper*, 22 February 2022, https://www.dlapiper.com/en/us/insights/publications/2022/02/exploring-the-metaverse/, (accessed 22 November 2022).

98 'What Is the Metaverse? An Explanation for People Who Don't Get It.', *Vice*, 15 March 2022, https://www.vice.com/en/article/93bmyv/what-is-the-metaverse-internet-technology-vr, (accessed 29 September 2022).

- *Identity*

  Proof of identity can be an issue in the Metaverse as bots can easily mimic an individual's style, data, personality and, indeed, whole identity. It has been suggested that users will need different verification methods like facial scans, retina scans, voice recognition for authentication.[99]

- *Addiction and mental health*

  Addiction to the virtual world may lead to mental health problems like depression, anxiety and cause obesity and heart problems due to the sedentary lifestyle.

  Internet or gaming addictions are already a big problem for kids and adults, and getting hooked on spending all our time in the Metaverse could be an even greater problem in the future.[100]

- *Privacy & data security*

  The Metaverse will be storing more than users' email addresses and passwords. It will store behaviours too. With such a large amount of data, the technology needs to ensure information privacy and personal data security for every user. This will require new security strategies.[101]

  Companies will also be able to monitor our physical reactions as we link to wearable and haptic devices that measure our emotions and physical reactions. Enormous amounts of data could be collected and used by companies for marketing or other purposes.[102]

- *Currency and digital payments*

  The Metaverse will not be limited to gaming. It will be another online marketplace connecting billions of users around the world. With so many currencies and different cryptocurrencies, there will likely be the need for quick and effortless exchanges as well as secure transactions.[103]

- *Law and jurisdiction*

  With social media already witnessing virtual crimes, the Metaverse will also experience criminal activity. Rules and regulations enshrined in proper legislation will be necessary.[104]

---

99 'Challenges faced by the Metaverse in becoming a reality', *DataDrivenInvestor*, 9 February 2022, https://medium.datadriveninvestor.com/challenges-faced-by-the-metaverse-in-becoming-a-reality-d02219d29370, (accessed 29 September 2022).

100 'Challenges faced by the Metaverse in becoming a reality', *DataDrivenInvestor*, 9 February 2022, (accessed 29 September 2022).

101 'Challenges faced by the Metaverse in becoming a reality', *DataDrivenInvestor*, 9 February 2022, (accessed 29 September 2022).

102 'Challenges faced by the Metaverse in becoming a reality', *DataDrivenInvestor*, 9 February 2022, (accessed 29 September 2022).

103 'Challenges faced by the Metaverse in becoming a reality', *DataDrivenInvestor*, 9 February 2022, (accessed 29 September 2022).

104 'Challenges faced by the Metaverse in becoming a reality', *DataDrivenInvestor*, 9 February 2022, (accessed 29 September 2022).

The Metaverse, however, is not going to exist in a real location. It will be a virtual world beyond international borders which means national authorities need to establish their jurisdiction to ensure a secure space for users.[105]

Consultation questions:

Question 1: Given the currently ambiguous status of the Metaverse and its development, is it necessary to begin regulating it now, or should authorities wait in order to understand better how it will function?

Question 2: What regulatory frameworks are required both internationally and in individual jurisdictions to address the risks associated with the Metaverse?

Question 3: How would any regulatory frameworks encompassing the Metaverse be enforced?

International

US Big Tech, and US investment in Australia

Investment from the United States in Australia has, in the past, been very significant and continues to be today. The United States Study Centre noted:

> While US investment into Australia would remain prominent in Australia for the decades after World War II, it was only after foreign investment regulations in Australia were relaxed in the 1980s that US investment into Australia began to look as it does today. From that period to today, US foreign investment into Australia has consistently comprised 25 per cent or more of all foreign investment into Australia — a far larger proportion than any other country.[106]

As it stands today:

> Looking cumulatively, the total US investment footprint in Australia — combining all forms of investment, including direct investment as well as portfolio investment — is valued at A$984 billion and is more than 40 per cent larger than the second-largest total investment footprint in Australia belonging to the United Kingdom at A$686 billion. The US direct investment footprint in Australia, cumulatively valued at A$205 billion, is more than 60 per cent larger than the second-largest direct investment footprint in Australia belonging to the United Kingdom at A$127 billion.
>
> Cumulatively, US firms in Australia employ more, sell more, own more, spend more, export more and contribute more to Australia's GDP than firms from any other country.[107]

This is also reflected in US Big Tech investments in Australia. As examples, here are five large US tech companies that have expanded into Australia:

---

105 'Challenges faced by the Metaverse in becoming a reality', *DataDrivenInvestor*, 9 February 2022, (accessed 29 September 2022).

106 'The role of US innovation in securing Australia's economic future', *United States Study Centre*, 20 August 2020, https://www.ussc.edu.au/analysis/the-role-of-us-innovation-in-securing-australias-economic-future (accessed 18 November 2022).

107 'The role of US innovation in securing Australia's economic future', *United States Study Centre*, 20 August 2020, https://www.ussc.edu.au/analysis/the-role-of-us-innovation-in-securing-australias-economic-future (accessed 18 November 2022).

Reddit

As part of an international push to offer more value to local brands and advertisers, Reddit expanded its business to Australia and opened an office in Sydney in July 2021. The online news aggregation and discussion website has 52 million daily active users globally and Australians make up the site's fourth largest user base, growing at 40 per cent a year. Interestingly, despite this huge number of active users, Reddit only has a few hundred full-time employees, in part because the online communities are managed by thousands of volunteers. [108]

Google

Google has two offices in Australia, one in Sydney and Melbourne, the most recent opened in 2018. The company's engineering hub is in Sydney, while the Melbourne office houses marketing, support, policy sales, and cloud computing staff.[109] In 2021, Google committed to investing A$1 billion in Australia over five years notwithstanding that this was just months after it threatened to pull its services from the country in response to tougher regulation.[110]

Square

Payment platform Square expanded into Australia in 2018 and chose Melbourne as its headquarters, which was a major boost for the city's reputation as a technology and cultural hub. Square announced that Melbourne was the best base for the company's Australian operations given its small business community and growing tech scene.[111]

Airbnb

Home-sharing company Airbnb established an office in Sydney in 2016 to attract more Australian hosts and guests to its online platform. The strategy appears to have worked because Australians have become some of the most prolific users of Airbnb and account for the largest share of accommodation bookings made on Airbnb globally. Sydney was a natural choice for the company's Australian office because it is the heart of the Airbnb community in the country and has strong expertise in the travel and online marketplace industries.[112]

Dropbox

Dropbox—the file hosting service—opened an office in Sydney in 2016, signalling its intent to reach local business users. Dropbox's Sydney office houses sales and user operations departments, in addition to customer support teams for Australian users.[113]

---

108 '6 Major US Tech Companies Have Expanded Into Australia, And Your Company Can Too', *LinkedIn*, 6 August 2020, https://www.linkedin.com/pulse/6-major-us-tech-companies-have-expanded-australia-your-fiona-wong, (accessed 18 November 2022). See also: 'Our favourite online hangouts revealed, as Reddit celebrates one year in Australia', *9News,* 19 July 2022, https://www.9news.com.au/technology/reddit-one-year-australia-favourite-online-hangouts-revealed/15e9c401-0740-4355-8ef7-416870780569; and 'Reddit Turns One Down Under', *Reddit*, https://www.redditinc.com/blog/reddit-turns-one-down-under, (accessed 22 November 2022).

109 '6 Major US Tech Companies Have Expanded Into Australia, And Your Company Can Too', *LinkedIn*, 6 August 2020, (accessed 18 November 2022).

110 'Google commits $740 million to Australia months after threatening to pull its services', *CNBC*, 15 November 2021, https://www.cnbc.com/2021/11/16/google-commits-740-million-to-australia-after-threatening-to-pull-out.html, (accessed 22 November 2022).

111 '6 Major US Tech Companies Have Expanded Into Australia, And Your Company Can Too', *LinkedIn*, 6 August 2020, (accessed 18 November 2022). See also 'Square Opens Office in Australia', *Square*, 21 May 2015, https://squareup.com/au/en/press/square-opens-office-in-australia, (accessed 22 November 2022).

112 '6 Major US Tech Companies Have Expanded Into Australia, And Your Company Can Too', *LinkedIn*, 6 August 2020, (accessed 18 November 2022).

113 '6 Major US Tech Companies Have Expanded Into Australia, And Your Company Can Too', *LinkedIn*, 6 August 2020, (accessed 18 November 2022). See also 'Dropbox to open first office in Australia', CRN, 15 April 2014,

Eventbrite

Australia is one of Eventbrite's fastest-growing markets so it makes sense that the San Francisco-born tech start-up would open an office in Melbourne back in 2014. With 400 employees globally, and a valuation of US$1 billion, the company could have chosen to base itself anywhere, but Eventbrite picked Melbourne. The small—but growing—Australian team supports live experiences in Australia for the online ticketing company.[114]

China and other countries

The US isn't the only country who platforms and companies have come to Australia generating interest from consumers and government authorities alike.

Of particular note is TikTok.

TikTok, (known in China as Douyin) is a short-format video service owned by the Chinese company ByteDance. It hosts a variety of user-submitted videos with durations from fifteen seconds to ten minutes which mostly focus on humour and entertainment.

TikTok was released in the Chinese market in September 2016, and in 2017 for iOS and Android in most countries outside of mainland China. It became available worldwide after merging with another Chinese social media service, Musical.ly, on 2 August 2018.

TikTok has garnered suspicion from western authorities. The webpage CSO noted:

> Both lawmakers and citizens in the US have questioned its data collection practices and potential ties to the Chinese state. The concerns have deepened after Buzzfeed published a report saying that data of some American users had been repeatedly accessed from China.
>
> TikTok's parent company, Beijing-based ByteDance, denied that it shared information with the Chinese government and announced that it had migrated its U.S. user traffic to servers operated by Oracle. Still, it was not enough to clear the air, and security and privacy experts continued to be worried.[115]

CSO argued that once governments get access to data owned by companies, they could leverage this in three primary ways:

- Learning more about citizens and foreigners;
- Intellectual property theft; and
- Highly targeted influence campaigns.[116]

Mikko Hyppönen, chief research officer for WithSecure (formerly F-Secure) commented that the concerns regarding TikTok are only a preview of what's about to come:

---

https://www.crn.com.au/news/dropbox-to-open-first-office-in-australia-382875, (accessed 22 November 2022).

114 '6 Major US Tech Companies Have Expanded Into Australia, And Your Company Can Too', *LinkedIn*, 6 August 2020, (accessed 18 November 2022).

115 '3 ways China's access to TikTok data is a security risk', *CSO,* 15 August 2022, https://www.csoonline.com/article/3670110/3-ways-chinas-access-to-tiktok-data-is-a-security-risk.amp.html, (accessed 21 November 2022).

116 '3 ways China's access to TikTok data is a security risk', *CSO,* 15 August 2022, (accessed 21 November 2022).

China is a rising power online, and this is only the beginning… "China's gross domestic product is growing at a staggering rate. It will catch up with the United States in a few years, bypassing Europe shortly after. China is becoming king of the hill.[117]

Dan Milmo too, writing for *The Guardian*, examined TikTok's activities and the extent to which the information it gathers is used by the Chinese Government. He noted that these concerns are being reflected internationally:

- **United States**: Donald Trump signed an executive order on 6 August 2020 that blocked people from downloading the app, which was followed by an order for TikTok to sell its US business. The order stated:
  - "TikTok automatically captures vast swaths of information from its users, including Internet and other network activity information such as location data and browsing and search histories. This data collection threatens to allow the Chinese Communist party access to Americans' personal and proprietary information."

  This, the order claimed, paves the way for China to track the locations of government employees, build dossiers for blackmail and conduct corporate espionage.

  The orders were never enforced due to legal challenges and then Trump leaving office. Trump's successor, Joe Biden, revoked the orders and instead directed the US commerce department to work with other agencies to produce recommendations 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, after warning that user data was being mined and profiled "by elements hostile to national security and defence of India".
- **Ireland**: the data protection watchdog, which regulates TikTok on behalf of the EU, in September 2021 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."
- **The UK**: Parliament shut down its TikTok account this August after a lobbying campaign by Conservative politicians. In a letter to the speakers of the Houses of Commons and Lords, politicians claimed "data security risks associated with the app are considerable". They also alleged that data from the UK, where the app has an estimated 18 million users, was "routinely transferred to China".[118]

Digital currency and payments issues

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. This is the new frontier of the Big Tech/finance world, and governments and regulators are still grappling with how best to deal with it.

---

117 Cited in '3 ways China's access to TikTok data is a security risk', *CSO,* 15 August 2022, (accessed 21 November 2022).

118 'TikTok's ties to China: why concerns over your data are here to stay', *The Guardian,* https://amp.theguardian.com/technology/2022/nov/07/tiktoks-china-bytedance-data-concerns, 8 November 2022, (accessed 21 November 2022).

With 20 per cent of Australians having owned some form of cryptocurrency, and the emergence of Central Bank Digital Currencies (CBDCs) issued by states that do not share Australia's liberal-democratic values, the need for consumer protection in this space is crucial.

Volatility

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. [119] 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. Its Chief Executive Officer, Sam Bankman-Fried, the 30-year-old founder of the exchange, himself lost US$25 billion.[120] Of particular note is how poorly the company was run, and how the unregulated environment of cryptocurrencies contributed to the collapse occurring:

Mr John Ray III, who oversaw some of the biggest bankruptcies ever, including the collapse of the energy giant Enron, said he had never seen anything as bad as FTX:

> Never in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here.
>
> From compromised systems integrity and faulty regulatory oversight abroad, to the concentration of control in the hands of a very small group of inexperienced, unsophisticated and potentially compromised individuals, this situation is unprecedented.[121]

Stable coins

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 relative to unpegged cryptocurrencies like Bitcoin.

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".[122] It would appear necessary that certain minimum standards must be introduced to ensure that stablecoin issuers provide consumers with at least the minimum standard of consumer protection.

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. Unfortunately, there are as many risks as there are opportunities when it comes to stablecoins.

Central Bank Digital Currency (CBDC)

One response of government is that central banks have begun examining the idea of an official digital version of the national currency. These have become known as CBDCs.

---

119 'Bitcoin's Price History', *Investopedia,* 2 July 2022, https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp, (accessed 18 November 2022).

120 'Crypto crisis continues. Here's the latest on the FTX collapse', *CNN*, 14 November 2022, https://edition.cnn.com/2022/11/14/business/ftx-crypto-collapse-updates-hnk-intl/index.html, (accessed 18 November 2022).

121 'New FTX boss, who worked on Enron bankruptcy, condemns 'unprecedented failure', *The Guardian,* 18 November 2022, https://www.theguardian.com/technology/2022/nov/17/ftx-enron-crypto-collapse-john-ray-unprecedented, (accessed 18 November 2022).

122 'An $85b crypto collapse reveals a new kind of bank run', *Australian Financial Review*, 25 May 2022, https://www.afr.com/technology/an-85b-crypto-collapse-reveals-a-new-kind-of-bank-run-20220524-p5anzq , (accessed 18 November 2022).

As part of this, regulators need to consider the privacy/big state implications. There are numerous privacy issues that could outweigh the benefits, and this is something that requires significant consideration.

The e-Yuan from the People's Republic of China (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 need to closely analyse the development and expansion of the e-Yuan, in conjunction with wider developments in the CBDC space to pre-empt the risks of currency substitution and privacy breaches. Transparency must be part of the solution.

There is a clear link between the Chinese CBDC and Chinese financial institutions and Big Tech organisations. Ahmet Faruk Aysana and Farrukh Nawaz Kayani noted in their article in the *Asia and the Global Economy* journal:

> The goal of the Chinese government is to reduce the power of private entities that offer digital transaction services, such as WeChat Pay and Alipay.[123] The success of these companies demonstrated the rising demand for digital currency and the strong potential for a market in it. Hence, the Chinese government seeks to seize this opportunity and to replace the fiat currency with a digital one that is universally accessible…
>
> Digital currency is already in broad circulation in China. China's payment system is largely dominated by the WeChat and Alipay digital wallets, with hundreds of millions of Chinese using their mobile payment services. Mobile payment and other digital systems have prioritized meeting a narrow set of design requirements, including increasing transaction speed and lowering the cost of use.[124]

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.

---

123 M.J. Kiff, J. Alwazir, S. Davidovic, A. Farias, M.A. Khan, M.T. Khiaonarong, M. Malaika, M.H.K. Monroe, N. Sugimoto, & H. Tourpe (2020). A survey of research on retail central bank digital currency. *IMF Working Papers,* referenced in 'China's transition to a digital currency does it threaten dollarization?', *Asia and the Global Economy*, Volume 2, Issue 1, January 2022, https://www.sciencedirect.com/science/article/pii/S2667111521000232, (accessed 25 November 2022).

124 'China's transition to a digital currency does it threaten dollarization?', *Asia and the Global Economy*, Volume 2, Issue 1, January 2022, https://www.sciencedirect.com/science/article/pii/S2667111521000232, (accessed 25 November 2022).

Consultation questions:

Question 1: How can Australia best approach regulating the increasing number of foreign owned tech companies that have established themselves in Australia?

Question 2: How should western democracies approach the data collection activities of companies based in countries whose political systems are more authoritarian and who may demand access to said data?

Question 3: How should Australia and other countries approach regulation of cryptocurrency, including the CBDCs of other countries?

Big Tech disinformation

Free speech and disinformation

The tension between online free speech, hate speech and disinformation is one that has increasingly occupied the minds of policy makers.

Irene Khan, Special Rapporteur on freedom of expression and opinion, United Nations Office of the High Commissioner, noted that:

> Disinformation online exploits political, economic and social grievances in the real world, and contributes to polarising public debate, eroding public trust in factual, scientific information, inciting violence and hatred against minorities, women and vulnerable groups, threatening human rights, and disrupting democratic and development processes.[125]

Dr MacKenzie Common and Professor Rasmus Kleis Nielsen, writing in a submission to the UN Special Rapporteur, provided a useful discussion of disinformation and free speech.

Disinformation, misinformation, and mal-information is, according to Dr Common and Professor Nielsen, widespread—especially online. Like much online communication of a more benign character, 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).[126]

Problematic information can also be accessed via search engines such as Google Search and other competitors (e.g., Bing, Yahoo, etc.). In addition to sometimes being surfaced by algorithmic ranking systems controlled by platform companies, it is also sometimes monetised by programmatic advertising services offered by the same companies. Smaller platforms such as Twitter, Snapchat, TikTok, can play an important role too, especially for specific forms of problematic information or communities who have been de-platformed elsewhere.[127]

---

125 'In my view: To tackle disinformation, we must uphold freedom of opinion and expression', OECD forum Network, 4 April 2022, https://www.oecd-forum.org/posts/in-my-view-to-tackle-disinformation-we-must-uphold-freedom-of-opinion-and-expression-d5b370e1-e96c-4273-82b2-332548c38c9b, (accessed 31 October 2022).

126 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, https://reutersinstitute.politics.ox.ac.uk/news/how-respond-disinformation-while-protecting-free-speech, (accessed 10 October 2022).

127 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, (accessed 10 October 2022).

According to Dr Common and Professor Nielsen, there is a real risk that the technical and commercial systems run by some of these companies can exacerbate some disinformation problems due to the way in which they incentivise actors (whether political, for profit, or with other motivations) through ranking decisions and through the flow of attention, advertising revenues and other valuable, scare resources.[128]

Increasingly, however, governments take an active and direct role in content moderation online, issues that were in practice left essentially to private companies in much of the world. There are, according to Dr Common and Professor Nielsen, many instances in which governments taking an active role, on the basis of clear and precise legislation, and in ensuring independent oversight, transparency, and due process, is entirely appropriate. But there is also a risk that some governments will pursue responses to disinformation that risk restricting free speech.[129]

Dr Common and Professor Nielsen noted that 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 and can 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.[130]

For example, in April 2020, Facebook announced that it had agreed to 'significantly increase' compliance with requests from the Vietnamese government to censor 'anti-state' content. Facebook's decision came after the Vietnamese government's decision to take Facebook's local servers offline for seven weeks, making the platform inoperable in Vietnam.[131]

Since the announcement, Amnesty International reports, there has been a 983 per cent increase in Facebook restricting content within Vietnam based on local law and Facebook has complied with 95 per cent of the government's requests. Similarly, in late 2020 and early 2021, YouTube and TikTok complied with Turkey's recently amended internet law making it much more susceptible to content removal and take-down requests by the Turkish authorities.[132]

Dr Common and Professor Nielsen provide a four-point set of recommendations on how disinformation issues could be handled in ways that will protect free expression and independent news media.

- *Practical responses*

  Empirical research identifies a number of practical responses to different kinds of disinformation that have been successful at reducing its effect directly or indirectly, reducing its spread, and increasing societal resilience to disinformation problems without infringing on free expression or other fundamental rights.

---

128 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, (accessed 10 October 2022).

129 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, (accessed 10 October 2022).

130 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, (accessed 10 October 2022).

131 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, (accessed 10 October 2022).

132 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, (accessed 10 October 2022).

Countries with diverse and robust independent news media seem more resilient to disinformation and such interventions have a proven track record, and do not restrict free expression or other fundamental rights. Instead of restricting speech, they qualify it. Instead of limiting independent news media, they enable them.

Governments wishing to counter disinformation are well-positioned to encourage the implementation of such measures by mandating transparency reports documenting who does/does not engage in proven examples of good practice, and by providing direct and indirect funding support for independent fact-checking, media literacy, and news media.[133]

- *Legal responses*

  The same standards of human rights protections should be applied to online conduct as are applied to offline conduct, and that the enforcement of legal restrictions on online speech are consistent, transparent, and ensure due process.

  To ensure that measures to counter disinformation protect free expression, states could commit to approaches where any legal restrictions on speech are clearly and precisely prescribed by law, only introduced where they are necessary to protect other fundamental values and are proportional to the specific threat at hand.[134]

- *Platform responses*

  Platforms should align their policies and processes with international human rights principles and point out when they believe that these may be in potential tension with local laws. Indeed "human rights standards, if implemented transparently and consistently with meaningful user and civil society input, provide a framework for holding both States and companies accountable to users across national borders."[135]

- *Oversight, transparency, and due process*

  Greater transparency in how platforms engage in content moderation broadly, and around disinformation specifically, would be an important step. This includes greater transparency, including on the use of artificial intelligence in content moderation around disinformation.[136]

One of Australia's leading law firms, Gilbert and Tobin, examined the tension between free-speech, disinformation and the effectiveness of regulation.[137]

The article argued:

- COVID-19 has accelerated many regulatory measures to address harmful false content online. Two of the swiftest examples are Australia and Europe's disinformation codes of practice. The appropriate scope and enforceability of these codes remains unsettled.

---

133 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, (accessed 10 October 2022).

134 UN Special Rapporteur cited in: 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, (accessed 10 October 2022).

135 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, (accessed 10 October 2022).

136 'How to respond to disinformation while protecting free speech', *Reuters Institute, University of Oxford,* 19 February 2021, (accessed 10 October 2022).

137 'How should Australia regulate disinformation and misinformation, and is that even the right question', *Gilbert and Tobin* webpage, https://www.gtlaw.com.au/knowledge/how-should-australia-regulate-disinformation-misinformation-even-right-question, 8 December 2021, (accessed 31 October 2022).

- Australia's code is the most expansive one yet. The decision to broaden the code's scope was arguably overinfluenced by the galvanizing yet reductive "infodemic" metaphor. However, the code's breadth also reflects the reality that harm can come from false information even when it is spread with good intent.
- The unsettled nature of these codes' scope illustrates how challenging the issue is. Careful code review will be vital to ensure that free speech without fear of persecution, privacy and our "collective sensemaking" in times of crisis are not lost to overregulation.[138]

Online safety and disinformation regulation in Australia

In Australia, there have been a number of reforms aimed at strengthening the online safety.

For example, the Australian Communications & Media Authority (ACMA) explains that the Australian Code of Practice on Disinformation and Misinformation was published in February 2021 by the Digital Industry Group Inc (DIGI). It currently has eight signatories: Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok and Twitter.[139] The ACMA currently oversees the Australian Code of Practice on Disinformation and Misinformation.

This voluntary code aims to provide safeguards against harms from the spread of disinformation and misinformation on digital platforms. On 6 June 2022, DIGI started a review of the code. In June 2021, ACMA provided a report to the then government on the adequacy of digital platforms' disinformation and news quality measures.[140]

The *Online Safety Act 2021*, assented into law in July 2021,[141] expanded Australia's protections against online harm, to keep pace with abusive behaviour and toxic content. The Act makes existing laws for online safety more expansive and much stronger.

According to the e-Safety Commissioner, the *Online Safety Act 2021:*

- creates a world-first Adult Cyber Abuse Scheme for Australians 18 years and older;
- broadens the Cyberbullying Scheme for children to capture harms that occur on services other than social media;
- updates the Image-Based Abuse Scheme that allows eSafety to seek the removal of intimate images or videos shared online without the consent of the person shown;
- gives eSafety new powers to require internet service providers to block access to material showing abhorrent violent conduct such as terrorist acts;
- gives the existing Online Content Scheme new powers to regulate illegal and restricted content no matter where it's hosted;
- brings app distribution services and search engines into the remit of the new Online Content Scheme;
- introduces Basic Online Safety Expectations for online service providers, and

138 'How should Australia regulate disinformation and misinformation, and is that even the right question', *Gilbert and Tobin* webpage, 8 December 2021, (accessed 31 October 2022).

139 'Online misinformation, Australian Communications & Media Authority (ACMA) webpage, https://www.acma.gov.au/online-misinformation, (accessed 21 November 2022).

140 'Online misinformation, Australian Communications & Media Authority (ACMA) webpage, (accessed 21 November 2022).

141 A copy of the law can be found here: https://www.legislation.gov.au/Details/C2021A00076 (accessed 21 November 2022).

- halves the time that online service providers have to respond to an eSafety removal notice, though eSafety can extend the new 24-hour period.[142]

The previous Morrison Government also introduced the Social Media (Anti-Trolling) Bill 2022 into the 46th Parliament. According to the explanatory memorandum, the bill aimed to:

- deem a person who administers or maintains a social media page not to be a publisher of third-party material and thereby be immune from potential liability under defamation law;
- deem the social media service provider to be the publisher of material published on their service that is posted in Australia for the purposes of defamation law;
- create a conditional defence for social media service providers in defamation proceedings that relate to material on their service that is posted in Australia if the provider:
    - has a complaints scheme that meets certain prescribed requirements
    - if a complaint is made—complies with the scheme
    - has a nominated entity in Australia
    - if requested under the complaints scheme—provides the relevant contact details of the person who posted the material said to be defamatory, to assist prospective applicants to identify and commence proceedings against the poster, and
    - if ordered to do so by a court pursuant to an end-user information disclosure order (EIDO)—provides the relevant contact details of the person who posted the material said to be defamatory, to assist prospective applicants to identify and commence proceedings against the poster;
- empower courts to issue EIDOs, which require providers of social media services to give the applicant relevant contact details and country location data in certain circumstances;
- require social media companies to have a nominated entity incorporated in Australia that will be able to discharge key obligations under the Bill; and
- enable the Attorney-General to intervene in defamation proceedings on behalf of the Commonwealth, in certain circumstances, and authorise a grant of legal assistance.[143]

The bill, however, lapsed with the dissolution of the 46th Parliament in April 2022.

Corporate responsibility

Big Tech companies have a corporate responsibility to ensure that their customers and their data are safe. The following section explains what is required of Big Tech companies when establishing their activities in Australia, and some of the responsibilities they must demonstrate.

---

142 'Learn about the Online Safety Act', *e-Safety Commissioner* webpage, https://www.esafety.gov.au/whats-on/online-safety-act,(accessed 21 November 2022).

143 A copy of the bill and its explanatory memorandum can be found here: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6831 , (accessed 21 November 2022).,

The American Chamber of Commerce (AmCham) has described the mechanisms through which US businesses be they Big Tech or otherwise are able to establish themselves in Australia. US companies essentially have two options:

- *A foreign branch*

  This is the establishment of an Australian branch of an existing US business.

  The US business trades in Australia. A foreign branch office is not a separate legal entity, however, the branch must comply with Australian legislation.

  To open and register a foreign branch in Australia, considerable corporate and supporting documentation need to be provided to the Australian Securities Investment Commission (ASIC), much more than starting an Australian company. A branch will then be subject to Australian regulations.

  ASIC requires foreign branches to annually lodge a balance sheet, profit and loss statements and any other documents the company is required to prepare by law in its country of origin.

  No audit is required; however, ASIC has the authority to request audited financial reports if previously lodged reports are insufficient.

  Taxation details of a foreign branch:

  - The foreign branch may not be taxable in Australia depending on whether it constitutes a 'permanent establishment' in Australia. Permanent establishment includes considerations such as a fixed place of business in Australia, the representatives in Australia closing contracts, the plant and equipment in Australia, if construction projects are taking place and how long your staff are spending in Australia.
  - A branch may not have to pay withholding tax.
  - Losses can be utilised in the US company
  - A sale of branch assets will generally be subject to capital gains tax (CGT).[144]

- *An Australian subsidiary company*

  The second option is that a US company establishes an Australian company. This becomes a subsidiary of the US company, and it is this Australian subsidiary company which trades in Australia. In most instances, the US company will own the shares of the Australian company.

  An Australian subsidiary is recognised as a separate legal entity with limited liability and is an Australian resident for tax purposes. The subsidiary can be wholly owned by a foreign shareholder. However. it is required to have at least one Australian resident director.

  ASIC requires Australian companies to submit an annual review statement verifying their shareholders, directors, and addresses with a small annual fee. A solvency resolution signed by the directors must be drawn as well.

  Taxation details of an Australian subsidiary:

144 'Branch vs. Subsidiary - Setting up your Business in Australia', *The American Chamber of Commerce*, https://amcham.com.au/web/Information/Blog_Articles/Branch_v_subsidiary_setting_up_your_business_in_Australia.aspx, (accessed 11 October 2022).

- It is taxed in Australia on taxable income at a rate of 27.5 – 30 per cent , depending on annual turnover.
- Profit repatriation is lost if an unfranked dividend from the Australian subsidiary were to be paid to its parent company.
- Losses are trapped in the subsidiary company.
- A capital gains tax (CGT) exemption may apply upon the ultimate disposal of shares in the Australian subsidiary.

Both branches and subsidiaries are subject to the application of Double Taxation Agreement, of which USA has an agreement.[145]

Directors' duties and obligations

It's important that directors in local branches and subsidiaries of foreign Big-Tech companies 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.

ASIC advise that as a director or officeholder of a company in Australia, key duties include:

- being honest and careful in all dealings;
- understanding what the company is doing;
- making sure the company can pay its debts on time;
- ensuring the company keeps proper financial records;
- acting in the company's best interests, even if this conflicts with the director's personal interests; and
- using any information only for the good of the company. Using information to gain an unfair advantage for oneself or others could be a crime.[146]

If an individual has any personal interests that conflict with their duties as a director, then that individual should disclose these at a directors' meeting.

ASIC further advises that a director's job is to manage the business affairs of a company. The company's constitution (should there be one) may set out a director's powers and functions.

One of the individual's main duties is to understand what the company is doing at all times. A director needs to:

- find out how any proposed actions will affect the company, especially if it involves large amounts of money;
- question managers and staff about aspects of the business if necessary;
- be active and engaged in directors' meetings;
- get independent advice if you need more information to make an informed decision.[147]

---

145 'Branch vs. Subsidiary - Setting up your Business in Australia', *The American Chamber of Commerce*, (accessed 11 October 2022).

146 'Your company and the law', Australian Securities and Investments Commission (ASIC), https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/your-company-and-the-law/, (accessed 11 October 2022).

147 'Your company and the law', ASIC, (accessed 11 October 2022).

A person should only agree to be a director if they understand their responsibilities and are willing to carry them out.

Consultation questions:

Question 1: Is the current regulatory framework governing disinformation and misinformation meeting community expectations and industry? Does is appropriately balance concerns about misinformation with freedom of expression?

Question 2: Should the Australian Code of Practice for Disinformation and Misinformation, which is currently voluntary, be enshrined into the law (as has been done in the EU)?

Question 3: Does the former government's Social Media (Anti-Trolling) Bill 2022 adequately address online safety and, if so, should it be reintroduced to the Parliament?

Question 4: Does the current regime of registering US (and other countries') companies adequately ensure that US Big Tech companies adhere to their corporate responsibilities in Australia?

Conclusion

Through this Issues Paper, the committee has outlined some of the issues it would like to examine more closely. As already mentioned, the summaries above are not authoritative nor exhaustive and are intended to provide a basis for discussion only.

It is clear from the discussion above, that the internet as foreseen in the 1990s hasn't quite developed in the manner expected. As a result of Big Tech's dominance, the anticipated 'democratisation' of the internet has not emerged and threats to security and privacy are increasing as more and more companies have found their security precautions to have been wanting.

The committee wishes to examine these issues in greater detail and through submissions welcomes to the inquiry further insights from subject matter experts into the topics above.

Further reading

The following articles may provide submitters with useful and informative perspectives. This list is not exhaustive and is provided as a starting point for research and discussion only.

Economics/General

Rietveld, J., & Schilling, M. A. (2021). Platform Competition: A Systematic and Interdisciplinary Review of the Literature. Journal of Management, 47(6), 1528–1563. https://doi.org/10.1177/0149206320969791

> Over the past three decades, platform competition—the competition between firms that facilitate transactions and govern interactions between two or more distinct user groups who are connected via an indirect network—has attracted significant interest from the fields of management and organizations, information systems, economics, and marketing. Despite common interests in research questions, methodologies, and empirical contexts by scholars from across these fields, the literature has developed mostly in isolated fashion.
>
> This article offers a systematic and interdisciplinary review of the literature on platform competition by analysing a sample of 333 articles published between 1985 and 2019. The review contributes by: (a) documenting how the literature on platform competition has evolved; (b) outlining four themes of shared scholarly interest, including how network effects generate 'winner-takes-all' dynamics that influence strategies, such as pricing and quality; how network externalities and platform strategy interact with corporate-level decisions, such as vertical integration or diversification into complementary goods; how heterogeneity in the platform and its users influences platform dynamics; and how the platform "hub" orchestrates value creation and capture in the overall ecosystem; and (c) highlighting several areas for future research. The review aims to facilitate a broader understanding of the platform competition research that helps to advance our knowledge of how platforms compete to create and capture value.

Tobin Center for Economic Policy (Yale University), Digital Markets Literature Review (database of articles)

> This literature review surveys the economics research related to antitrust enforcement directed at conduct by digital platforms. The database is organized into five categories—platform competition, the role of apps and complements on the platform, behavioural biases and competition, the role of data on competition, and potential competition—with an additional section that samples the law-related literature on these topics.

Picht, Peter Georg and Freund, Benedikt, Competition (Law) in the Era of Algorithms (May 15, 2018). Max Planck Institute for Innovation & Competition Research Paper No. 18-10, Available at SSRN: https://ssrn.com/abstract=3180550 or http://dx.doi.org/10.2139/ssrn.3180550

> Algorithm-driven computer programs have become key instruments for market success in a digitalized economy. They can generate positive effects on consumer welfare and welfare in general. On the other hand, algorithms may foster tacit collusion, adversely affect consumer choice, even pose a threat to pluralism. Especially since algo-driven market interactions call traditional economic models into question, it is still unclear whether and how the new challenges can be addressed within the existing framework of

(competition) law or whether new legal tools, such as algorithm-focused regulation, must be developed. To approach these questions, the Center for Intellectual Property and Competition Law (CIPCO) at the University of Zurich held a workshop in February 2018. The first part of the workshop focused on technical and economic fundamentals, the second on effects on consumers, and the third part on the existing case-law, as well as on the practice and policy of competition agencies. The paper reflects the discussions and results of the workshop.

Salil K. Mehra, Antitrust and the Robo-Seller: Competition in the Time of Algorithms, 100 MINN. L. REV. 1323 (2016)

Sellers use dynamic-pricing algorithms to gauge supply and demand and set prices not only for books and air tickets online, but increasingly, for consumer electronics, groceries, and other tangible goods in brick-and-mortar stores. An industry has rapidly sprung up to provide software-embedded mathematical models that digest mass-collected data to monitor market conditions and make pricing decisions.

This article offers the first descriptive and normative study of this change and its critically important implications for antitrust law. This article has two goals: first, it provides a descriptive picture of the sea change in commerce that is taking place due to the spread of algorithm-driven dynamic pricing. Second, using that snapshot as a base, this article strives to identify and analyse the broader normative consequences for consumer welfare and antitrust law. To be sure, such an effort to describe and predict the course of a quickly evolving business world must be preliminary at best. But it must be examined, as the change entailed has become too significant and wide ranging to avoid discussion.

Picht, Peter Georg and Loderer, Gaspare, Framing Algorithms – Competition Law and (Other) Regulatory Tools (October 30, 2018). Max Planck Institute for Innovation & Competition Research Paper No. 18-24, Available at SSRN: https://ssrn.com/abstract=3275198 or http://dx.doi.org/10.2139/ssrn.3275198

As other fields of law, competition law is put to the test by new technologies in general and algorithmic market activity in particular. This paper takes a holistic approach by looking at areas of law, namely financial regulation and data protection, which have already put in place rules and procedures to deal with issues arising from algorithms. Before making the bridge and assessing whether the application of any such tool might be fruitful for competition law, the paper discusses important competition cases regarding algorithms, including the Google Shopping, Lufthansa and Facebook case. It concludes with some policy recommendations.

OECD, 2021 OECD Competition Open Day – Replay Panel 2. Digital Ecosystems (video of panel discussion)

Panel II discussed the competition dynamics of digital ecosystems. The panel, composed of Daniele Condorelli, Daniel Crane, Elizabeth Dubois, Amelia Fletcher and Eugene Kanel, was moderated by Ania Thiemann and explored the economics of ecosystems and the role that ecosystems play today in digital markets.

The discussion highlighted how competition in the digital economy is increasingly a competition between ecosystems; how competition between ecosystems may differ from competition between traditional firms; the reasons why some ecosystems succeed while some fail; and the consequences for the enforcement of competition law.

Australia

Australian Competition and Consumer Commission (ACCC), Digital Platform Services Inquiry Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services, Feb 2022

> The characteristics of digital platform markets, such as high barriers to entry due to economies of scale and scope (including in relation to data) as well as significant network effects, have led to and entrench the powerful positions held by some large digital platforms. These market characteristics, in addition to the fast-moving, dynamic nature of digital platform services, have created challenges for traditional competition and consumer protection law enforcement in recent years.
>
> The ACCC has growing concerns that enforcement under existing competition and consumer protection legislation, the *Competition and Consumer Act 2010* (CCA) and the *Australian Consumer Law* (ACL), which by its nature takes a long time and is directed towards very specific issues, is insufficient to address the breadth of concerns arising in relation to rapidly changing digital platform services.
>
> In light of these concerns, and given that this is the half-way point of the Digital Platform Services Inquiry, the ACCC considered this is an appropriate time to assess whether Australia's current competition and consumer protection laws, including merger laws, are sufficient to address the competition and consumer harms that have been identified in relation to digital platform services.

ACCC, Digital advertising services inquiry - final report, Sept 2021

> On 28 September 2021, the ACCC published its final report as part of its inquiry into the markets for the supply of ad tech services and ad agency services.
>
> This report provides in-depth analysis of competition and efficiency in the supply of these services and details its recommendations to improve competition and efficiency in the supply of ad tech services.
>
> (See also: Interim Report, Issues Paper)

Lexology GTDT, Competition in Digital Markets: Australia, November 2021

> Quick reference guide enabling side-by-side comparison of local insights into applicable legislation, enforcement authorities and regulatory guidelines; horizontal agreements; vertical agreements; unilateral anticompetitive conduct; merger control; and recent trends.

International

Veljanovski, Cento, The Competition Economics of Digital Platforms (February 3, 2021). Singapore Economic Review 2021, Available at SSRN: https://ssrn.com/abstract=3923884 or http://dx.doi.org/10.2139/ssrn.3923884

> This article provides an overview of the competitive issues surrounding online platforms. The general theme is that while much has been made of the structural features of online platforms there is little hard evidence that these are durable monopolies. Nonetheless, there are concerns about the behaviour of large online digital platforms arising from their vertical integration, self-preferencing, killer acquisitions, and agglomeration. Developments in and relevance to ASEAN countries are discussed.

APEC Competition Policy and Law Group, Competition Law and Regulation in Digital Markets, March 2022

> The report explores approaches to competition law in digital markets and work in the APEC region on regulating the digital economy by examining approaches across APEC member economies and work underway across APEC on competition and regulatory issues arising from the digital economy.
>
> In particular, the report aims to increase:
>
> - Understanding of how the COVID-19 pandemic has affected the digital economy, the economic opportunities presented for growth, and the challenges for competition and regulatory agencies;
> - Understanding of the interplay between competition law, consumer protection, privacy, and personal data protection when considering issues arising in digital platforms and markets;
> - Practical ways of facilitating cross border cooperation between competition and regulatory agencies that will complement the knowledge base of member economies regarding the policy options and issues arising in digital platforms and markets.

Terry Flew, Fiona R. Martin (eds), Digital Platform Regulation: Global Perspectives on Internet Governance (Palgrave Macmillan, 2022) (e-book)

> This Open Access volume provides an in-depth exploration of global policy and governance issues related to digital platform regulation. With an international ensemble of contributors, the volume has at its heart the question: what would *actually* be involved in digital platform regulation?'. Once a specialised and niche field within internet and digital media studies, internet governance has in recent years moved to the forefront of policy debate. In the wake of scandals such as *Cambridge Analytica* and the global 'techlash' against digital monopolies, platform studies are undergoing a critical turn, but there is a greater need to connect such analysis to questions of public policy. This volume does just that, through a rich array of chapters concretely exploring the operation and influence of digital platforms and their related policy concerns. A wide variety of digital communication platforms are explored, including social media, content portals, search engines and app stores.

Kerber, Wolfgang, Updating Competition Policy for the Digital Economy? An Analysis of Recent Reports in Germany, UK, EU, and Australia (September 14, 2019). Available at SSRN: https://ssrn.com/abstract=3469624 or http://dx.doi.org/10.2139/ssrn.3469624

> All over the world a new critical discussion has emerged about the concentration tendencies in the digital economy and the market power of large digital firms and platforms, like Google, Facebook, Amazon, and others. A particular important question is whether the current competition policies are capable of dealing with these new challenges or whether competition laws have to be amended or complemented by other new policies, e.g. regulatory solutions. This paper analyses four recent extensive reports about this question that were commissioned by the governments of Germany, UK, Australia, and the EU Competition Commissioner Margrethe Vestager (Schweitzer et al report, Furman report, ACCC report, Crémer et al report). In its analysis the paper focuses on the two topics 'platforms, large digital firms, market power, and abusive behaviour' and 'data access/sharing/portability and the specific problems of digital IoT

ecosystems.' An important result is that the reports largely agree on the severity of the market power and competition problems but differ with regard to their main strategies how these problems should be solved.

Schweitzer, Heike and Gutmann, Frederik, Unilateral Practices by Digital Platforms: Facts and Myths about the Reach and Effectiveness of Competition Law (June 1, 2021). Available at SSRN: https://ssrn.com/abstract=3857751 or http://dx.doi.org/10.2139/ssrn.3857751

A frequent starting point of the ongoing debates on a future platform regulation – in the EU in the form of a *Digital Markets Act* (DMA) – is the alleged ineffectiveness of competition law enforcement in the digital realm, and in particular when it comes to 'abuse of dominance' or monopolization proceedings against the largest digital platforms.

This paper aims to do add to this debate in two ways: in a first part, it provides a rough overview of the competition law cases on unilateral practices in digital markets that have been initiated and partly completed over the last ten years or so, with a strong focus on cases against large digital platforms. While there is a focus on the EU and its member states, the overview also looks at relevant cases in other jurisdictions like the U.S., Australia, India, Russia and China in order to give an impression of the global enforcement dynamics.

The overview—which is mostly based on the concurrences database, with only some additional research on our part, which is by necessity selective—does not dive into a discussion of the merits of the cases. Rather, it is meant to systematize the enforcement actions and to provide a clearer picture when, where and why action has been taken on which grounds. A second part strives to draw some tentative conclusions from this overview against the background of ongoing policy debates. Has enforcement indeed been intolerably slow? Does the enforcement panorama indicate what's special about ensuring undistorted competition in the presence of gatekeepers and why we might need a special regime of platform regulation? Does it tell us something about the optimal scope of such a regulation, and about the interaction of com-petition law, the law on unfair business terms and consumer protection law in the digital realm? Does it hold insights about what we can expect from public and private enforcement respectively?

Michael Byowitz , Jacqueline Downes , John Eichlin, Elizabeth Wang & Pierre Zelenko, Navigating the New Competition Law Frontier: Reviewing Global Antitrust Approaches to Technology Platforms, 52 INT'l LAW. 159 (2019)

Large multi-sided technology platforms have redefined how people interact around the world. As network effects concentrate usage onto a relatively small number of platforms (e.g., Amazon, Apple, Facebook, and Alphabet's Google), those firms are increasingly targets of politicians, regulators, and enforcement authorities who express concern about the economic importance of one or more platforms, and whether each has or could achieve dominance. While many antitrust experts argue that traditional antitrust tools are ample to address any legitimate concerns about these firms, others (sometimes referred to as antitrust 'hipsters') question whether more is required to adequately protect consumers, advertisers, or journalists.

The issue is complicated because the application of competition laws to technology platforms in key jurisdictions has been diverging. This article provides an overview of

the current dialogue globally, including the status of enforcement and market studies in Europe, the United States, Australia, China, and other key economies.

Jasper P. Sluijs, Pierre Larouche & Wolf Sauter, cloud Computing in the EU Policy Sphere: Interoperability, Vertical Integration and the Internal Market,
3 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 12 (2012)

cloud computing is a new development that is based on the premise that data and applications are stored centrally and can be accessed through the Internet. This article sets up a broad analysis of how the emergence of clouds relates to European competition aw, network regulation and electronic commerce regulation, which relate to challenges for the further development of cloud services in Europe: interoperability and data portability between clouds; issues relating to vertical integration between clouds and internet Service Providers; and potential problems for clouds to operate on the European Internal Market. These issues are not adequately addressed across the legal frameworks that we analyse and argue for further research into how to better facilitate innovative convergent services such as cloud computing through European policy—especially in light of the ambitious digital agenda that the European Commission has set out.

Jenny, Frederic, Competition Law Enforcement and Regulation for Digital Platforms and Ecosystems: Understanding the Issues, Facing the Challenges and Moving Forward (June 1, 2021). Available at
SSRN: https://ssrn.com/abstract=3857507 or http://dx.doi.org/10.2139/ssrn.3857507

Competition authorities are under severe political pressure to intervene quickly against the digital behemoth for a variety of reasons. Various expert reports have suggested that traditional antitrust or competition law enforcement and merger control are inadequate or insufficient to deal with competition issues in the digital sector.

This paper explores the competition issues raised by digital platforms and ecosystems, the extent to which these issues can be dealt with by competition law and whether regulation could be a complement or a substitute to competition law enforcement.

The paper is divided into three sections. In the first section we look at the economics of digital platforms and ecosystems and their business models. In the second part, the authors analyse the main challenges faced by competition authorities when they apply their traditional analytical tools to antitrust or merger control cases in the digital sector. The third part compares the EU *Digital Market Act* proposal to regulate Gatekeeper platforms and the UK proposal to establish an enforceable code of conduct to govern the behaviour of platforms funded by digital advertising that are designated as having strategic market status.

The paper concludes with a research agenda to help competition authorities avoid the risks of inadvertently giving in to the political pressure of economic populism or ideology or issuing misguided decisions which may be ineffective or, even worse, restrict competition or innovation in the digital sector.

Nyman,Sara; Barajas Aparicio,Rodrigo. Antitrust and Digital Platforms : An Analysis of Global Patterns and Approaches by Competition Authorities (English). Equitable Growth, Finance and Institutions Insight Washington, D.C. : World Bank Group. http://documents.worldbank.org/curated/en/893381632736476155/Antitrust-and-Digital-Platforms-An-Analysis-of-Global-Patterns-and-Approaches-by-Competition-Authorities

The pace at which markets are evolving, thanks to the accelerated adoption of digital technologies, poses important challenges to competition law and its enforcement. This work aims to support this process by building an understanding of the experiences of competition authorities in deciding on competition enforcement cases in the digital economy.

This note analyses the global digital antitrust database of the markets, competition, and technology unit (the MCT DAD or the database) and provides a summary of key patterns and trends in antitrust in the digital economy (and specifically in relation to digital platforms firms). This database aims to be a holistic source of information on abuse of dominance, anti-competitive agreements, and merger cases involving digital platforms, which have been finalized by antitrust authorities worldwide. It also identifies some risks to competition arising from various digital platform business models in different sectors and generates learnings for antitrust authorities globally on the approach to assessing such cases.

The analysis contributes to the discussion and learning on competition assessments in the digital economy. The data also show how different sectors may be prone to different types of anticompetitive behaviour, depending on the typical business models of digital platforms. Antitrust authorities in less developed countries should be encouraged to participate more actively in the debate on data protection and privacy as a dimension of competition. Finally, authorities should continue to strive to make their decisions public and provide clarity about the factors justifying their decisions.

Regulation-'sceptic' perspectives

Pawel Popiel, Yoonmo Sang, 'Platforms' Governance: Analyzing Digital Platforms' Policy Preferences', Global Perspectives (2021) 2 (1): 19094.

Growing political distrust in digital platforms has galvanized policy debates about how to best address issues associated with their market power and ad-run business models—including the proliferation of misinformation, privacy threats, and electoral interference. The range of proposed solutions includes growing calls for public-private policy regimes, such as co-regulation. Such proposals envision a role for digital platforms in addressing platform-related problems, whose contours need to be defined.

In this article, the authors examine how platform companies attempt to influence these debates and define this role, focusing on the biggest US digital platform companies: Amazon, Apple, Google, Facebook, and Microsoft. The authors conduct a content analysis of a sample of 2019 public policy blogs, statements, and testimonies by key personnel at these companies to gain insight into (a) the policy issues they engage, (b) the policy preferences they communicate, and (c) what these communications reveal about their regulatory philosophies and visions of platform governance.

The findings shed light on the politics underlying the debates over platform governance and provide insight into what co-regulatory approaches might look like in practice. The authors call these policy paradigms 'frictionless regulation': light and narrow regulatory oversight confined to baseline standard-setting, receptive to the private sector's ongoing feedback, and prioritizing fast responsiveness to market needs over the slow and deliberative responsiveness to the public that is typical of democratic governance.

Catherine Tucker, 'Network Effects and Market Power: What Have We Learned in the Last Decade?', Antitrust, Spring 2018: 22

> Since the early years of platform and antitrust analysis, network effects have been an important consideration when analysing potential market power. This is because the competitive advantage bestowed by network effects was thought to increase as the size of the firm increased. This article describes three recent advances in the analysis of network effects and, in particular, how the understanding of network effects has evolved in the digital economy. These new findings suggest that network effects are not the guarantor of market dominance that antitrust analysts had initially feared.

Owen, B.M. Antitrust and Vertical Integration in "New Economy" Industries with Application to Broadband Access. Rev Ind Organ 38, 363–386 (2011). https://doi.org/10.1007/s11151-011-9291-y

> Whether the firms that supply Internet hardware and software should face restrictions on the use of their property is an important and controversial policy issue. Advocates of 'net neutrality'—including former US President Obama and the current FCC majority—believe that owners of broadband distribution systems (hardware used to distribute Internet and video services) and producers of certain 'must-have' video content should be subject to prophylactic regulation that transcends present-day antitrust law enforcement. In the economic terms that are used in debates on competition policy, the concern is with vertical integration that may give firms both the opportunity (through denial of access or price discrimination) and incentive (increased profit) to restrict competition. This paper's central point is that virtually every production process in the economy is vertically integrated, and economics predicts changes in the extent of vertical integration—that is, changes in the boundaries of the firm—in response to changes in relative prices, technology, or institutions. Both vertical integration and changes in the extent of vertical integration are benign characteristics of efficient, dynamic, competitive markets.
>
> While there is no shortage of theoretical models in which vertical integration may be harmful, most such models have restrictive assumptions and ambiguous welfare predictions—even when market power is assumed to be present. Empirical evidence that vertical integration or vertical restraints are harmful is weak, compared to evidence that vertical integration is beneficial—again, even in cases where market power appears to be present. Thus, it is reasonable to conclude that prophylactic regulation is not necessary and may well reduce welfare. Sound policy is to wait for ex post evidence of harm to justify interventions in specific cases. Net neutrality, recently enacted by the FCC but subject to judicial review, is an unfortunate idea.