ACCC Digital Platform Services Inquiry

March 2025 Final Report

Google's Response to the ACCC's Issues Paper

13 September 2024

INTRODUCTION

We welcome the opportunity to comment on the ACCC's consultation on the final report of the Digital Platform Services Inquiry (**DPSI 10**). Below, we provide our observations on the following focus areas identified in the ACCC's Issues Paper of 25 July 2024[1] (**Issues Paper**):

- **Topic 1:** international regulatory and legislative developments in markets for digital platform services.
- **Topic 2:** developments and key trends in online private messaging and app stores.
- **Topic 3:** online gaming, cloud and generative AI (**genAI**).

TOPIC 1: INTERNATIONAL REGULATORY DEVELOPMENTS

> The ACCC invites interested parties to share their views on the impact that international regulatory developments, and other significant developments with respect to digital platform services, have had on competition and consumers.
>
> The ACCC acknowledges that in most cases, legislation has only recently been enacted and the full impact of recent international regulatory developments cannot yet be observed. Noting this, parties are invited to provide their views on these developments more broadly, including views on *potential or anticipated* impacts on competition and consumers.

1. Since the start of the ACCC's Digital Platform Services Inquiry, new competition rules targeting digital platforms have been legislated in the European Union (**EU**) (Digital Markets Act (**DMA**)), Germany (s. 19a German Competition Act), Japan (Act on Promotion of Competition for Specified Smartphone Software (**Smartphones Act**)), and United Kingdom (**UK**) (Digital Markets, Competition and Consumers Act (**UK DMCC Act**)). The Issues Paper also refers to India and South Korea who are also assessing the need for similar legislation.

2. To assist the ACCC's consideration of these issues, we share our views on these recent international regulatory developments, and their implications for competition, consumers and innovation in the markets for digital platform services.

3. As a preliminary matter, new rules have only recently come into force in the EU and Germany. There is not yet a body of evidence on the effects of these regimes. As the ACCC acknowledged in its Issues Paper, the full effects of these new regulations cannot yet be observed. Their impact on consumer welfare, innovation, efficiency and competition will take time to be known. Against this backdrop, we make the following observations based on early experience in the EU and recent developments in India, South Korea, Japan and the UK.

[1] See ACCC, 'Digital Platform Services Inquiry - March 2025 - Final Report: Issues Paper', *ACCC Digital Platform Services Inquiry* (25 July 2024) (**Issues Paper**).

Early responses to DMA compliance

4. The DMA came into force for designated companies on 6 March 2024. A number of the DMA rules involve difficult trade-offs that will impact the people and businesses who use our products. We have approached compliance with our DMA obligations with transparency and meaningful product changes even where we have concerns that some rules risk harm to businesses and reduce choice for users in Europe. Early results, following changes made to comply with the DMA, are already showing adverse impacts on a range of European consumers and businesses.

5. The impacts of DMA rules on Search provide some practical examples of unintended negative consequences. Google is continually investing in and innovating its products to improve Search, and to respond to changes in technology and user preferences. However, our early testing in the EU shows that the DMA's outright prohibition of self-preferencing on Search is potentially undoing advances that users and businesses have found useful. This is clearly not a desirable outcome. For example, as a result of the DMA, Google had to remove certain links to Maps from the Search results page in the EU. Google has received feedback from users that they see this as a reduction in the quality of Search in Europe.[2] Users have also publicly complained asking us to bring this back, given how helpful they found this feature.[3] A browser extension to restore Maps links has over 100,000 users according to the Chrome Web Store.[4] Research by the Center for Economic Studies found that the removal of clickable maps from Search has led to an increase of 25% in searches for Maps on Search, increasing the search cost for users.[5]

6. A more detailed description of our concerns with the DMA's Search obligations, including the difficulty of developing a click-and-query data sharing rule that protects user privacy while being useful to search engines to innovate, was provided to the ACCC as part of the September 2024 Digital Platform Services Inquiry on "Revitalising General Search Services" (**DPSI 9**).[6] We don't repeat this information here, but we encourage the ACCC to also consider these issues as part of DPSI 10.

7. The early impacts of the DMA are not only felt in Search. For example, DMA rules that apply to app stores also involve difficult trade-offs, impacting consumers and developers:

---

[2] See comments received from Google users on Google Search Help - Google, 'Google Maps not being linked from Google Search results page', *Google Search Help* (Web Page, 2024).
[3] See e.g., user comments on message boards (for example, Reddit, 'Why doesn't maps show up under Google searches anymore?', *r/GoogleMaps* (Web Page, 2024)) and in our help forum (Google, 'Maps filter missing', *Google Search Help* (Web Page, 2024)). Someone has even created a browser extension to make Maps more accessible (see 'Google Search Maps Button', *Chrome Web Store* (Web Page, 2024)). See also Adam Cohen, 'New competition rules come with trade-offs', *Google's The Keyword* (Blog Post, 5 April 2024).
[4] See 'Google Search Maps Button', *Chrome Web Store* (Web Page, 2024).
[5] Louis-Daniel Pape and Michelangelo Rossi, 'Is Competition Only One Click Away? The Digital Markets Act Impact on Google Maps', *CESifo Working Paper No. 11226* (July 2024).
[6] Google, 'September 2024 report on "revisiting general search services": Google's Response to ACCC Issues Paper', *ACCC Digital Platforms Services Inquiry* (3 May 2024).

Impact on consumers - security, trust and user experience

a. **Risks from DMA alternative billing and linkouts obligations:** The European Commission's (**EC**) interpretation of the DMA's alternative billing requirements and linkouts obligations may create consumer protection and user experience risks.

Play provides a protected and secure environment for users and developers to connect, including through our app review process and integrated billing system, Google Play Billing (**GPB**). GPB was built to the highest privacy and safety standards so that users can be confident making in-app purchases.[7] Users value the safety and security that Play provides. A survey of Android EU users, conducted by Google in partnership with Kantar,[8] found that 87% of those who use GPB trust that when they make in-app purchases in an app downloaded from Play, their payment information will be kept secure. Of those who trust Play, 96% said this trust is influential on their decision to make in-app purchases in apps downloaded from Play.[9]

The EC has interpreted the DMA obligation on billing optionality to permit developers only (rather than users) to choose billing systems, which may result in users not having the option of using GPB at all. An alternative billing system selected by a developer may not offer the same protections or payment options and features of GPB — such as parental controls, family payment methods, subscription management, Play gift cards, and Play Points.

Further, individual developers do not necessarily have the same incentives as Google to act in the interests of users or the Play ecosystem as a whole. Therefore, forcing unrestricted linkouts and allowing developers to offer *only* their alternative billing system (without also offering GPB) could increase security issues and risks poor user outcomes. For example, there is a real risk that consumers who pay through a developer's alternative billing system may face difficulty in obtaining refunds, and in tracking their subscriptions. A 2021 consumer protection lawsuit against Match Group Inc (**Match**) alleged that Match charged customers for automatic renewal of subscriptions without consent.[10] Similarly, in 2023 the US Fair Trade Commission found that Epic Games engaged in unfair and deceptive practices by employing dark patterns aimed at tricking consumers to make unintended in-game purchases.

[7] Discussed in more detail in Topic 2 below, at paragraphs 79 and 80.
[8] The survey was conducted in 2023. Kantar is a global data, insights, and consulting company. For further information, see Kantar, '[About Kantar](#)', *Kantar* (Web Page, 2022).
[9] Kantar survey of a sample of app store users with an Android phone, conducted by Kantar on behalf of Google. See Access Partnership, '[Powering the global app economy: Android and Google Play's contributions](#)', (April 2024), 13.
[10] Match did not admit wrongdoing, but paid US $2 million to settle the lawsuit. See Los Angeles County District Attorney's Office, '[Match.com Settles Consumer Protection Lawsuit](#)', *Los Angeles County District Attorney's Office* (Media Release, 7 July 2021).

The Issues Paper also highlights consumer risks around developers employing manipulative or deceptive design elements.[11] The ACCC Chair has specifically called this out as an ACCC enforcement priority in online gaming:[12]

> "*we will be closely looking at the video gaming industry in particular in-app purchases…Far too often we hear concerns about consumers incurring huge purchases because of in-app offerings that have inadequate safeguards, or in some cases, deliberately target and nudge or confuse consumers.*"

Against this background, the EC's interpretation of the DMA requirements may raise more risks to users. In Topic 2 (paragraphs 53-55) below we discuss Google's User Choice Billing (**UCB**) solution, which we think is a better way to provide developers with additional billing options, while putting the choice in the hands of users.

Impact on small developers and non-paying developers

b. **Artificially splitting Play's service fee is not in developers' or users' best interests:** In the EU, we have introduced the External Offers program[13] in order to comply with the DMA's rules about promotion of external offers.[14] The External Offers program breaks out Play's standard fee into two separate components: (a) a fee for facilitating the initial acquisition of end users, and (b) separately, a fee for Play's ongoing service, which comprises the ongoing tools, technologies and features that support the app throughout its entire lifetime (e.g. delivery of updates, security vetting and developer reporting and analytics). The decision to break out Play's fee is informed by the specific language of Recital 40, which refers to Play being able to charge for "*facilitating the initial acquisition of the end user*".

We consider that this is an artificial split, which does not reflect the value of Play and the full range of features it provides users and developers, nor is it in developers' and users' best interests. The environment of user trust and confidence that Play's service creates and that facilitates transactions is the product of all its features, which operate together as a single, integrated service.

A developer that chooses to disseminate its apps on Play does so in the knowledge that its apps benefit from the ongoing trust, confidence and support that Play creates via its network of sophisticated security, updating and reporting features. Splitting out the components of this service potentially compromises the integrity of this ecosystem and does not reflect the wishes of users (see the results of the Kantar survey referenced in (a) above) or developers:

---

[11] Issues Paper, page 12. For example, "*the use of design elements which may cause users to make unintended purchases*."
[12] See Gina Cass-Gottlieb, 'Committee for Economic Development of Australia (CEDA) speech 2024)', (Speech, Committee for Economic Development of Australia 2024, 7 March 2024).
[13] See Google, 'Enrolling in the external offers program', *Play Console Help* (Web Page, 2024).
[14] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), Art. 5(4).

i. 92% of Play EU developers reported being satisfied or very satisfied with Play as a platform for distributing apps and games, with only 1% dissatisfied.[15] Satisfaction rates were high (at least 89%) across all categories of respondents surveyed.

ii. Similarly, recent engagement with over 100 Australian developers that use Play found that:

- 100% of developers reported being satisfied with the platform.
- 98% of developers agree that Play delivers value across the entire user lifecycle, from installation to retention.
- 97% of developers expect app stores to provide integrated billing services.
- 100% of developers were satisfied with GPB. Developers also found that GPB provides value and see GPB as delivering well against all measured benefits.

c. **Implications for fees:** As described in section 2 below, our fee structure avoids heavy up-front charges that would be harder for small developers to bear. We believe that our business model supports the freemium model, benefits developers, and has facilitated a hugely rich ecosystem of apps for consumers to enjoy.[16]

Some app developers have suggested that the DMA's requirements relating to the treatment of business users by app stores means that app stores should charge upfront fees (to all developers) based on volume of downloads. Notably, Apple has responded to the DMA's requirements by imposing fixed fees for all developers (via Apple's core technology fee).

Such an interpretation of the DMA's requirements risks unintended consequences - namely, favouring the interests of large developers at the expense of small and emerging developers, with implications for future innovation and consumer choice.

The App Association has previously raised concerns that ex ante rules may harm smaller developers:

> "*...policymakers should be wary of opportunistic behaviour by well-resourced competitors disguised as antitrust concern. Those that are most vocal often imply they are speaking for the app economy as a whole, but in reality, they tend to be*

[15] Based on a survey of 500 respondents from 8 European countries conducted by Google in partnership with MTM in September 2023. See MTM, 'Google: European Economic Area (EEA) Developer Attitudes Towards App Stores', *MTM* (Web Page, September 2023).
[16] Play's business model results in 97% of developers not paying fees, and 99% of developers subject to a fee qualify for a fee of 15% or less.

> *larger companies seeking to use antitrust law or other policy levers to undermine competitors.*
>
> *Right now, the largest software platforms generally charge the same (as a percentage of revenue) for developer services regardless of a company's size or political clout, or in some cases less for smaller developers. Smaller developers have the advantage in either of these arrangements because they do not have the leverage to negotiate better terms on their own, as larger companies do.*
>
> *Overtures to have ACCC or other policymakers involve themselves in developer-platform relations, therefore, may benefit the largest software companies on the platforms while leaving small developers like App Association members worse off.*"[17]

8. In addition, there is a clear risk that the DMA's rules will reduce innovation and competition by erecting regulatory barriers to the launch of new products and services in the EU. Despite being a recent reform, these DMA impacts are already becoming observable. For example:

    a. **Apple Intelligence will not launch in the EU this year**: Apple will reportedly not roll out its Apple Intelligence AI product to the EU (together with iPhone Mirroring and enhancements to SharePlay) when it launches later this year due to "*regulatory uncertainties*" arising from the DMA.[18]

    b. **Meta delayed the launch of Threads in the EU**, reportedly due to the DMA.[19] In July 2023, Meta launched Threads (intended to compete more effectively with X) in more than 100 countries, except in the EU.[20] Although Threads was ultimately launched in Europe, this occurred five months after its release in other countries.

9. As the former Italian Prime Minister and President of the European Central Bank Mario Draghi said in his recent report for the EC on the future of European competitiveness, "*innovative companies that want to scale up in Europe are hindered at every stage by inconsistent and restrictive regulations*".[21] As regards the DMA in particular, Draghi noted that it was "*early to fully gauge the impact*".[22] But he also noted the highly complex nature of assessing DMA compliance and the imperative of avoiding "*producing administrative and compliance burdens and legal uncertainties*".[23] He also recognised that if the rules were not applied "*effectively*" then

---

[17] The App Association, 'Comments of ACT | The App Association to the Australian Competition & Consumer Commission's Digital platform services inquiry 2020-2025, September 2022 interim report', *ACCC Digital Platform Services Inquiry* (1 April 2022), 9.
[18] Rohan Goswami, 'Apple Intelligence won't launch in EU in 2024 due to antitrust regulation, company says', *CNBC* (Article, 21 June 2024).
[19] Makena Kelly, 'Here's why Threads is delayed in Europe', *The Verge* (Article, 11 July 2023).
[20] Lauren Feiner, 'Threads, Meta's Twitter competitor, is not yet available in the EU due to regulatory concerns', *CNBC* (Article, 6 July 2023); Jon Porter, 'Threads launches for nearly half a billion more users in Europe', *The Verge* (Article, 14 December 2023).
[21] Mario Draghi, 'The future of European competitiveness - A competitiveness strategy for Europe', *European Commission* (9 September 2024), 2.
[22] Ibid, 79
[23] Ibid, 302 and 79 respectively.

economic damage would follow, including "*the reduced appetite for multinational companies to invest in Europe and the delayed deployment of technological advances*."[24]

10. Consumers benefit from greater choice and from having access to new and innovative products, including from large platforms and other global firms. And the introduction of such products helps increase competition - including between large platforms - which in turn is a key source of further innovation and consumer benefits.

11. Broader long-term implications of the DMA could include a reduction in innovation of emerging AI technologies and possibly other future technologies yet to be developed. This risk is illustrated by Meta's recent decision to withhold its future open multimodal models from the EU and EU companies (albeit reportedly due to the General Data Protection Regulation). According to one commentator, all this could serve to further extend Europe's "*digital winter*".[25]

Other more nascent regimes

12. The other countries mentioned in the Issues Paper are currently developing their own new policy proposals for digital platform ex ante regulation. This is leading to a diverse set of proposals that contain specific elements designed for each jurisdiction. Although nascent, in some instances these proposed ex ante regimes have already attracted significant concern from stakeholders in the relevant jurisdictions.

13. By way of example:

    a. **India:** India's proposed digital platform ex ante regulation, the draft Digital Competition Bill (**DCB**), was released for consultation by the Ministry of Corporate Affairs (**MCA**) on 12 March 2024. The public consultation process and resulting commentary has identified significant concern across a broad group of Indian stakeholders on the move to an ex ante framework and other aspects of the DCB.[26] Media has reported that there are different views within the Indian Government on whether the proposed ex ante framework should be retained in the draft DCB.[27]

    The Dialogue, a public policy think tank in India, commented that alternate modes of intervention must be considered, as: "*the DCB may involve high error costs and capacity demand for the CCI. Further, it may have unintended consequences for the economy and may not be effective in regulating competition in digital markets...the current ex-ante law,*

---

[24] Ibid, 302.
[25] David S. Evans, 'Why Europe Must End Its 30-Year Digital Winter to Ensure Its Long-Run Future', *SSRN* (Article, 18 April 2024).
[26] See SME Connect, 'MeitY seeks inputs from industry, think tanks on digital competition bill', *SME Connect* (Article, 25 June 2024); see Charles McConnell, 'India targets large platforms for ex ante regulation', *Global Competition Review* (Article, 13 March 2024); see Suraksha P, 'Big Tech says ex-ante antitrust regulations will hurt innovation', *The Economic Times* (Article, 30 April 2024); see Yuthika Bhargava, 'Govt panel recommends a digital competition law for big tech, pre-emptive regulations', *ThePrint* (Article, 14 March 2024); see Manu Kaushik, 'Experts wary of digital competition law, says it could throttle innovation, tech transfer', *Financial Express* (Article, 14 March 2024).
[27] See Aashish Aryan, 'MeitY may ask MCA to keep ex-ante out of Digital Competition Bill for now', *The Economic Times* (Article, 15 July 2024).

i.e., the DCB, should be reconsidered".[28] Issues raised by The Dialogue include that the the MCA should only implement an ex ante regime with respect to digital markets after it has gathered: (i) sufficient evidence about its potential efficacy and unintended consequences; and (ii) inputs from a wide group of stakeholders, including micro, small and medium enterprises, startups, gig workers, non-technology companies, think tanks and civil society.[29]

Similarly, in its public submission on the draft DCB, the Computer & Communications Industry Association (**CCIA**) commented:

> "*CCIA strongly believes that, to determine if there are any potential competition concerns that need to be addressed through regulation, it is paramount for Indian policymakers to understand the various digital business models and services fully and accurately, as well as the industries in which they operate. As such, when proposing any ex-ante regulatory framework for digital markets, Indian policymakers must consider market realities and how the proposed regulation might affect businesses, consumers, and the country's overall economy.*"[30]

Most recently, Professor Viswanath Pingali of the Economics faculty of the Indian Institute of Management Ahmedabad considers: "*The DCB could benefit from several changes to better accommodate the dynamic nature of digital markets. Incorporating exemptions that allow the regulator to consider the pro-competitive effects of conduct would be a first step in balancing regulatory oversight with the ability to leverage the benefits of digital platforms.*"[31]

There appears to be uncertainty on the future progress of the draft DCB given the significant concerns that have been raised by stakeholders and it remains subject to ongoing discussion between Indian policy makers and the digital sector.[32] As recently as 7 September 2024, Competition Commission of India (**CCI**) Chief Ravneet Kaur commented that the Indian government and the CCI are considering whether to raise the thresholds for designating digital platforms as part of the draft DCB following feedback received during the public consultation process.[33]

[28] See The Dialogue, 'Written Comment: Report of the Committee on Digital Competition Law and The Digital Competition Bill, 2024', *Report of the Committee on Digital Competition Law and The Digital Competition Bill, 2024* (15 May 2024), i.
[29] Ibid.
[30] See Computer & Communications Industry Association, 'CCIA Comments on the Report on Digital Competition Prepared by the Indian Ministry of Corporate Affairs' Committee on Digital Competition Law and Draft Digital Competition Bill', *Report of the Committee on Digital Competition Law and The Digital Competition Bill, 2024* (2024), 1.
[31] See Viswanath Pingali, 'A case for nuance', *Financial Express* (Article, 12 August 2024).
[32] Giresh Chandra Prasad, 'Digital competition bill pushed to next year amid turf war, big tech pushback', *Mint* (Article, 9 September 2024).
[33] Charles McConnell and Victoria Ibitoye, 'India plans to revise digital competition bill following stakeholder criticism', *Global Competition Review* (Article, 9 September 2024).

b. **South Korea**: In South Korea, the introduction of the draft Platform Competition Promotion Act (**PCPA**) attracted fierce backlash and the draft legislation has not been progressed through the National Assembly. Criticism included:

i. The Centre for Strategic and International Studies (**CSIS**), a nonprofit policy research organisation, commented at the time that the proposed PCPA may create "*national security implications*" and that "*the emerging competition policy frameworks also entail compliance costs that may be passed on to consumers and small businesses.*"[34]

ii. The Information Technology and Innovation Foundation, a leading think tank for science and technology policy, also criticised the PCPA at the time, including the risk of preventing pro-competitive behaviour and stifling innovation:

> "*Shifting from evidence-based law enforcement to heavy-handed digital regulation could stifle the innovation Korea needs and lead to various unintended consequences. As the Korean proverb goes, it's unwise to "burn down the hut to catch a bedbug".*
>
> *Inspired by the European Union's (EU) Digital Markets Act (DMA), the act fails to appreciate the important differences between European and Korean digital markets.*
>
> *...the PCPA's potentially strict provisions could prohibit pro-competitive behavior. For example, per se bans on self-preferencing would condemn behavior that is not only ubiquitous across the digital economy but almost always leads to a better user experience by integrating various products and services and increasing the platform's competitiveness.*
>
> *...the PCPA is a solution in search of a problem, and Korea should prioritize fostering innovation through its existing and robust law enforcement tools.*"[35]

The Opposition has introduced its own bill, the Online Platform Antitrust Regulation Act. CSIS has similarly criticised this bill, including that "*the bill may only raise costs for the South Korean small and medium-sized enterprises (SMEs) and consumers it seeks to protect*"; and "*the bill may have unintended consequences, similar to the DMA*".[36]

Relatedly, the Korean Venture Business Association has warned that, "*by stifling platforms that have grown to a certain size, the South Korean bill could inadvertently discourage*

[34] William Alan Reinsch and Kati Suominen, '[Korea's Move to Ex Ante Competition Regulation Discriminates against U.S. Business]', *Center for Strategic & International Studies* (Article, 11 January 2024).
[35] Lilla Nóra Kiss, '[Will Korea Burn Its Digital Future Down]', *Information Technology and Innovation Foundation* (Article, 12 June 2024).
[36] Kati Suominen, '[South Korea's New Digital Competition Bill: A Step Backward for Innovation and Investment]', *Center for Strategic & International Studies* (Article, 16 August 2024).

venture investment into platform startups and deter foreign investment, ultimately deterring innovation."[37]

On 9 September 2024, the Korean Fair Trade Commission announced that the Korean government (and ruling party) will no longer seek to legislate an ex ante approach such as the proposed PCPA. It will instead seek to amend the existing Monopoly Regulation and Fair Trade Act.[38] The proposed amendments adopt a "ex-post presumption" model (instead of a model under which certain platforms are designated). Under the new framework, if a "dominant platform"—defined as having a market share of over 60% and annual sales exceeding 4 trillion won—engages in certain prohibited practices, the business will have to prove that its actions were not anti-competitive.[39] Given there is no political consensus across the various Korean political parties on these issues at present, it remains unclear whether any significant changes to digital platform competition regulation will be enacted in the near future.

c. **Japan**: In Japan, the recently enacted Smartphones Act is narrower in purpose and scope than the DMA. The Smartphones Act's purpose is to clarify but not expand existing competition law in Japan, and its scope is limited to specified services provided on smartphones. The Diet has taken a significantly different approach to the DMA with the legislation including protections and safeguards that seek to ensure it does not impede innovation, security, privacy and user convenience.

The detail underpinning the new regime is still to be developed in public consultations led by the Japan Fair Trade Commission (**JFTC**). We have already seen that some stakeholders have been warning about potential harms if the new rules are not appropriately implemented. For example, Shigeru Kitamura, president and CEO of Kitamura Economic Security, raised concerns about companies being forced to open their platforms, commenting at a panel discussion that "*competition should not come at the cost of security.*"[40]

The Information Technology and Innovation Foundation has also raised significant concerns and offered the following recommendations:

i. "*The JFTC should first leverage its existing tools to address specific anti competitive behaviours as they occur and only implement new laws if the current ones are incapable of responding to new challenges.*"[41]

ii. "*The* [Smartphones Act's] *broad, per se prohibitions fail to distinguish between practices that harm competition and those that enhance consumer welfare. If*

[37] Ibid.
[38] Jung Min-Hee, 'FTC Abandons Pre-Designation System, Amending Fair Trade Act to Regulate Platform Monopolies', *BusinessKorea* (10 September 2024).
[39] Ibid.
[40] Mackenzie Holland, 'South Korea, Taiwan, Japan monitor EU's Digital Markets Act', *TechTarget* (Article, 19 July 2024).
[41] Joseph V. Coniglio and Lilla Nora Kiss, 'Comments to Japan's Fair Trade Commission Regarding the Smartphone Software Competition Promotion Act', *Information Technology & Innovation Foundation* (Article, 3 September 2024).

enacted, the [Smartphones Act] *is highly likely to chill procompetitive conduct that benefits consumers and innovation, thus stifling the growth of the very markets it seeks to promote.*"

iii. "*Japan's strong alliance with the United States is critical amidst the global technology race against China. In this vein, the JFTC should consider how the* [Smartphones Act] *could have negative effects not just in the form of hindering Japanese innovation, but by targeting American companies, like Apple and Google.*"

i. "*The competitive position of Japanese companies should not be the focus of the* [Smartphones Act], *especially in the digital space. Many, if not all, of the proposed changes here would end up making Japanese digital consumers' lives worse, not better.*"

d. **UK:** The UK conducted an exhaustive process over a substantial period in developing its own digital competition regime. This culminated in the UK Parliament passing the UK DMCC Act in May this year. The UK DMCC Act institutes a tailored company-specific approach and is a significantly different regime to that established by the DMA. The draft legislation received widespread criticism during the public consultation process, including that it may create uncertainty in its application and chill innovation in the UK. For example:

i. The CSIS commented: "*Giving an unprecedented amount of power to a single regulatory body with few checks and balances, however, promises to transform the UK business environment for digital firms, creating serious concerns for the attractiveness of the United Kingdom for tech investment. These dramatic changes should be weighed with care and circumscribed judiciously – particularly for UK entrepreneurs, who may find a more accommodative regulatory environment in Boston or Silicon Valley*".[42]

ii. The Institute of Economic Affairs raised concerns that the broad discretion and enforcement powers afforded to the Competition and Markets Authority (**CMA**) under the regime will have unintended consequences for consumers, such as:

"*It endows the CMA, acting through the newly created Digital Markets Unit (DMU) with extensive new powers to categorically prohibit certain types of conduct at an incipient stage and impose far-reaching remedies with limited consideration of countervailing consumer benefits…*

In addition, the procedural safeguards contemplated by the Bill may enable overenforcement in ways that hurt consumers. In practical terms, this could mean new products will not be developed in the UK and that new features could be delayed or not introduced for British users, as firms seek to minimise the risk

[42] Meredith Broadbent, 'UK Digital Markets, Competition and Consumers Bill: Extraterritorial Regulation Affecting the Tech Investment Climate', *Center for Strategic & International Studies* (Article, 4 March 2024).

of falling afoul of the new regime and incurring hefty fines and stringent remedies. This could, in turn, deter post-Brexit investment in the British economy and damage job creation in high-tech industries."[43]

iii. The Centre for Policy Studies was similarly concerned about the potential for the UK DMCC Act to create an uncertain regulatory environment for businesses, and lead to a lack of innovation for consumers: "*The extent of these powers and the lack of restraint on their use creates an uncertain and unpredictable policy environment for businesses. This will make it harder for firms to bring new services to market. It will therefore over time lead to consumers in the UK no longer being among the first in the world to access many new digital tools, and undermine the UK's place as a prime destination for global tech investment.*"[44]

14. As a result of this criticism, the UK Government made significant changes to the original draft of the UK DMCC Act that were ultimately legislated. This includes a proportionality requirement whereby the CMA cannot impose a conduct requirement or pro-competition intervention on a firm unless it is proportionate to do so and there is a strong evidence base behind the intervention.

Implications for Australia

15. We acknowledge that the Government is progressing work on the design and form of a possible legislative framework which could enable the creation of service-specific codes, and that it is closely monitoring international developments.[45]

16. We reiterate our previous submissions about the importance of being satisfied that regulation will deliver net benefits, and the need to undertake a thorough cost/benefit analysis. The costs in this context are not simply costs of compliance for digital platforms and the costs of administering new regulation — they include impacts on business and economic effects such as distortion of competition, reduced incentives or ability to innovate, and higher input or production costs. They also include resulting impacts on consumers such as higher prices and reduced utility (quality, choice etc) of products. Firms may be forced to roll out localised versions of platforms to Australia in order to comply with regulations, which may delay or deny Australians access to global advancements and updates associated with those platforms. There may also be costs to the community such as lower economic growth. Some of these costs are already being seen in Europe, as described above.

17. We note that ACCC Chair, Gina Cass-Gottlieb, recently commented that the DMA reforms are estimated by the European Parliament to increase consumer surplus by €13 billion (or AUD$21.4 billion) per year, suggesting that the "*potential for economic benefit from such measures is*

[43] Dirk Auer, Matthew Lesh and Lazar Radic, 'Digital Overload: How the Digital Markets, Competition and Consumers Bill's sweeping new powers threaten Britain's economy', *Institute of Economic Affairs* (Article, 18 September 2023).
[44] Matthew Sinclair, 'The unregulated regulator: How the Digital Markets, Competition and Consumers Bill could undermine dynamism in digital markets', *Centre for Policy Studies* (Research Paper, 29 June 2023), 1-2.
[45] Australian Government, 'Government Response to ACCC Digital Platform Services Inquiry', (8 December 2023), 4.

significant."[46] We believe that a more robust analysis of consumer surplus is required to support such far-reaching regulatory change in Australia.

18. The quoted consumer surplus estimate was taken from the 2020 EC DMA Impact Assessment (**Impact Assessment**), which comes with a number of significant caveats. Notably footnote 271 itself states that "*such quantification remains a highly theoretical exercise*".[47] The European Parliamentary Research Service (**EPRS**), whose role is to provide independent, objective and authoritative analysis of policy issues for Members of the European Parliament, critically evaluated the strengths and weaknesses of the Impact Assessment and noted the following specific problems with the methodology used:

    a. First, the EPRS found that, in comparing the efficiency of different regulatory intervention options, the EC had used a "*qualitative methodology*" conditioned by a "*lack of reliable data, which the* [Impact Assessment] *acknowledges openly*".[48] In general, the EPRS found that the "*assessment and comparison is in many respects a qualitative exercise*".[49] This leaves the €13 billion consumer surplus estimate with little quantitative support.

    b. Second, "*[t]he* [Impact Assessment] *does not quantify the impact of the options on SMEs, with the lack of reliable data cited in the* [Impact Assessment] *possibly playing a part in this*".[50] This methodological choice could mean that the figures overlook significant costs to SMEs of imposing these options.

19. We urge the ACCC and Australian Government to undertake a more comprehensive, evidence-based assessment of the costs and benefits of an ex ante digital platform regime. As described above, early results following changes made to comply with the DMA are already showing adverse impacts on a range of European consumers and businesses. We encourage the ACCC and Australian Government to benefit from observing the real-world impacts of the DMA and other nascent regimes in due course, and refining their view of the benefits of an appropriate ex ante regime for Australia based on robust quantitative and qualitative analysis. We believe that global leadership in digital regulation will be achieved by the countries that implement ex ante regulation "best" (that is, without risks to innovation, consumers and their economy), not necessarily the countries that do it first.

20. We also note that the Government is considering a raft of reforms to competition and consumer laws that are also likely to have impacts on digital platforms, including a new merger control regime, the introduction of a prohibition on unfair trading practices, a new scams code framework, a reset of the consumer data right regime and changes to "bedrock" competition

[46] Gina Cass-Gottlieb, '[ACCC/AER Regulatory Conference 2024 opening address]', *ACCC/AER Regulatory Conference* (Speech, 1 August 2024).
[47] European Commission, '[Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector]', (15 December 2020).
[48] European Parliament, '[Initial Appraisal of a European Commission Impact Assessment]', *Digital Markets Act* (May 2021), 6.
[49] Ibid, 8.
[50] Ibid, 6.

law policy through Treasury's consultation on "Revitalising National Competition Policy".[51] In addition, on 7 September 2024 the Department of Industry, Science and Resources published a Voluntary AI Safety Standard[52] and opened consultation on new AI laws[53] in the form of a proposal paper to introduce mandatory guardrails for AI in high-risk settings. The proposal paper outlines the need for a regulatory framework to mitigate risks associated with AI in high-risk settings, enhance public trust, and ensure the safe and responsible use of AI technologies. We urge the ACCC and Australian Government to consider the potential overlaps between these reforms with new ex ante digital platform regulation proposals, and the cumulative impact. As Mario Draghi observed in his recent report on the future of European competitiveness, the accumulation of tech-focused laws and regulators in the EU has led to a "*regulatory stance towards tech companies that hampers innovation*".[54]

Necessary safeguards in any new regulatory framework

21. Any Australian ex ante regime should promote pro-consumer outcomes and not dampen incentives to innovate and invest. To achieve this, we believe the overarching regulatory regime must contain the following elements:[55]

    a. **Enhancing consumer welfare:** Promoting competition and innovation, and enhancing the welfare of consumers, should be the ultimate objectives. The framework should not permit obligations that promote the interests of individual competitors.

    For example, consumer benefits is also an overarching defence in the UK and German ex ante regimes. Additionally under the UK DMCC Act, the CMA cannot impose a conduct requirement on a designated firm without first considering its likely consumer benefits, and those benefits must be set out in the CMA's reasons for imposing the requirement.

    b. **Proportionate obligations:** Rules on conduct (and the consequences of non-compliance) should be necessary and proportionate to the seriousness of the anticipated harm and the likelihood of it occurring.

    For example, under the UK DMCC Act, in order to impose a conduct requirement, the CMA must consider that it would be proportionate to impose the conduct requirement for the purpose of one or more explicit statutory objectives. It remains to be seen how this requirement is implemented in practice.

---

[51] Australian Government, 'Revitalising National Competition Policy Consultation Paper', (August 2024).
[52] See Department of Industry, Science and Resources, 'Voluntary AI Safety Standard', *Australian Government* (Standard, 5 September 2024).
[53] See Department of Industry, Science and Resources, 'Introducing mandatory guardrails for AI in high-risk settings: proposals paper', *Australian Government* (Consultation, 5 September 2024).
[54] Mario Draghi, 'The future of European competitiveness - A competitiveness strategy for Europe', *European Commission* (9 September 2024), page 26.
[55] Consistent with the six principles we outlined in Google, 'September 2022 Report on updating competition and consumer law for digital platform services: Google's Response to the ACCC's Discussion Paper', *ACCC Digital Platform Services Inquiry* (8 April 2022), 3-4 (**Google's DPSI 5 submission**).

c. **Safeguards and justifications:** Evidence-based justifications for conduct under scrutiny should be embedded in the overarching framework.

Such justifications are a feature of the UK DMCC Act, the Japanese Smartphones Act and the German ex ante regime.

Our experience to date shows that blunt rules that seek to redesign products, with no safeguards to allow for the assessment of consumer or business benefits, risk causing serious unintended harm. We note that in the global debate on potential ex ante rules for digital platforms, many stakeholders have expressed concerns about the lack of safeguards in the DMA:

i. Experts consistently call for allowing "*an explicit and well-framed defence*", to prevent the unintentional outlawing of beneficial conduct and depriving Europeans of the benefits that such conduct brings.[56]

ii. Advocate-General G. Pitruzzella has explained that "*too much rigidity could hinder efficiency and introduce a disproportionate limitation on the freedom to conduct a business*".[57]

iii. The German Monopolies Commission "*considers that there are weighty reasons to supplement the DMA to include an efficiency defence on a case-by-case basis*"; it recommended allowing firms to defend their conduct by showing it "*promotes technical development or economic progress*".[58]

iv. Professor Richard Whish has described the DMA as having been shaped by "embryonic" abuse of dominance cases. For Whish, the DMA's rules are based on theories of harm that are not yet conclusively anticompetitive.[59] This is particularly dangerous if there is no scope to justify deviation from these rules.

---

[56] Luis M. B. Cabral et al, 'The EU Digital Markets Act: A Report from a Panel of Economic Experts', *Boston University Questrom School of Business Research Paper No. 3783436* (18 February 2021), 9 ("*one of the main challenges in the implementation of the DMA is how to separate the positive efficiency and welfare gains that platforms generate* [...] *from negative anti-competitive and welfare-reducing platform behaviour* [...] *Pro-competitive remedies should not undermine the efficiency gains of platforms*"); Centre on Regulation in Europe, 'The European proposal for a Digital Markets Act: A first assessment', (19 January 2021), 22 ("*given that many practices in the digital economy have multiple positive and negative effects on contestability and fairness (as well as on welfare and innovation) and the (still) many unknowns in competitive dynamics of digital technologies and markets, it is appropriate to provide for an explicit and well framed defence that could be brought by the gatekeepers.*"); Nicholas Hirst and Lewis Crofts, 'Comment: EU's 'mechanical' approach to Big Tech regulation in the spotlight', *MLex* (15 February 2021) ("*Blunt rules will make it harder for Big Tech players to innovate, and may degrade consumers' enjoyments of their services*"); Jennyfer Chrétien and Henri Isaac, 'Digital Markets Act: A Revolution or a Legal Contradiction?', *Renaissance Numérique* (29 March 2021) ("*the proposed DMA introduces a sort of presumption of competitive guilt*").

[57] Nicholas Hirst and Lewis Crofts, 'EU gatekeeper regulation raises questions of 'proportionality,' member of top court says', *MLex* (Article, 10 March 2021).

[58] Monopolies Commission, 'Recommendations for an effective and efficient Digital Markets Act', (5 October 2021), para 131-138 for rationale.

[59] Janith Aranze, 'DMA obligations influenced by unresolved tech cases, Whish says', *Global Competition Review* (Article, 13 July 2022).

d. **Appropriate legal rights:** Suitable protections and review mechanisms should be incorporated to ensure the integrity of a new regulatory framework. As under the *Competition and Consumer Act 2010* (Cth) today, the Federal Court should be responsible for determining whether a breach of the regime has occurred. Full merits review by a Court should be available (where appropriate) for decisions that have legal consequences.

As the Constitution requires, and consistent with how the *Competition and Consumer Act 2010* (Cth) operates today, the task of formally deciding whether a company has breached an ex ante rule - or can justify its conduct under the regime - should be assigned to the Courts, along with the determination of any penalties. This will act as a crucial safeguard to encourage objective and disciplined decision making, and allow errors and shortcomings to be corrected by an independent tribunal.

The DMA contains a merits review to the EC Courts where all errors of fact and law can be appealed. The UK DMCC Act is lacking in this respect - all appeals against CMA decisions can only be brought on judicial review principles, except for appeals against penalty decisions (which will be determined on the merits).

e. **Separation of powers in the making of rules and enforcement of rules:** There should be a separation of powers between the bodies making rules (and if applicable, designation) and enforcing the rules.

The DMA is based on a model under which rules are made by Parliament, and enforced by the competition regulator. By contrast, under the UK DMCC Act, the CMA is responsible for designating platforms, imposing conduct requirements and enforcement. The UK has sought to minimise the risks of actual or apparent bias and conflicts of interest in the CMA's decision making processes[60] through statutory safeguards embedded within the *Enterprise and Regulatory Reform Act 2013* (**EERA**) which require separation between decision makers within the CMA. These requirements also apply to the CMA's role and functions under the UK DMCC Act.

We consider that using different institutions for making the rules and enforcing the rules is a more effective way to deal with the risks discussed above. Importantly also, it is critical that the body responsible for making the rules possesses or has access to considerable expertise and knowledge of technology markets in order to design and/or apply regulatory solutions that are evidence-based.

[60] For example section 49 of the EERA provides that separately constituted CMA groups must act independently of the CMA Board. Section 51 of the EERA provides that each CMA group must have their own rules of procedure.

TOPIC 2: MAJOR DEVELOPMENTS IN DIGITAL PLATFORM MARKETS

> The ACCC invites interested parties to share their views on whether there have been any major developments or key trends in the markets for online private messaging and app marketplaces since the ACCC completed its previous reports on these topics in September 2020 and March 2021 respectively.
>
> Parties are also invited to share their views on further major developments or key trends in services or markets considered in other earlier reports of the Inquiry (that is, those published prior to September 2022).

Topic 2 - 1.2.1: Report on Online Private Messaging

22. We make the following observations to assist the ACCC's further consideration of online private messaging.

Our messaging and video conferencing products

23. Since the ACCC released its first interim report in September 2020 (**DPSI 1**), there have been changes to our online messaging and video conferencing products. In 2020, we replaced Google Hangouts (our online instant messaging or chat service) with Google Chat,[61] and in 2022 we upgraded and rebranded Google Duo (our video call service) to incorporate it into Google Meet.[62] But consistent with the data in the Issues Paper, we remain a relatively small supplier of online messaging and video calling services in Australia and globally, as compared to Apple (iMessage and Facetime) and Meta (WhatsApp and Messenger).[63]

24. The relevant products that we currently offer, and some of their important privacy and safety features, are described in **Annex A**. Importantly, we don't use content or other information from Google Messages, Google Meet or Google Chat, for advertising purposes.

Our efforts to protect user privacy and combat scams

25. We recognise that as the internet and smartphones have integrated into our daily lives, scammers are applying a variety of deceptive tactics across a range of always expanding channels like fraudulent messages, alluring offers, impersonation and more.

26. To help combat this, we have focussed on developing messaging technology with built-in security measures: a secure-by-default approach.[64] For example:

---

[61] Ravi Kanneganti, 'Upgrading from Google Hangouts to Google Chat', *Google's The Keyword* (Blog Post, 27 July 2022).
[62] Google, 'FAQ: Transition from legacy calls to the new Meet calling experience', *Google Meet Help* (Web Page, 2024).
[63] Issues Paper, 9-10.
[64] Lucinda Longcroft, 'How we're stopping scams and working to create a safer internet', *Google Australia Blog* (Blog Post, 6 February 2024).

a. Google Messages provides end-to-end encryption (or, in the case of meetings on Meet, cloud encryption).[65] With end-to-end encryption, no one, including Google and third parties, can read eligible messages as they travel between a user's phone and the phone they message.[66]

b. Google Messages identifies over 2 billion spam messages a month. Many of these are automatically moved to a spam folder before the user sees the message. In other instances, a spam warning banner appears when a user opens the message. Google Messages is the highest rated built-in texting app for anti-phishing and scams protection according to analysts reports.[67]

c. As discussed further below, we have sought to improve and encourage industry adoption of the Rich Communication Services (**RCS**) standard for messaging, which helps combat scams as described below in paragraphs 29 to 32.

d. Android enables third-party app developers to readily include end-to-end encryption in messaging apps, as well as contact verification with participating contacts apps on a user's device.

27. More broadly, we combat scams on our online private messaging services through a combination of:

a. Google policies: For example, Google Chat's Acceptable Use Policy[68] prohibits use of the product to:

i. Send or facilitate the transmission of spam, large numbers of commercial messages, or automated messages or calls.

ii. Phishing, including soliciting or collecting sensitive data such as passwords, financial details and social security numbers, and impersonating another person.

iii. Transmit malware, viruses, Trojan horses, corrupted files, destructive code or anything that may harm or interfere with the operation of the networks, servers, or other infrastructure of Google or others.

iv. Exploit children.

---

[65] Google, 'How end-to-end encryption in Google Messages provides more security', *Google Messages* (Web Page, 2024); Google, 'Learn about call & meeting encryption in Google Meet', *Google Meet Help* (Web Page, 2024).
[66] Encryption is a critically important tool in protecting individuals, companies and government from a broad range of security threats including the interception and misuse of personal, financial or national security information. This includes by creating protections that make it harder for criminals to get sensitive user data through hacking and phishing attacks. We believe protecting privacy and supporting law enforcement are not incompatible goals. We support the Government's efforts to protect Australians, and we work hard to comply with legitimate requests from law enforcement, while protecting the privacy and security of our users.
[67] Leviathan Security Group, '2023 Competitive Security Feature Review: Mobile Platform Scam and Phishing Prevention', (Web Page, 11 September 2024).
[68] Google, 'Google Chat Acceptable Use Policy', *Google Chat Help* (Web Page, 2024).

v. Harass, threaten or intimidate others.

vi. Distribute personal and confidential information of others.

vii. Promote, organise or engage in illegal activities.

b. Giving users the ability to block (and report) senders of spam/abusive content.[69]

c. Providing users with a means to report activity to Google that violates the relevant product's policies or Google's general terms of service - for example, by using the reporting feature within the service.

d. Enforcement efforts, including classifying communication from a scammer as spam, or issuing service-level or account-level suspensions for violations of our terms or policies. We use a combination of automated detection technology and human review processes based on network signals, previous account activity, behaviour patterns and user feedback to detect bad actors.

28. While we are focused on product design and policies that prevent scams, we recognise that creating a safer internet for everyone is a collective effort. This is why we also invest in broader consumer awareness raising exercises such as supporting Scamwatch during Scam Awareness Week[70], promoting Google's Security Checkup on the Google homepage in Australia and posting practical tips on how to stay safe online on our Safety Centre[71]. We've also worked closely with the Australian Government's economy-wide efforts to address scams.

Importance of RCS to user privacy and combating scams

29. RCS messages is an upgrade to SMS and MMS and provides an improved, rich messaging experience. RCS gives users greater control over privacy including the ability to manage read receipts, typing indicators, and the option to block contacts. It also allows for the sharing of media and documents within a secure environment.

30. We have adopted the RCS standard for our messaging products to reduce spam and prevent abuse, and have encouraged others in the industry to do the same. Specifically, we have supported the development of three layers of protection in RCS:

a. Protections to prevent abusive users from provisioning (i.e., using) RCS, by seeking to verify and allow only trustworthy devices to use the service.

b. Server-side protections to identify and block spam and abusive messages and senders. The protections include limits on the numbers of messages sent, and behavioural analysis to identify behaviour linked to abuse.

---

[69] See for example, for Google, '[Block and report someone]', *Google Chat Help* (Web Page, 2024).
[70] Lucinda Longcroft, '[How Google is protecting you from scams this Scams Awareness Week 2023]', *Google Australia Blog* (Blog Post, 27 November 2023).
[71] Google, '[Google Safety Centre]', *Safety Centre* (Web Page).

c. Additional protections on Google Messages, such as warnings for messages and links that may be spam or abusive, moving messages to a spam folder, and enabling users to report messages as spam.

31. We have also developed RCS Business Messaging (**RBM**) for business users. RBM enables verification of business users (with a "verified" icon shown to customers) and encryption of messages, and provides business users with enhanced customer interactions, rich media and other benefits.[72]

32. On 11 June 2024, Apple announced that its messaging app, iMessage, would support the RCS standard in the upcoming iOS 18 update.[73] The expectation is that this will not be rolled out in Australia. Apple has also not publicly agreed to a timeline for rolling out encryption. And we are concerned in any event that Apple's implementation of RCS will not provide the full privacy and spam prevention benefits when users of iMessage and messaging apps on non-iOS devices interact.

Support for messaging interoperability

33. We support greater messaging interoperability. Users should be free to choose their preferred messaging app and to communicate with friends, colleagues, and businesses on popular services, such as iMessage (Apple) and WhatsApp and Messenger (Meta), securely and without degradation of content, features, and capabilities.

34. The DMA has sought to promote effective interoperability in messaging.[74] In our view, the DMA interoperability obligations as interpreted by the EC are not scalable and will be cost prohibitive for smaller app developers to implement, which will undermine the potential competition and innovation benefits.

35. We encourage the ACCC to consider current barriers to interoperability and how greater messaging interoperability can be encouraged in Australia both to promote competition and innovation and to improve consumer trust of those services by increasing privacy and reducing scams.

---

[72] Google for Developers, 'The future of messaging for brands', *Business Communications* (Web Page).
[73] Apple, 'iOS 18 makes iPhone more personal, capable, and intelligent than ever', *Apple Newsroom* (Press Release, 11 June 2024).
[74] That is, end-to-end encrypted messages over IP networks, high quality photo and video sharing, and group messaging support.

Topic 2 - 1.2.2: Report on App Marketplaces

36. We make the following observations relevant to the ACCC's further consideration of app store issues.

Update on app marketplaces

37. The ACCC's interim report on App Marketplaces published in March 2021 (**DPSI 2 Report**) identified several concerns relating to Play and the App Store's alleged market power; their policies regarding access, data, safety and security, and payments; and the risk that they will engage in self-preferencing.

38. Google's strong view remains that those concerns do not reflect the competitive constraint that Google faces from Apple's iOS ecosystem and within Android. In particular:

    a. Competition with iOS is a principal driver of Google's strategy for Android and Play. In order to attract and retain device manufacturers, developers and users to Android, Google must continually invest in the development of new features for Android devices and in the pricing and quality of the services provided by Play. Android's competitiveness against iOS and Google's ability to generate revenue from the services it makes available on Android depends on its ability to bring high-quality, safe and consistent experiences to Android users, including through Play.

    b. Users and developers also have greater choice on Android than they do on iOS, exposing Play to increased competition. Users can access apps and purchase in-app content from many locations within Android, including through Play, third-party Android app stores, pre-installed apps, directly downloading apps, web apps, streaming services and out-of-app purchases on a developer's website.[75] Users can also choose to consume digital content on Android but spend on other platforms (e.g. they can play a game on their Android device using in-game tokens purchased on their gaming console or the developer's website). Developers also have choices about the extent to which they invest in Android apps and how they monetise their apps, and can bypass Play's service fee altogether by moving to a consumption-only mode (i.e. apps that do not enable users to purchase access to digital goods or services from within the app), as popular apps like Netflix and Binge have done. Out of all these choices, Play only receives a service fee if the developer monetises within their Android app and the user decides to transact via Play.

39. The competitive pressure that Android and Play face is reflected in several developments that have occurred since the DPSI 2 Report. These include service fee reductions, the introduction of UCB and Google's recent partnerships and technical enhancements in relation to privacy and security discussed further below.

[75] These alternatives to Play are regularly used, with 84% of the top-50 apps by consumer spend on Play being available through at least one other Android distribution channel (including 72% via the Amazon Appstore, 34% via the Samsung Galaxy Store, 22% via web-apps and 12% via direct-downloading. In November 2020, 12% of app installation on Android devices were from outside Play.

40. The DPSI 2 Report proposed the following six potential measures for Play and the App Store:

a. Allow developers to communicate within their app about alternative payment options.

b. Provide more information on ranking and notice of algorithm changes.

c. Allow users to rate and review first-party apps.

d. Allow users to change pre-installed and default apps.

e. Implement additional measures to address the risks of malicious or otherwise harmful apps that are available on their app marketplaces.

f. Ring-fence data collected from app stores from other first-party business operations and services.[76]

41. At the time of the DPSI 2 Report's publication, Play already fully complied with three of the six proposed measures (c, d and f). On each of the other proposed measures, we were at least in partial compliance at this time.

42. In September 2022, the ACCC published its interim report on Regulatory Reform (**DPSI 5 Report**), which recommended the introduction of service specific codes of conduct for designated digital platforms, including an app store code. The DPSI 5 Report essentially repeated concerns previously raised about app stores, which materially overlap with the potential measures proposed in the DPSI 2 Report, about:

a. The use of data collected from third-party developers to inform the development of first-party apps.[77]

b. Pre-installation of first-party Google apps on Android devices.[78]

c. Purported tying of in-app payment systems with app stores.[79]

d. Restrictions on interoperability for third-party app stores on mobile OS and app stores.[80]

e. Ability to unilaterally vary terms of service.[81]

43. To assist the ACCC's updated consideration of these issues, we address each of the proposed measures and concerns from the DPSI 2 and DPSI 5 Report's below. We encourage the ACCC to specifically take these developments into account as it updates its app store findings and recommendations. In light of these developments, we also submit that the ACCC should not recommend mandatory rules in respect of Play.

---

[76] ACCC, '[Digital platform services inquiry - March 2021 interim report]', *ACCC Digital Platform Services Inquiry* (28 April 2021) (**DPSI 2 Report**), 14.
[77] ACCC, '[Digital platform services inquiry - September 2022 interim report]', *ACCC Digital Platform Services Inquiry* (11 November 2022) (**DPSI 5 Report**), 124.
[78] DPSI 5 Report, 135.
[79] Ibid, 132.
[80] Ibid, 156.
[81] Ibid, 133.

App marketplaces and developments since DPSI 2

DPSI 2 Proposed Measure 1: Developers on Play can communicate in-app about alternative payment options

44. The DPSI 2 Report raised concerns with the service fee applied by Apple's App Store and Play and developers' ability to provide users with information about alternative payment options. In this context, the ACCC proposed a measure to require app stores to allow developers to provide users with information about alternative payment options.

45. Google believes its service fee model aligns its success with developers' success, and is appropriate in light of the services and value it provides. However, since the DPSI 2 Report, Google has taken further steps which materially address the ACCC's concerns. These include introducing tiered service fees and the UCB pilot program.

Reduction in Play service fees

46. Like all businesses, Play charges, and is entitled to charge, for the services and value it provides. The service fee helps support Google's ongoing investment in Android and Play, is one way it earns revenue as a business, and reflects the value provided by Android and Play. It also enables Google to deliver affordable and innovative user experiences, keep the Play and Android ecosystems safe and secure and help developers reach users and build sustainable businesses.[82]

47. Google's business model aligns its success with developers' success. Developers pay Play a service fee only if they monetise their app via a paid download or in-app purchases of digital content or services via Play. If the developer chooses to distribute its app for free, distribute its app outside of Play, or monetise its app in any other way (e.g., through advertising, or outside Play, such as selling digital content through the developer's website that can then be accessed in the app), the developer does not pay any service fee.[83]

48. Since the DPSI 2 Report, Google has introduced the following changes that have reduced the service fee:

    a. In June 2021, Google launched the Play Media Experience Program to assist developers in building high quality apps that deliver video, audio or book content by offering eligible developers a service fee of 15% or lower, among other benefits.[84]

    b. In July 2021, Play began offering a service fee of 15% for the first USD $1 million of developer earnings each year via Play (**15% Service Fee Tier**).[85]

---

[82] As a result of our continued investment to support users and developers, today Play provides approximately two million apps and games to billions of people around the world. Developers on Play have generated over $120 billion in earnings to date. See Google Play, 'How Google Play Works', (Web Page).
[83] Examples of developers who offer user subscriptions outside of Play to access content in-app, and therefore do not pay a service fee, are Netflix, Stan, Binge and Amazon Kindle.
[84] Further information is available here: Google Play, 'Play Media Experience Program', (Web Page).
[85] Our March 2021 announcement is available here: Google, 'Changes to Google Play's service fee in 2021', (Web Page, 2024).

c. In January 2022, Google reduced the service fee charged on automatically renewing subscriptions to 15% (previously 30% for the first year), regardless of the amount of revenue earned by the developer.[86]

49. These changes to the service fee mean that of the 4% of Australian developers who pay Google a service fee, 99% are now eligible for a fee of 15% or less.

50. The large developers that pay most of Play's service fees also have many ways to reach users to monetise their content. The top 25 developers on Play in Australia (by service fee revenue) account for almost half of Play's service fees. All of those developers also monetise their content via an iOS app and at least one other channel (including the web and PC apps). In all cases their content purchased on other channels can be accessed in the version of the app downloaded from Play without Google receiving any service fee.

51. Google remains firmly of the view that the service fees charged by Play for in-app payments are not 'inflated', as the ACCC suggested in the DPSI 2 Report.[87] Our service fee model is fair and reasonable and Play's fees are the lowest among major app stores.[88]

Expanding billing optionality and in-app communication

52. As with any multi-sided product, to maintain a successful and thriving app distribution platform, Play must appropriately balance a range of often competing stakeholder interests. Play's Payments Policy appropriately balances the need to: (i) cover ongoing investments in Play; (ii) provide a seamless and safe user experience; and (iii) give developers flexibility to communicate with users both within and outside their app. On the latter, Google already provides developers with significant flexibility:

a. Outside their app, developers can freely communicate with users, including about alternative purchase options. They can use email marketing and other channels outside of the app to provide subscription offers and even special pricing.

b. Within their app, developers can include links to web pages outside of their app, such as an account management page, privacy policy or a help centre, as long as the link does not lead to alternative payment options. For consumption-only apps, developers can communicate with users about purchasing options and can direct users to such alternatives on their website by including in-app language such as "*you can purchase the book directly on our website*", as long as they do so without direct links. This is contrary to the suggestion in the DPSI 2 Report that Play prohibits developers from informing users about an alternative billing system.[89]

---

[86] Our October 2021 announcement is available here: Sameer Samat, 'Evolving our business model to address developer needs', *Android Developers Blog* (Blog Post, 21 October 2021).
[87] DPSI 2 Report, 9.
[88] Deloitte, 'Fees applied by distribution platforms to transactions by developers and content providers', (Benchmark Study, 2022), 11.
[89] DPSI 2 Report, 79.

53. Notwithstanding this existing flexibility, Google has recognised the ongoing discussion around billing choice, including the ACCC's proposed measure on developers' ability to communicate with users about alternative billing systems. In this context, Play announced the UCB pilot program in March 2022, to explore how to enable developers to offer alternative billing systems on Play whilst maintaining the high standards of trust, safety and security that users expect. In September 2022, Google chose Australia as one of the first jurisdictions to benefit from this program.

54. Under the UCB pilot program, eligible developers can implement an alternative billing system alongside GPB for in-app purchases of digital content within non-gaming apps.[90] Where a user pays with an alternative billing system, Play's service fee is reduced by 4%. This means that for the 4% of Australian developers who pay a service fee, those that have enrolled in the UCB pilot program benefit from a reduced fee of: (i) 11% or lower for transactions subject to the 15% Service Fee Tier or Play Media Experience Program; or (ii) 26% for transactions subject to the 30% service fee.

55. At the heart of the UCB pilot program is Google's belief that the best way to offer alternative billing for in-app purchases is to put the choice in the hands of users. As explained above at paragraph 7, alternative proposals that allow developers to choose to show users *only* their alternative billing system: (i) could deprive the users of the option to transact via GPB; and (ii) may compromise user security and safety, given that developers do not necessarily have the same incentives to act in the best interest of users or the app store ecosystem. These concerns and risks are minimised under the UCB pilot program.

56. Developers enrolled in the UCB pilot program can tell users about their alternative billing system and any special pricing or promotions within the app before the purchase screen. Outside of the app, all developers on Play, including those enrolled in the UCB pilot program, remain free to promote offers and tell users about alternative payment options that may be available on the developer's website or other channels. We think this flexibility to communicate with users both within and outside of the app about billing optionality materially addresses the ACCC's concerns. This is on top of the material flexibility already afforded to developers under Play's business model and the Android ecosystem more broadly.

57. On Play, developers have significant and viable choices on: the business model they want to use; how they charge users for in-app content; the payment processors and forms of payment they want to offer; and how they communicate to users both within and outside of the app. Google is the only major app store to offer developers this flexibility in Australia.

[90] For a business of Play's scale, implementing the UCB pilot program is a complex and technical exercise. Most importantly, we need to make sure alternative billing systems meet minimum safety standards and are capable of guarding against fraudulent behaviour. Games carry specific consumer protection needs so eligibility in the pilot program is limited to developers of non-gaming apps at this time.

DPSI 2 Proposed Measure 2: Play provides developers with transparent and sufficient information on app ranking and discoverability

58. The DPSI 2 Report highlighted developers' desire for information on how apps are ranked and displayed on Play, including the operation of Play's search algorithm. Google recognises the importance of this and was largely already compliant with the second proposed measure at the time of the DPSI 2 Report.

59. Play applies transparent, fair and non-discriminatory conditions for app rankings and provides detailed information on Play Help Centre pages that:

    a. Disclose the key parameters that impact the ranking and organising of apps on Play.[91]

    b. Provide additional information and suggestions to assist developers to enhance the discoverability of their apps when users search on Play.[92]

60. However, as the DPSI 2 Report acknowledges, it is crucial that public disclosures are avoided which might allow developers to "game" Play's search algorithm. We believe that Google's current level of transparency strikes the necessary balance between avoiding this risk while enabling developers to understand how their apps are ranked and displayed, in order to maximise discoverability.

61. The measures Google takes to provide transparency on ranking are consistent with international regulatory developments. For instance, our disclosure regarding the key parameters that impact the ranking of apps on Play is in accordance with the EU Platform-to-Business Regulation and the DMA.

62. Play strives to treat developers fairly and equitably whether big or small, third-party apps or first-party Google apps. All apps are therefore subject to the same set of rules and policies, and all apps are promoted in Play according to the same principles. Play does not discriminate between first-party and third-party apps in ranking. In fact, Google regularly promotes apps developed by competitors in the "Editors Choice" list on Play, and our global policies on app ranking comply with the DMA's ban on self-preferencing.

DPSI 2 Proposed Measure 3: Users on Play can rate and review any app, first-party or third-party

63. Google already complied with the third proposed measure at the time of the DPSI 2 Report's publication. Ever since Play introduced the functionality to rate and review apps, users have been able to rate and review all apps, including Google's first-party apps.

64. Google recognises that underlying this measure is the idea that third-party apps should be able to compete on the merits with first-party apps. We support this idea and seek to apply it across all of Play's policies and processes.

---

[91] See Play Console Help, '[App Discovery and Ranking]', (Web Page, 2024).
[92] See Play Console Help, '[Get discovered on Google Play search]', (Web Page, 2024).

DPSI 2 Proposed Measure 4: On Android, users can easily move, delete or disable pre-installed apps and change default settings

65. Google was also already compliant with the proposed measure to give users the "*ability to change any pre-installed default app on their device that is not a core phone feature*".[93]

66. Google provides incentives for device manufacturers to pre-install certain Google apps (including Play) so that Android devices come with a consistent and high-quality set of apps that provide basic functionality. Providing a high-quality "out of box" experience is an important way that Android devices compete with iOS devices. However, Android users are able to freely customise their devices irrespective of which apps are pre-installed. Users can easily change the default apps for "non-core phone features" (e.g. the default browser, music player, mail app etc) and can either delete or disable all pre-installed apps and utilise other apps that are pre-installed, installed from pre-installed third-party app stores or sideloaded. To assist users, Google provides clear step-by-step guidance on how to do so on its public help pages.[94]

67. Unlike iOS devices, over 70% of Android devices come with two or more app stores pre-installed, and users can install others if they want. All Samsung devices have the Galaxy Store pre-installed on their default home screen. As with all pre-installed Google apps, users can remove Play from their default home screen or move it to another screen on any Android device.

DPSI 2 Proposed Measure 5: Play dedicates significant resource to keep users safe

68. Google is aligned with the ACCC's concerns about the need to protect users from the risks associated with harmful or malicious apps, including those that entice consumers into investment or other scams. With around 3.2 million apps available on Play in Australia, Google commits significant resources and is continually working on ways to weed out harmful apps, and keep users and developers safe. As a result, and as recognised by the ACCC, apps downloaded via Play are far less likely to harm users or their devices when compared with apps downloaded from other app distribution channels.[95]

69. Some of the processes and steps taken to monitor and shut down harmful apps include:

    a. Play's comprehensive app review process, which checks whether an app complies with Google's policies, including those that prohibit apps that pose risks of harm to users. Contrary to the suggestions made in the DPSI 2 Report that the policies and processes governing app reviews and approvals may at times be opaque,[96] Play's app review processes and policies are clearly set out (with step by step instructions) and easily accessible on our public help pages. Moreover, where enforcement action is taken, Google strives to provide individualised information such as evidence of the relevant policy violation through screenshots to provide developers with guidance and

---

[93] DSPI 2 Report, 7.
[94] See Android Help, 'Disable apps that came with your Android device', (Web Page, 2024); Pixel Phone Help, 'Set or clear default apps', (Web Page, 2024); and Android Help, 'Delete apps on your Android device', (Web Page, 2024).
[95] DPSI 2 Report, 11.
[96] Ibid, 56.

information. Developers that wish to appeal enforcement decisions can do so by filing an appeals form. As explained on Play's public help page, Google reinstates apps in appropriate circumstances, including if an error was made in enforcement.

b. Google Play Protect, which runs on devices and conducts a safety check on apps before an app is installed, scans over 125 billion apps per day to protect users from malware.

c. Reviewing reports submitted by users via the Report a Policy Violation Form[97] on harmful or malicious apps that do not comply with Play's Developer Program Policies.

70. Year on year, Google makes improvements and implements new measures to continue to keep Play's users safe, even as the threat landscape evolves. This commitment is consistent with the DPSI 2 Report's suggestion that Play continue to take more steps to proactively monitor apps' compliance with policies. In 2023 alone, Play:

a. Partnered with Microsoft and Meta through the App Defense Alliance to support industry-wide adoption of app security best practices and guidelines.[98]

b. Enhanced Google Play Protect's security capabilities with real-time scanning at the code level to combat novel malicious apps.[99]

c. Updated Play's policies around genAI apps, requiring developers to provide users with the ability to report or flag offensive AI generated content within the app.[100]

d. Announced expansions to privacy protections so that apps can only access a user's photos and videos for purposes directly related to app functionality.[101]

e. Introduced new testing requirements developers must satisfy before they can make their app available on Play, including a requirement to run a closed pre-launch test so that developers have an opportunity to fix issues and ensure the app complies with Play's policies.[102]

71. Play also invests in keeping users safe when it comes to online games. As recognised by the ACCC[103] and outlined in paragraph 55, developers do not necessarily have the same incentives as platforms to act in the best interests of users. Bad actors may seek to deliberately target, nudge or confuse users into making unintended purchases (including in-game purchases). This risk is heightened when the user is a child, so to help parents keep their children safe, Play makes it easy to set up parental controls that restrict what content can be downloaded or

---

[97] See Play Console Help, 'Report a Policy Violation', (Web Page, 2024).
[98] See Google Security Blog, 'How we fought bad apps and bad actors in 2023', (Blog Post, 29 April 2024).
[99] See Google Security Blog, 'Enhanced Google Play Protect real-time scanning for app installs', (Blog Post, 18 October 2023).
[100] See Karina Newton, 'Announcing Policy Updates to Support App Quality on Google Play', *Android Developers Blog,* (Blog Post, 25 October 2023).
[101] Ibid.
[102] Play Console Help, 'App testing requirements for new personal developer accounts', (Web Page, 2024).
[103] Gina Cass-Gottlieb, 'Committee for Economic Development of Australia (CEDA) speech 2024)', (Speech, Committee for Economic Development of Australia 2024, 7 March 2024).

purchased from an Android device based on maturity level.[104] Parental controls can be set up for games, as well as other apps and digital content. Parents can also manage their child's Play apps, including by blocking or unblocking an app.[105]

72. Google will continue to develop and launch new security initiatives, and promote a safe and trusted Play experience.

DPSI 2 Proposed Measure 6: Play strives to treat all apps equally

73. Google was already compliant with the DPSI 2 Report's suggestion for app stores to ring-fence their operations from other business activities. The DPSI 2 Report raised concerns that Google and Apple have superior access to information about the app ecosystem, allowing Google and Apple to monitor all apps and gain valuable competitive insights.[106]

74. Google provides developers access to an extensive set of data through the Play Console,[107] in downloadable formats and APIs,[108] and continually invests to make metrics and analytics more helpful. The data available to developers include insights on top countries where apps have been installed as well as insights on language-specific downloads. Through Play Console, developers can review reports on app installs, uninstalls, ratings, revenue, and crashes. This allows developers to track how their apps are performing, and to make changes to improve their performance. For example, the data shared with developers helps them understand the lifecycle of their app: from how it is discovered in Play, to how users engage with it, and what users pay for. We also allow developers to benchmark their app's performance against other apps in the same category or region, providing valuable information about the app ecosystem. They can see how their app ranks in terms of key metrics such as retention, engagement, monetisation, and quality. Developers can easily compare their app to other apps of their choosing by setting custom peer groups.[109]

75. Play has formal policies in place that prohibit the sharing of non-public, identifiable third-party developer data with other parts of Google, except where it would benefit the Play ecosystem (e.g., to develop anti-fraud features). Specific mechanisms for internal information control include separate reporting lines between different teams within Google and restrictions on sharing certain data. In connection with our compliance under the DMA, Google built on these existing policies and practices, and created a set of central standards for handling such data. These central standards help promote awareness and ensure consistency in practices across Google regarding our data sharing restrictions, and ensure that access to such data is limited and governed by appropriate processes and controls. Google promotes competition on the merits and strives to treat all apps equally. These policies and procedures on data separation (which apply globally) are part of Google's efforts towards achieving this.

---

[104] See Google Play Help, 'How to set up parental controls on Google Play', (Web Page, 2024).
[105] See Google Play Help, 'Manage your child's Google Play apps', (Web Page, 2024).
[106] DPSI 2 Report, 127.
[107] See Play Console Help, 'View app statistics', (Web Page, 2024).
[108] See Play Console Help, 'Download and export monthly reports', (Web Page, 2024).
[109] See Play Console Help 'Compare your app's Android vitals and ratings with custom peer groups', (Web Page, 2024).

DPSI 5 on Play

DPSI 5 Issue 1: Google's first-party apps compete against third-party apps fairly and on the merits

76. As explained above in paragraph 75, non-public data from and about third-party apps on Play is not used inappropriately in Google's business. To create a thriving ecosystem on Play, Google is incentivised to ensure that all apps compete effectively and on a level playing field, regardless of whether they are third-party and first-party apps. Google agrees that third-party developer data should not be used unfairly by app stores to benefit competing first-party services, and this is reflected in our global policies and practices.

77. Separately, we disagree that providing original equipment manufacturers (**OEMs**) with the option to pre-install first-party Google apps on Android devices reduces consumer choice and heightens barriers to entry and expansion in app stores and downstream app markets.[110] As set out in paragraph 66 above, Android users can easily uninstall or delete first-party Google apps, and unlike iOS devices, the vast majority of Android devices come with two or more app stores pre-installed. For example:

    a. The Samsung Galaxy Store is pre-installed on every Samsung Galaxy device, which accounts for approximately two-thirds of all Australian Android devices. Accordingly, developers have a meaningful alternative distribution method to users on these devices.

    b. As at November 2020, 12% of app installs on Android devices were outside Play.

    c. Several developers have successfully utilised preinstallation deals to reach users. For example, out of over 5 million new Android smartphones active in Australia in 2021, the number of pre-installations was 3.7 million for Microsoft OneDrive, 3.3 million for Facebook and 2.7 million for Netflix.

78. The suggestion that Google has entrenched its position and foreclosed rivals by entering into pre-installation agreements with OEMs[111] does not properly account for the freedom OEMs have both before and after entering the Mobile Application Distribution Agreement or the fact that users can easily delete or hide pre-installed apps.

DPSI 5 Issue 2: Eligible developers on Play can offer alternative billing systems that users can choose to transact on

79. As mentioned above at paragraph 7, for users, GPB provides a safe, secure, and convenient way to pay for digital content on Play using their preferred forms of payment. GPB reassures users that their payments are safe, and enables them to set budget controls and manage and monitor purchases. Prior to a purchase being made, GPB allows users to understand exactly what they are purchasing, how much it costs, and if it is a recurring charge. It then flows through to reminders about free trials and introductory pricing ending, order management and subscriptions management and cancellation options in the subscription centre and other customer support and purchase controls (e.g. parental controls) and user-friendly features (e.g.

[110] DPSI 5 Report, 140.
[111] DPSI 5 Report, 142.

budgeting controls).

80. By creating high confidence among users, GPB in turn maximises the output and return of developers. Further, GPB provides developers with an efficient, secure and reliable process for collecting payments for their apps and in-app content, and for managing refunds and customer complaints. This is particularly valuable for the numerous app developers who do not have such capabilities in-house.

81. Contrary to the ACCC's suggestion,[112] GPB does not prevent users from paying using their chosen method and has not resulted in increased prices. GPB provides over 200 forms of payment. Further, Play's service fee is not a payment processing fee. Developers receive significant value from Android and Play, and our service fee reflects this value.[113] For these reasons, Google considers that the concerns in the DPSI 5 Report on Play and the use of GPB were misplaced.

82. However, Google has recognised the ongoing discussion around billing optionality and, as described in paragraphs 53 and 55, rolled out the UCB pilot program to give users and developers more flexibility. We have iterated the UCB pilot program in response to developer feedback.[114] We expect to continue to evolve the program and will continue to explore and iterate how to make the implementation of UCB effective and safe for users and developers.

83. Alongside the various business models and distribution options developers on Play and Android can choose from, the roll out of UCB pilot program to eligible developers directly addresses the ACCC's concerns.

DPSI 5 Issue 3: Google supports and enables competition for app distribution on Android devices

84. As an open source platform defined by choice, Android supports and enables competition for app distribution. On Android, developers can access a wide array of app distribution channels, including via Play, pre-installed app stores, other app stores that users can directly download onto their devices and sideloading. As demonstrated at paragraph 77, these alternative app distribution methods are used extensively in practice. Of the top 50 apps by consumer spend on the Australian Play Store, 84% are available through at least one other Android distribution channel, including 72% via Amazon Appstore, 34% via the Samsung Galaxy Store, 22% via web-apps, and 12% via direct-downloading.

85. The ACCC acknowledges this optionality but notes that third-party app stores cannot be downloaded through Play. Google strongly opposes any proposal that would require third-party app stores to be available on Play because such a requirement would:

---

[112] DPSI 5 Report, 133.

[113] As noted above at paragraph 51, Play's service fee is competitive and the lowest of any major app store.

[114] This includes moving from two UCB screens to one, launching alternative billing APIs which streamline implementing user experience requirements and reporting, and enabling developers to self-service enrol their apps into UCB through Play Developer Console. We also launched other features in the Play Developer Console such as allowing developers to make more frequent enrollment changes, providing more detailed transaction reporting, and allowing developers to edit self-serve alternative billing settings. See Play Console Help, '[Enrolling in the user choice billing pilot]', (Web Page, 2024).

a. **Require an exponential amount of work for Play to maintain user protection policies**: If third-party app stores were distributed on Play, we would need to review each app available for download on each third-party app store to ensure it complies with Play's policies (otherwise this would undermine Play's approach to user safety). Given the large number of apps from multiple developers available through third-party app stores and given that such apps are updated all the time, this would require an exponential amount of work to apply. This process would be incredibly burdensome and technically onerous.

b. **Potentially harm users and developers:** Even if Google undertook to review every third-party app store for compliance with Play's policies, we could not provide the same level of safety and security to users because we do not manage the third-party app store.

c. **Negatively affect the competitive dynamics in app distribution**: If third-party app stores were distributed on Play, they would need to comply with Play's policies. However, app store policies are a parameter of competition to attract both developers and users. For example, we prohibit the distribution of apps featuring explicit adult content on Play, but other app stores may allow such apps. If a third-party app store was available on Play, the apps they contain would have to comply with our policies. As such, developers would have less choice about which app store's policies they want to comply with and users may only be able to access content supported by Play.

86. The DMA does not require third-party app stores to be available on Play, but instead imposes an obligation that operating systems must be compatible with third-party app stores, which Android already is. Google encourages the ACCC to similarly focus on ensuring open operating system ecosystems that enable interoperability with third-party app stores.

DPSI 5 Issue 4: Developers on Play already receive advance notice of policy changes

87. Google recognises the importance of maintaining an open dialogue with developers and providing them with the tools, information and support they need to succeed on Play. That is why Google has implemented systems and procedures to ensure developers are treated fairly when policies are developed, released or updated.

88. Google strives to take into account developers' interests when developing policy changes by conducting impact assessments and reviewing developer feedback post-launch to inform possible corrections or updates to policies. When new developer policies are introduced or updated, developers are given at least 30 days prior notice to comply. To promote transparency, policy changes are also always publically available and developers can easily check upcoming policy deadlines and find additional resources via the Google Play Developer Policy Center.[115]

89. Google is aligned with the ACCC's position that without advance notice, unilateral changes in an app store's terms and conditions may reduce developers' capacity and incentives to invest and

[115] See Play Console Help, '[Policy Deadlines]', (Web Page, 2024).

innovate.[116] Play's current processes guarantee an advance notice period of 30 days for any policy change, which we believe strikes the right balance between providing notice to developers while allowing us to move quickly where needed to address broader ecosystem concerns.

Given the flexibility and openness, Play should not be the priority platform for an app store code

90. The Treasury has indicated that the Government would take a harms-based approach to prioritising digital platform regulation.[117] As set out above, Google supports many of the ACCC's aims. To that end, we already complied with or have since taken steps to materially address all six of the ACCC's proposed measures in the DPSI 2 Report.

91. Furthermore, unlike other mobile and app ecosystems, Play and Android are open ecosystems. Google considers that the flexibility and openness of the Android and Play ecosystems should be taken into account if the Government proceeds to develop service-specific codes of conduct as recommended in the DPSI 5 Report, both in determining what services and platforms take priority, and the content of the rules.

92. Google also considers any service-specific code to address competition issues in app stores should consider competition for user and developer attention across devices as a whole. This should include web apps and Progressive Web Apps, which provide an important alternative avenue for developers to reach potential users across different devices and platforms.

93. For web apps to serve as a viable alternative to native apps, they require browser engine support in order to offer robust functionality that rivals native apps. For example, Android supports both native apps and web apps, and Android allows users to choose their preferred app as well as for browsers to build on whichever engine offers the functionality they require. Apple only allows iOS web apps built on Apple WebKit.[118] Because of the limitation in the WebKit browser engine, web apps installed through Safari on iOS have more limited device integrations (and hence features and functionality) than native apps.[119] This means that on iOS, not only can users not use any alternative app stores, but they also have limited access to competitive web apps, further frustrating app distribution alternatives on the platform.

94. As the ACCC itself acknowledged in the DPSI 5 Report, regulatory intervention must be balanced, targeted and take into consideration legitimate justifications to avoid unintended consequences.[120] Adopting this approach, Android and Play should not be the priority of any app store code. If the Government is minded to introduce an app store code, it should first aim to increase developers' freedom in closed ecosystems.

[116] DPSI 5 Report, 183.
[117] Australian Government, 'Government Response to ACCC Digital Platform Services Inquiry', (8 December 2023), 4.
[118] Under section 2.5.6 of Apple's App Store Review Guidelines, "*Apps that browse the web must use the appropriate WebKit framework and WebKit Javascript.*" See Apple's App Store Review Guidelines at Developer Apple, 'App Review Guidelines', (Web Page, 2024). This requires all browser apps on iPhones and iPads to use Apple's WebKit browser engine, and prevents them from making modifications to it.
[119] In addition, Safari on iOS does not prompt a user to install a web app or show banners; the user must choose to "share" in order to install, scroll down below the fold to discover the "add to home screen" option and click on that. By contrast, on Android, Chrome automatically generates an install banner.
[120] DPSI 5 Report, 131.

Any app store rules must be carefully designed

95. The ACCC recognises the challenge in finding a balance between interventions designed to promote competition in digital marketplaces and protecting consumers on those platforms.[121] Indeed, there is an inherent tension between proposed ex ante regulation of app stores and the protection of app store users because such regulation can undermine the ability of app stores to ensure a safe and secure platform for its users. In line with the ACCC's enforcement priorities for 2024,[122] DPSI 10 will examine potential consumer welfare concerns in online gaming and in particular in-app purchases and offerings that may have inadequate safeguards and deliberately target or confuse customers. This is just one area where Play's policies and practices are designed to protect the safety and security of its users. By ensuring that users feel safe transacting on GPB and on Play, this ultimately benefits developers and the ecosystem more broadly. As discussed above at paragraph 7, regulatory interventions overseas highlight this tension between ex ante regulation and consumer protection.

96. Regulatory intervention that is not properly designed can compromise user choice, safety and convenience, and ultimately undermine the sustainability of an app store ecosystem. In this context, if the Government and ACCC consider mandatory ex ante rules for app stores that apply to Play are needed, Google urges that regulatory intervention be approached with caution. We suggest that Australia should take the time to monitor the implications of overseas interventions such as the DMA to learn lessons and avoid pitfalls.

[121] In the DPSI 10 media release, ACCC Chair Cass-Gottlieb refers to "[the ACCC's] *ambition in finding a balance between competition in the digital marketplace and protecting consumer*s". See ACCC, '[Final digital platforms report to focus on global developments and emerging competition and consumer issues]', (Media Release, 25 July 2024).

[122] Gina Cass-Gottlieb, '[Committee for Economic Development of Australia (CEDA) speech 2024)]', (Speech, Committee for Economic Development of Australia 2024, 7 March 2024).

TOPIC 3: IDENTIFYING POTENTIAL OR EMERGING ISSUES

Topic 3 - 1.3.1: Potential competition and consumer issues in online gaming

The ACCC invites interested parties to share their views on potential or emerging competition and consumer issues in relation to online gaming in Australia. *Please provide as much detail or evidence as you can to support your response.*

97. Google provides the below observations as the ACCC considers potential competition and consumer issues relating to online gaming. Given the nature of the concerns and examples given in the Issues Paper, we understand the ACCC's focus to be on the conduct of participants other than Google, including certain developers and competitors to Play.

Android and Play face vigorous competition in the gaming industry

98. As we explain in paragraph 38, Google faces strong competition from within and outside the Android ecosystem. Gaming is an exceptionally competitive industry in which Google and its rivals compete to attract and retain users (particularly high-spending gamers), and for the titles and investment of game developers (including promotions and priority or exclusive launches or features).

99. Google's competitors in the gaming industry are numerous and competition is dynamic. Competing distributors of online games include Apple's App Store, third-party Android app stores (such as the Samsung Galaxy Store, Amazon Appstore and Aptoide), console manufacturers (including Sony (PlayStation), Microsoft (Xbox) and Nintendo (Nintendo Switch)), PC gaming stores (such as Steam), cloud gaming and game subscription services, and developers' own websites. The gaming industry continues to evolve with regular new entry and innovation. Recent developments include:

    a. The launch of several cloud gaming services on Android, including Amazon Luna, NVIDIA's GeForce Now and Microsoft's Xbox Cloud Gaming, each of which have large game catalogues from across several large game studios.

    b. Epic Games' recent launch of its game store on Android globally[123] and Microsoft's planned launch of its game store on Android[124], each of which will offer users access to a range of first-party and third-party titles.

    c. The release of mobile game subscription services, including Apple Arcade, Play Pass, GameClub and Netflix Games.

    d. Valve's launch of the Steam Deck mobile gaming console, which provides users with access to their library of games downloaded from the Steam games store on PC.

[123] See Epic Games, 'The Epic Games Store Launches on Mobile', (Media Release, 16 August 2024).
[124] As announced by Sarah Bond (President of Xbox) on 9 May 2024. See Tom Warren, 'Microsoft's new Xbox mobile gaming store is launching in July', *The Verge* (Article, 10 May 2024).

100. Many popular games available on Play, particularly online or multiplayer games, are also available on other mobile and non-mobile platforms. Popular titles include Among Us, Call of Duty: Mobile, Minecraft, MONOPOLY GO! and Roblox.

101. The intense competition to attract gaming users and developers means that we need to constantly improve our products, capabilities and offerings to remain competitive.

Google's investments in the gaming industry

102. Play's launch, and the introduction of features such as in-app purchases and subscriptions, played a central role in expanding the number and variety of games available on mobile devices, particularly from independent and smaller game developers. Google helped remove significant friction from the game discovery, purchasing and downloading experience, and our policies relating to billing and security provide users with the confidence that they can transact safely on Play.

103. Google continually invests in the competitiveness of Android's and Play's gaming-related capabilities. Recent examples include:

a. **Google Play Games:** A PC app that lets users browse, download and play thousands of games from Play on a Windows PC using their keyboard and mouse.[125] It is currently available as a beta version in more than 120 countries, including Australia. Google Play Games is part of Google's efforts to increase the reach and availability of games available on Play.

b. **Google Play Points:** Play's loyalty program that rewards users who engage with the Play ecosystem by allowing users to earn points on purchases via Play and redeem them for in-app items offered by participating developers.[126]

c. **Google Play Pass:** Play's game subscription service, which provides users with exclusive offers in top games every month and access to a catalogue of over 1000 games that do not have ads and in-app purchases, with games that ordinarily show ads having them disabled.[127] Play pays royalties to developers who publish their games on Google Play Pass.

d. **Pre-registration:** Play enables developers to inform users that their game or app is being released in a certain number of days, and for users to opt-in to being alerted when the app or game is available.[128] For games, pre-registration is a key tool that developers can use to build hype and anticipation around their content.

e. **Promoting cloud gaming:** The adoption of cloud gaming has been much faster on Android than on rival mobile platforms, in a large part because we permit the distribution of cloud gaming apps via Play and do not impose any rules or restrictions on

---

[125] See Google Play Games, 'Take mobile gaming to your PC', (Web Page).
[126] See Google Play, 'Google Play Points', (Web Page).
[127] See Google Play, 'Google Play Pass', (Web Page).
[128] See Google Play, 'Play Console, Pre-registration' (Web Page).

browsers using alternative browser engines. We have also made significant investments in technologies that enable graphics-rich apps such as games to be developed as web apps (for example, WebGL, WebGPUand Gamepad API). The ACCC's Issues Paper references concerns from the CMA's Mobile Browsers and Cloud Gaming Market Investigation, suggesting they relate to app stores generally.[129] We want to make clear that the concerns the subject of the CMA's recent working papers relating to the requirement for browsers operating on iOS devices to use Apple's WebKit browser engine,[130] the ability to install web apps via third-party browsers on iOS,[131] and the impact of the App Store's policies on cloud gaming services do not arise in respect of Android or Play.[132]

104. Play also competes vigorously to secure titles and developer investment in order to remain competitive for users. Developing and fostering strong relationships with game developers and other participants in the gaming industry is central to our ability to provide Android users with high-quality gaming experiences and innovative technologies, including by reducing development costs. For example:

   a. We engage directly with major game developers to help them increase the engagement and monetisation of their games by providing advice and best practices on topics such as cloud gaming, game subscription services and publishing games on a multi-platform basis.

   b. We provide all developers with tools, samples, libraries and guidance via our Android Games Developer Centre website.[133] In addition, Google Play Games Services enables developers to build cross-platform capabilities and other popular gaming features into their games through various APIs.[134] We also offer developers free access to our Android Game Developer Kit, which is a set of tools and libraries that help developers develop and optimise Android games while integrating with existing game development platforms and workflows.[135]

   c. We work with game engines and providers of other game development tools, such as APIs, which is largely directed to incentivising them to build and optimise their offerings for Android, among the other platforms they support.

Subscription and purchasing practices

105. Google supports the ACCC's consideration of potential competition and consumer concerns relating to transparency around subscription practices and purchases in the gaming industry,

---

[129] Issues Paper, section 1.3.1.
[130] See CMA, 'WP2: The requirement for browsers operating on iOS devices to use Apple's WebKit browser engine', (Working Paper, 27 June 2024).
[131] See CMA, 'WP3: Access to browser functionalities within the iOS and Android mobile ecosystems', (Working Paper, 27 June 2024), paragraphs 3.17 to 3.18.
[132] See CMA, 'WP6: Cloud gaming services: nature of competition and requirements for native apps on mobile devices', (Working Paper, 5 July 2024), paragraphs 4.2 to 4.18.
[133] See Developers, 'Android Games Developer Centre', (Web Page, 2024).
[134] See Google Play Games Services, 'Google Play Games Services', (Web Page, 2024).
[135] See Developer, 'Android Game Development Kit', (Web Page, 2024).

including the use of design to manipulate, mislead or deceive users, particularly children and vulnerable users.

106. We are fully committed to reducing the prevalence of those practices and their impact on Android users. In particular, we regularly update and enforce Play's policies on subscriptions and payments, which address many of the practices identified in the Issues Paper. We also invest in developing new safety features (such as parental controls relating to authorising payments), and publishing materials on user safety that users, parents, and developers[136] can access irrespective of whether they use Play.

107. As discussed above at paragraphs 69-70, Play's consumer protection efforts, including the ability for us to enforce our policies, enhance user trust to the benefit of the wider Android ecosystem while enabling users to make informed choices as to where they purchase in-app content. Balancing choice and safety (including security) is part of Android's competitive proposition and is an essential consideration in formulating any ex ante regulation (see paragraphs 95-96 above).

Google Play Pass

108. Google Play Pass is Play's game subscription service, discussed in paragraph 103 above.[137] As with all paid Google services, we have strived to equip users with the information necessary to make an informed choice as to whether to purchase a Google Play Pass subscription. This includes:

  a. Clearly explaining to users that they are purchasing a subscription for access to the games within Google Play Pass' catalogue and exclusive offers in selected games outside that catalogue.[138]

  b. Prominently displaying price and renewal frequency information on relevant landing pages and checkout screens.

  c. Providing users with help centre materials (including on subscribing and unsubscribing)[139] and responses to frequently asked questions.[140]

  d. Informing users during checkout that they can cancel their subscription at any time via Play, and providing them with a link to Play's Terms of Service.[141]

109. If a user cancels their monthly subscription within the first 48 hours and requests a refund, we may refund them the subscription cost for that month.[142]

---

[136] See, e.g. Android Developers, 'Design for Safety', (Web Page, 2024) and Building for Kids, 'Building Safer Apps', (Web Page, 2024).
[137] All games available via Google Play Pass can be accessed through Play without a subscription to Google Play Pass, but may contain ads and in-app purchases.
[138] See Google Play Pass, 'Join Google Play Pass', (Web Page, 2024).
[139] See Google Play Help, 'Subscribe to Google Play Pass', (Web Page, 2024).
[140] See Google Play Pass, 'Frequently Asked Questions', (Web Page, 2024).
[141] See Google Play, 'Google Play Terms of Service', (Web Page, 2024).
[142] See Google Play Help, 'Learn about refunds on Google Play', (Web Page, 2024).

Play's policies

110. We take steps to minimise the risk of users being manipulated or deceived by developers, including reviewing apps for compliance with Play's Developer Program Policies along with reviewing user complaints.

   a. Play's Subscriptions policy contains clear requirements for developers (including Google) offering subscriptions via Play and provides examples of violations.[143] It also addresses the use of deceptive or manipulative purchase experiences, the requirement that subscriptions provide sustained or recurring value to users rather than being one-time benefits, and contains other transparency requirements.

   b. Play's Payments policy addresses a range of matters relating to the sale of in-app content via Play. It includes requirements that developers must clearly and accurately inform users about the terms and pricing of their app or any in-app features or subscriptions. It also requires that apps and games offering mechanisms to receive randomised virtual items from a purchase including "loot boxes" must clearly disclose the odds of receiving those items in advance of, and in close and timely proximity to, that purchase.[144]

111. We also provide users with information on how they can obtain refunds for purchase via Play, including an easy to use refund request form and information on refund eligibility for different types of content, including Google Play Pass, Google Play Movies & TV, and YouTube.[145]

Play's parental controls

112. Our parent guide to Play contains information on finding content for kids within Play and Play's parental controls.[146] These include blocking apps from a child's device, requiring purchases of new apps or in-app purchases made via GPB to be approved, and restricting access to mature content. Our Family Link app provides parents with the ability to manage these controls, understand how their child is spending time on their device, share their location and manage privacy settings, among other easy-to-use tools.[147] Additional information on the privacy and safety features we offer families across Google's services can be found on our Google Families web page.

113. Play's Developer Program policies also contain additional requirements for apps whose target audiences include children.[148] These include ensuring that the content is deemed appropriate for children and restrictions relating to the ads that can be displayed to children and how they

[143] See Play Console Help, 'Subscriptions', (Web Page, 2024).
[144] See Play Console Help, 'Payments', (Web Page, 2024).
[145] See Google Play Help, 'Learn about refunds on Google Play', (Web Page, 2024).
[146] See Google Play Help, 'Parent guide to Google Play', (Web Page, 2024).
[147] See Family Link, 'Google Family Link', (Web Page, 2024).
[148] See Play Console Help, 'Google Play Families Policies', (Web Page, 2024). See Play Console Help, 'Families Self-Certified Ads SDK Policy', (Web Page, 2024).

are displayed. We also provide developers with specific information on building safe apps for children.[149]

Topic 3 - 1.3.2: Potential competition and small business issues in cloud computing

> The ACCC invites interested parties to share their views on potential or emerging competition and small business issues in relation to cloud computing in Australia.
>
> *Please provide as much detail or evidence as you can to support your response.*

114. To assist the ACCC, Google provides the following views on competition issues in cloud computing in Australia:

    a. The basic elements of cloud computing, including different categories of services and delivery models.

    b. The cloud value chain.

    c. The competitive structure of the market for cloud services, both in Australia and globally.

    d. How traditional enterprises migrate from on-premises to the cloud.

    e. How Microsoft's licensing restrictions push software customers towards Azure.

The basic elements of cloud computing

115. Cloud computing is the provision of remote access to computing resources (such as compute, storage, and networking) on demand and over a public or private network. This is in contrast to traditional IT infrastructure, which is made up of data centres, servers, networking hardware, desktop computers, and applications, and is usually installed on-premises for private use by an organisation.

116. Cloud services are typically classified according to their service models. The three main service models are:

    a. Infrastructure as a service (**IaaS**).

    b. Platform as a service (**PaaS**).

    c. Software as a service (**SaaS**).

[149] See Building For Kids, '[Building Safer Apps]', (Web Page, 2024).

117. These service models form a "vertical stack" where each layer is notionally built on top of the previous one(s):

a. **IaaS solutions** are cloud services that provide access to the basic capabilities provided by a physical server, i.e., data processing (or computing), data storage, and networking; each supported by "virtualisation" software that simulates individual "virtual machines" allocated to specific customers and residing on clusters of physical servers hosted in a data centre. This is the fundamental layer of the cloud on which all other cloud services are built.

b. **PaaS solutions** are cloud services that provide access to a virtual environment for customers to develop, test, deploy, and run applications hosted on cloud infrastructure. These include application development computing platforms and pre-built application components and tools which can be used to build and manage full applications. PaaS services may be supplied by the IaaS provider or by an independent software vendor (**ISV**).[150]

c. **SaaS solutions** are complete applications hosted in the cloud. These cloud applications can be offered by the IaaS provider or by an ISV. Most modern consumer and business facing applications are SaaS.

118. Cloud infrastructure services can be made available in one of three main ways:

a. **Shared cloud**: this is the most common and cheapest model, where services are open to all customers willing to pay and computing resources are shared between them. Shared cloud infrastructure is also often referred to as multi-tenant cloud infrastructure.

b. **Dedicated cloud**: where computing resources are dedicated to (as opposed to shared between) individual customers. It combines the benefits of cloud computing with the security and control of traditional IT, but is more expensive than using shared cloud infrastructure.

c. **Hybrid cloud**: a cloud deployment model involving a combination of shared and dedicated cloud infrastructures, or on-premises resources, which allow the workloads to be shared between them.

The cloud value chain spans several layers, with established as well as challenger players operating at each layer

119. The cloud services market value chain consists of the following layers:

a. **Data centre infrastructure.** Data centre infrastructure is either developed and operated in-house by cloud service providers or offered through leasing services by third-party providers. Given the vast amount of capacity that can be leased in data centres operated by third parties (i.e. co-location providers), new entrants seeking to

[150] ISVs are suppliers of cloud services, typically PaaS and/or SaaS, that do not own the underlying infrastructures.

grow their cloud services offering or existing players looking to expand do not have to incur any upfront data centre investment costs.

b. **Cloud infrastructure services (IaaS and PaaS):** In the supply of cloud infrastructure services, Amazon Web Services (**AWS**) and Microsoft Azure are by far the largest providers.[151] Google Cloud primarily competes alongside other smaller competitors in Australia, including IBM, Oracle, Salesforce, Snowflake and Databricks.

c. **Cloud software (SaaS):** Looking beyond cloud infrastructure services to the broader supply of cloud software services, cloud software markets are even more fragmented and competitive. The cloud SaaS market now comprises thousands of software vendors (such as Salesforce, SAP, ServiceNow, Accenture, OutSystems, Cisco, Hewlett Packard, GitLab, Databricks, Snowflake etc.).

d. **ISVs:** Cloud providers, such as Google Cloud, often supply their services through partnerships with ISVs. Many ISVs build or sell third-party solutions that are based on products and services provided by cloud providers including AWS, Microsoft, Oracle and Google.[152]

120. In recent years there has been rapid growth in overall spend on cloud services both in Australia and globally[153] as: (i) more enterprises migrate from their traditional on-premises IT architecture to cloud; and (ii) once migrated, run more of their workloads on the cloud. According to Gartner data published in the CMA's recent Cloud Services Market Investigation Competitive Landscape Working Paper, worldwide spending on public cloud services has grown by approximately $200 billion in the last two years, and is forecasted to increase by 20% in 2024 alone.[154] Building on the trends seen in recent years, Google anticipates that further growth will come from the significant proportion of large enterprises and public sector bodies with legacy on-premises IT infrastructure (known as traditional enterprise customers) that have not yet migrated to cloud.

The cloud providers in Australia and elsewhere

121. The core premise of cloud computing technology is to provide customers with access to configurable computing resources from any location. The structure and competitive dynamics

---

[151] IDC data shows that in 2022 AWS and Microsoft had a combined market share in the supply of cloud infrastructure services globally of 60-70%. Furthermore, recent analysis carried out by the CMA finds that AWS and Microsoft have a combined market share in the supply of cloud infrastructure services in the UK of 70-80%. We have no reason to believe that this figure is likely to be materially different in Australia. See CMA, 'Cloud Services Market Investigation Competitive Landscape Working Paper', *CMA Cloud Services Market Investigation* (6 June 2024), 106.
[152] Critically, in 2022 Microsoft announced that from October 2025 ISVs will no longer be free to sell Microsoft software if it is hosted on certain third-party cloud platforms (including Google) – a restriction that CISPE suggests will transform ISVs into "*mere resellers of Microsoft software*". See Nicole Dezen, 'New licensing benefits make bringing workloads and licenses to partners' clouds easier', *Microsoft Partner Blog* (Blog Post, 29 August 2022).
[153] See IDC, 'Spending on Shared Cloud Infrastructure Continues to Lead the Way in Enterprise Infrastructure Investments', *IDC* (Web Page, 29 March 2024).
[154] See Gartner, 'Gartner Forecasts Worldwide Public Cloud End-User Spending to Surpass $675 Billion in 2024', *Gartner* (Media Release, 20 May 2024).

of the cloud market in Australia therefore largely mirrors the structure and competitive dynamics of the cloud market globally.

122. The CMA has recently found that there are indicators of market power being held by the largest two cloud providers, AWS and Microsoft.[155] In Australia, AWS and Microsoft are also the major players with the largest market shares.[156] Having been the first provider to enter the cloud market in 2006, AWS has benefited from having a first-mover advantage and a historically high market share.[157] Microsoft has been growing its market share more rapidly than its rivals in recent years and closing the gap with AWS, largely driven by the high rate at which Microsoft's existing software customers are migrating to Azure.

123. Google Cloud is a distant third in terms of market share to AWS and Microsoft and competes alongside other challengers such as IBM, Oracle, Salesforce, Snowflake, Databricks and local providers including AUCloud, Vault Cloud, Orion VM, Hosted Network, and Iocane[158] often to become the "*secondary provider for existing cloud customers (i.e., with AWS or Microsoft remaining as the primary provider)*".[159]

Traditional enterprise customers and Microsoft's ecosystem of business software

124. For cloud providers, the overwhelming majority of the addressable market is made up of workloads that are currently running in an on-premises environment. Microsoft's ecosystem of business software, which it has developed over the past 30 years, is central to a traditional enterprise customer's on-premises IT footprint and includes several key products in relation to which the CMA has found that Microsoft has significant market power.[160]

125. It follows therefore that Microsoft software-related workloads account for a significant proportion of all workloads that have not yet migrated to the cloud.

126. It can be technically and operationally challenging, as well as time-consuming, to migrate on-premises workloads to the cloud, especially given that many companies have developed their IT architectures over several decades to run in their own on-premises data centres without ever planning to migrate those workloads to a new environment. That is why many customers

[155] See CMA, 'Cloud Services Market Investigation Competitive Landscape Working Paper', *CMA Cloud Services Market Investigation* (6 June 2024), paragraph 9.24.
[156] See ACCC, 'Interim report 7: Report on expanding ecosystems of digital platform service providers', *ACCC Digital Platform Services Inquiry* (September 2023), 33-34, which notes that Amazon is the leading supplier of cloud infrastructure services in Australia with 32% market share (followed closely by Microsoft at 30%). See also Statista, 'Public Cloud - Australia', (Web Page, 2024) section on Key Players indicating that AWS has 25% market share and Microsoft has a 20% share.
[157] See CMA, 'Cloud Services Market Investigation Competitive Landscape Working Paper', *CMA Cloud Services Market Investigation* (6 June 2024), paragraph 5.12.
[158] See Aeroleads, 'Top IaaS companies in Australia', (Web Page, 2024).
[159] See CMA, 'Cloud Services Market Investigation Competitive Landscape Working Paper', *CMA Cloud Services Market Investigation* (6 June 2024), paragraph 5.21. See Ofcom, 'Final report', *Cloud services market study* (5 October 2023). Google has no reason to believe that its share of the market for cloud infrastructure services would be any different in Australia to what it is in the UK (i.e. ~5-10%).
[160] See CMA, 'Cloud Services Market Investigation Licensing Working Paper', *CMA Cloud Services Market Investigation* (6 June 2024), paragraph 6.13.

with a significant on-premises footprint prefer, at least at the point of first migration, to replicate their existing IT set-up in the cloud. Customers typically do this by adopting a so-called "lift-and-shift" approach, whereby they simply replicate their existing on-premises set-up in a cloud environment without making any material changes (including in relation to the tools and software they need to operate their IT infrastructure, i.e., their server operating systems, such as Windows Server or Linux).

127. In turn, this is why, when a customer migrates to the cloud, they need to be able to use their existing Microsoft software licences (e.g., for Windows Server) in the cloud environment of their choice. However, as Microsoft itself advertises[161] and Professor Jenny[162] and Ofcom[163] have both reported, Microsoft ensures that it is not commercially feasible for customers to transfer (or migrate) their existing Microsoft software from an on-premises environment to a cloud environment operated by a so-called Listed Provider other than Azure (namely, Alibaba Cloud, AWS and Google Cloud).

128. Google believes that Microsoft's software licensing restrictions are the only material barrier to fair and effective competition in the market for cloud infrastructure services, both in Australia and globally, and that absent the restrictions that Microsoft imposes, the market is capable of delivering good outcomes for customers in terms of quality, price and innovation.

Microsoft's licensing restrictions push software customers towards Azure

129. Pre-cloud, Microsoft did not have its own networking hardware offering and was therefore agnostic as to the hardware infrastructure used by its customers to run its products. However, following the launch of Azure, Microsoft came into direct competition with AWS, Google Cloud and other cloud providers, and therefore had a fresh incentive to restrict where customers could use its software. After noticing that most of its Windows Server customers were using its software in AWS, Microsoft started to impose significant restrictions that favour its own cloud offering, Azure.

130. Over time, Microsoft has strengthened restrictions on its existing on-premises customers' ability to "bring your own licence" (**BYOL**) to rival cloud infrastructure providers, thereby reducing competition and limiting customer choice.[164] Microsoft announced[165] two of the most

[161] Microsoft advertises that it is "*up to 5 times more expensive*" to migrate Windows Server and SQL Server to AWS than to Azure (see Microsoft, 'Optimize your Azure costs', *Microsoft* (Web Page, 2024)), and that customers can meet their "*mission-critical requirements up to 5 times faster while paying up to 93 percent less than with AWS*" (see Microsoft, 'Azure vs. AWS', *Microsoft* (Web Page, 2024).
[162] Professor Frédéric Jenny, 'Unfair Software Licensing Practices: A quantification of the cost for cloud customers', *CISPE* (Report, 21 June 2023).
[163] In its Final Report, Ofcom referred to one of Microsoft's blog posts describing how its licensing practices mean that "*Azure customers 'don't pay double*'", meaning that Azure customers – unlike AWS and Google Cloud customers – don't have to pay additional licensing fees when for migrating Windows Server and other key Microsoft software to the cloud (see Ofcom, 'Final report', *Cloud services market study* (5 October 2023), paragraph 9.21).
[164] See CMA, 'Cloud Services Market Investigation Licensing Working Paper', *CMA Cloud Services Market Investigation* (6 June 2024), section 2.
[165] See Microsoft, 'Updated Microsoft licensing terms for dedicated hosted cloud services', (Media Release, 1 August 2019).

notable restrictions to its licensing arrangements in 2019 and 2022, which are described in detail in section 2 of the CMA's Cloud Services Market Investigation Competitive Landscape Working Paper:[166]

a. **Pre-2019**: With certain specific exceptions, prior to October 2019 customers with perpetual on-premises licences for certain Microsoft software did not have the right to deploy these licences on the shared infrastructure (i.e., the public cloud) of non-Azure cloud providers on a BYOL basis. This meant that if customers wanted to use certain Microsoft software (e.g., Windows Server, which the CMA's research found is "*key, critical, fundamental or foundational*" for customers[167]) in competing cloud environments, they would have to repurchase new licences from the relevant cloud provider (or a third-party provider) pursuant to their Service Provider License Agreement (**SPLA**) at significant additional cost.[168]

   If a customer was willing to pay the higher prices associated with running their software on dedicated infrastructure, customers could use their existing licences on any cloud on a BYOL basis, irrespective of whether that dedicated hardware was provided by Azure or another cloud provider.

b. **2019 changes**: In 2019 Microsoft modified its licensing terms to shut down this dedicated option as well. Microsoft created a new category of "Listed Providers" (Azure, Alibaba Cloud, AWS, and Google Cloud), and changed its licensing terms such that customers with perpetual Windows Server licences could no longer deploy them on dedicated infrastructure offered by Listed Providers. That is, customers could no longer use their pre-existing Microsoft software licences, in which they had invested a significant amount, on Listed Provider infrastructure. While Microsoft includes Azure as a Listed Provider, it has effectively circumvented the restrictions by implementing the 'Azure Hybrid Benefit' programme, which allows customers with existing Windows Server or SQL Server licences to convert those licences to Azure at a significant discount that in effect means there are minimal additional licensing-related costs associated with migrating to Azure.[169] In contrast, customers who prefer to use these products in a non-Azure Listed Provider environment — Google Cloud, AWS, or Alibaba Cloud — must repurchase a new licence, essentially paying Microsoft a considerable and often cost-prohibitive penalty to do so.

---

[166] See CMA, 'Cloud Services Market Investigation Licensing Working Paper', *CMA Cloud Services Market Investigation* (6 June 2024).
[167] Ibid, paragraph 3.59(a).
[168] The SPLA is an agreement between Microsoft and Google pursuant to which Google can resell Windows Server and SQL Server licences to end customers for use on Google Cloud infrastructure. Google understands that the price and non-price terms on which Google can resell Microsoft's software are far less attractive than the terms on which other non-Listed Providers, partners and third-party managed service providers (**MSPs**) are able to sell equivalent licences.
[169] In addition, the licence that is purchased is not the same as the previously owned one, in that it cannot then be brought to other clouds if the customer wishes to switch away from Azure. In this way, Microsoft converts licences which could be BYOL into ones which will only be valid on Azure.

c. **2022 changes**: In response to complaints from Aruba, OVHcloud and the Danish Cloud Community to the EC, on 1 October 2022, Microsoft introduced licensing changes globally that were designed to enable customers to use subscription licences in any non-Listed Provider cloud free of any additional charge. The penalty facing customers who prefer Listed Providers remained firmly in place. In addition, Microsoft announced at the same time that from 2025, third-party providers will be prohibited from licensing any software via their own SPLAs, if that software will ultimately be deployed on Listed Provider infrastructure. Instead, those providers would need to run their solutions on Azure to maintain their eligibility to supply SPLA licences. This eliminates the other way customers could attempt to use products like Windows Server on Listed Provider clouds.

131. In summary, Microsoft's restrictions mean that:

a. Customers with existing licences to key products like Windows Server are unable to use those licences on Google Cloud infrastructure.

b. The only way for customers (even those that have invested a significant amount building up a Windows Server footprint over several years or decades) to currently use Windows Server on Google Cloud infrastructure is if they purchase new licences from either Google or a third-party managed service provider (**MSP**) at a significant additional cost. By contrast, Microsoft's Azure Hybrid Benefit means that its existing Windows Server customers can freely BYOL their existing licences to Azure infrastructure at minimal additional cost.[170]

c. From October 2025, customers will no longer be able to purchase Windows Server licences from third-party MSPs (meaning the only way for them to use Windows Server on Google Cloud infrastructure will be if they purchase costly new licences from Google).

132. The result of these restrictions is that customers who wish to use AWS, Alibaba Cloud or Google Cloud are forced into significantly higher costs if they want to continue to use Microsoft's software than they would incur to use that same software on Azure.[171] Price is an essential

[170] CMA, 'Cloud Services Market Investigation Licensing Working Paper', *CMA Cloud Services Market Investigation* (6 June 2024), paragraphs 4.10, 5.29, and 6.5. The only new migration-specific cost for on-premises customers that applies equally irrespective of whether they move to Azure or a third-party cloud provider like Google Cloud, is the price of Software Assurance, which is generally 25% of the underlying licence cost. Marketed as a Microsoft maintenance programme, Software Assurance includes Licence Mobility, which is effectively a commercial add-on fee to existing on-premises Microsoft software licences to make those licences 'cloud eligible'.

[171] Evidence in support includes: (i) Jigsaw's customer research commissioned by the CMA, which found that "*[m]ost customers* [...] *identified that there were price advantages from using Microsoft software products on Azure.*" Customers explained that (a) "*Microsoft make[s] it cheaper to use [some of the services that the customer wanted to use in the cloud] in [Azure] than they do if you use it in somebody else's cloud*", and (b) "*[b]ecause Microsoft owned those licence agreements [for software like Windows Server and SQL Server], they were in control. They were able to heavily discount down*". See Jigsaw, 'Cloud Services Market Investigation, Qualitative Customer Research', (23 May 2024), 29 and 86; and (ii) Microsoft's own advertising which claims that "*AWS is up to 5 times more expensive than Azure for Windows Server and SQL Server*". See Microsoft, 'Azure Hybrid Benefit webpage', *Microsoft* (Web Page, 2024). See Google, 'Google Cloud's response to the CMA's Competitive Landscape working paper dated 23 May 2024', (23 May 2024), paragraph 8.

parameter of competition in cloud. By creating large price differences depending on where customers deploy software such as Windows Server, Microsoft is driving customers to Azure.

133. Microsoft also imposes artificial non-price differences that further exacerbate the effects on customer choice and rivals' ability to effectively compete. In particular:

a. Microsoft supplies dual use rights, which allow customers to freely deploy software in the cloud and on-premises at the same time to facilitate a customer's initial migration, to Azure customers for free. In contrast, Microsoft refuses to supply dual-use rights to customers that purchase Microsoft software from Google Cloud.

b. Microsoft also refuses to supply failover rights, which customers can use to freely deploy workloads that are exclusively used for disaster recovery purposes, for use on Google Cloud.

c. Microsoft requires customers that purchase Microsoft software from Google Cloud to purchase extended security updates (**ESUs**), which are necessary to maintain the security and viability of software, directly from Microsoft at a significant cost. Microsoft also limits the availability of those ESUs for Google Cloud customers to three years whereas it supplies Azure customers with ESUs for four years at no cost. In other words, Microsoft is skewing competition with respect to the vast majority of the addressable cloud infrastructure market in favour of its own Azure offering.[172]

134. The effects of the above restrictions and differences are further exacerbated by Microsoft's technical restrictions. As a result of the strong technical links between Active Directory – Microsoft's proprietary on-premises identity and access management (**IAM**) tool – and Microsoft's enterprise software, Active Directory has become a product that customers need their cloud-based IAM tools to integrate with as they migrate to the cloud. Active Directory operates seamlessly with Microsoft's own cloud-based IAM tool, Entra ID, but Microsoft refuses to supply sufficient interoperability information to allow competing cloud-based IAM providers to achieve the same level of integration.

135. Driving Azure usage via the licences of its key products has proven to be an effective strategy for Microsoft. As recently recognised by the CMA, Microsoft has significant market power in relation to several individual software products.[173] By imposing significant price differences and restrictions on Microsoft software when used with rival cloud infrastructure compared to when used with Azure, these practices are "*hav[ing] the effect of making a significant proportion of*

[172] Customer research by Jigsaw supports the idea that the interconnectedness of Microsoft's software increases its overall market power. The Jigsaw research finds that customers have a "*clear general desire to keep everything within a Microsoft ecosystem within their organisation*". See Jigsaw, 'Cloud Services Market Investigation, Qualitative Customer Research', (Report, 23 May 2024), paragraphs 1.4.37 and 7.1.
[173] CMA, 'Cloud Services Market Investigation Licensing Working Paper', *CMA Cloud Services Market Investigation* (6 June 2024), paragraph 6.13.

customer demand less contestable to rivals," thereby weakening "*its rivals' ability*" to compete.[174]

Microsoft's licensing practices are already having a detrimental effect on competition

136. The effects of Microsoft's restrictions are already being felt. Microsoft has rapidly increased its share of the market since implementing its most restrictive licensing practices in 2019 and is winning a significantly greater share of new cloud customers than other providers.[175] In addition, the future market opportunity that is presented by Microsoft software-related workloads that currently remain on-premises is significant. We therefore expect the negative effects to significantly worsen as traditional enterprise customers accelerate their transition from on-premises to the cloud.

137. Not only is Microsoft's conduct having an impact on those customers that are yet to migrate to the cloud – it is also having an impact on customers that already have. Developing an integrated multi-cloud architecture[176] can be challenging: when integrating workloads across public cloud environments, customers need to be able to freely port their data and decouple their applications from any underlying hardware or operating system. But an integrated multi-cloud architecture can also unlock substantial benefits such as the ability to (i) choose best-in class tools that are optimised to suit specific needs and (ii) securely distribute applications and data across environments and thereby enhance operational resilience.

138. That is why Google Cloud[177] and others are working towards reducing technical barriers to multi-clouding and migrating between different cloud providers, including by making significant investment in technological innovations[178] and network infrastructure to facilitate multi-cloud adoption. But for multi-cloud strategies to work, all industry players need to equally commit to abstaining from practices that lock-in customers.[179] Currently, Microsoft lacks any incentive to do so and the result is that customers face less choice and are exposed to a single point of

[174] See Jigsaw, 'Cloud Services Market Investigation, Qualitative Customer Research', (Report, 23 May 2024), paragraph 1.13. See CMA, 'Cloud Services Market Investigation Licensing Working Paper', *CMA Cloud Services Market Investigation* (6 June 2024), paragraph 1.13.
[175] Professor Frédéric Jenny, 'Unfair Software Licensing Practices: A quantification of the cost for cloud customers', *CISPE* (Report, 21 June 2023), paragraph 43.
[176] Integrated multi-cloud refers to the scenario where customers mix and match cloud services from different cloud providers and there is a degree of integration between these services (i.e. data stored in one cloud environment can be analysed by services hosted in another).
[177] As part of our efforts on the Data Cloud Alliance initiative, Google Cloud is working with industry leaders to promote open standards and interoperability, with a view to alleviating the burden on customers when overcoming inherent technical barriers. Google Cloud also continues to support open source database engines like MongoDB, MySQL, PostgreSQL, and Redis, as well as running its own databases like Cloud Bigtable, Firestore, and Cloud Spanner which equally support the portability and data export needs of our customers. In addition to building products on open source technologies, Google Cloud offers a wide range of managed proprietary services which provide integrated open source components that improve data interoperability and portability and provider switching solutions (e.g., Google Kubernetes Engine, Cloud Composer, Dataflow, and Anthos).
[178] Including BigQuery Omni, Anthos and AlloyDB Omni.
[179] Google Cloud is and remains a consistent advocate and ally for the open source community, data portability, and interoperability, as is evident from its ongoing contributions to open source projects like TensorFlow and Kubernetes.

failure that creates significant operational and security risks[180] for customers. Customers were starkly reminded of these risks during the recent Crowdstrike outage that affected millions of devices worldwide and reportedly caused more than US$500 million in damages.

139. The practices carried out by Microsoft have attracted the attention of competition agencies globally, with the CMA currently investigating whether its licensing practices disincentivise *"customers from using rival providers"*.[181] Microsoft's licensing practices are also being investigated by the EC[182] and others. We encourage the ACCC to similarly investigate these practices and restrictions.

140. The cloud market is at an inflection point in the transition from legacy on-premises IT services to the cloud. For customers to fully reap the benefits of cloud services, they must have the option to choose cloud service providers based on the merits of their propositions. Google strongly believes that when migrating to the cloud for the first time, switching, and/or using multiple cloud infrastructure providers, customers' freedom to choose among providers would be significantly improved if customers could deploy existing, previously purchased software licences in any cloud environment without incurring the significant artificial surcharge or other technical restrictions imposed by Microsoft.

Topic 3 - 1.3.3: Potential competition issues in generative artificial intelligence

The ACCC invites interested parties to share their views on potential or emerging competition and consumer issues in relation to generative AI in Australia. *Please provide as much detail or evidence as you can to support your response.*

141. We offer the following perspectives to inform the ACCC's consideration of competition and consumer issues in genAI in Australia.

142. GenAI is a transformational technology with huge potential for driving innovations to unlock new discoveries that will be critical to tackling humanity's greatest challenges and opportunities. Our approach to developing and harnessing the potential of genAI is grounded in our founding mission - to organise the world's information and make it universally accessible and useful - and we believe both individual and collective efforts are essential to getting AI right.

143. The Issues Paper recognises that "*Generative AI products and services may present new opportunities, but also new challenges*". We agree - this is why we have voluntarily adopted AI

---

[180] See Cyber Safety Review Board, 'Review of the Summer 2023 Microsoft Exchange Online Intrusion', (20 March 2024).
[181] See CMA, 'Public cloud infrastructure services market investigation: Issue statement', *Public Cloud Infrastructure Services Market Investigation* (5 October 2023).
[182] The EC is informally investigating Microsoft's alleged anti-competitive licensing and tying/bundling tactics based on a complaint made by CISPE (now withdrawn) – a European cloud industry association. On 11 July 2024, Microsoft and CISPE reached a settlement agreement, which included a significant payment by Microsoft to CISPE. See CISPE, 'CISPE and Microsoft Agree Settlement in Fair Software Licensing Case', *CISPE.cloud* (Media Release, 11 July 2024).

Principles,[183] which describe our commitment to developing technology responsibly and work to establish specific application areas we will not pursue.

144. As explained in our DPSI 9 response and in further detail below, there is continued dynamism and innovation at every layer of the AI value chain, driven by grassroot players, open source organisations, academic institutions and a myriad of new start-ups alongside established industry players. In particular:

   a. **The AI industry is characterised by a high degree of dynamism bringing significant growth opportunities:** The increasing rate of AI company formation in Australia and around the world and widespread dissemination of AI tools is driving innovations and competition and unlocking growth opportunities, helping small and large businesses to innovate and grow.

   b. **Openness has been a cornerstone of AI:** At Google we have been prominent supporters of open science and open software as a way to foster innovation and competition.

   c. **A collective effort by all stakeholders is necessary to get AI right:** We believe that all stakeholders must work together to find solutions that strike a careful balance between the great potential of AI to benefit people, society and humanity and the risk of misuse and unsafe applications.

Our approach to AI

145. Google believes that openness will continue to drive growth and innovation in the AI industry while maintaining low barriers to entry and expansion in any related market. Google is committed to openness and is proudly the leading contributor to the open source community.[184]

146. While we recognise the significant national security and public safety considerations at play, we have been key contributors[185] to responsible open research, open source AI projects and open models that have laid the foundation for today's progress. Key contributions we have made include:

   a. **Open source code**. We have been one of the leading contributors of open-source code, including fundamental technologies like Kubernetes and the Go programming language.

   b. **Major research breakthroughs**, such as the "Transformer" architecture,[186] which now forms the backbone for the large foundation models (**FMs**) that sit behind most AI capabilities. The transformer technology — the "T" in OpenAI's ChatGPT — is what

[183] Google, 'Our Principles', *Google AI* (Web Page).
[184] See 'Open Source Contributor Index', (Web Page).
[185] Eric Brewer and Abhishek Arya, 'Shared success in building a safer open source community', Google's The Keyword (Blog Post, 12 May 2022).
[186] See Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, Illia Polosukhin, 'Attention is all you need', *Accessibility Forum,* (Web Page, last revised 2 August 2023).

enables genAI and was developed by Google researchers and made freely available in 2017.

c. **Industry-wide AI/ML software**, such as the TensorFlow[187], JAX[188] and PaxML[189] machine learning (**ML**) frameworks, which are coding libraries designed to streamline the FM development process.

d. **Open FMs**, which began with our open source software model BERT[190] (on top of which the AI community developed numerous innovations, e.g., RoBERTa[191]), and recently our new family of smaller-scale open models, Gemma.[192] In particular, Gemma can be run on a laptop and hosted by rival cloud platforms, thereby lowering barriers to entry and spurring innovation.

147. **Google is also keenly aware of the safety challenges that open AI models present** – in particular with respect to the most advanced ("frontier") AI systems and if model weights are made publicly available. This is because, unlike other digital services, the proliferation of AI model capabilities (especially "frontier" capabilities) to and by bad actors could pose serious safety challenges. It is therefore critical to strike the right balance between harnessing the benefits of open source and managing AI's significant risks.

148. We understand that models with open weights can pose unique risks, because it is impossible to reverse the decision to make weights available widely. For example, we open-sourced AlphaFold[193] only after extensive consultations with bioethicists, and the tool is now used by 1.5 million biology researchers around the world. Likewise, the release of our Gemma family of open models was grounded in our approach to safety and responsibility. As a founding member of the Frontier Model Forum,[194] we are committed to advancing AI safety research and developing best practices for the industry.

149. As a leading proponent for Responsible AI,[195] Google takes our AI Principles[196] seriously. This careful balancing of openness, opportunity, responsibility and security underpins our approach to AI development and access.

a. **We develop best practices based on these principles that help reduce the risk of harm when designing AI systems.** These include, for example, using a human-centred design approach (e.g., by making appropriate disclosures and incorporating human feedback before and throughout development); using more than one metric to assess

[187] See GitHub, 'tensorflow/tensorflow', (Web Page, 2024).
[188] See GitHub, 'google/jax', (Web Page, 2024).
[189] See GitHub, 'google/paxml', (Web Page, 2024).
[190] See Hugging Face, 'BERT', (Web Page).
[191] See Hugging Face, 'RoBERTa', (Web Page).
[192] See Google, 'Building Open Models Responsibly in the Gemini Era', *Google Open Source Blog* (Blog Post, 21 February 2024).
[193] See Google, 'AlphaFold', *Google DeepMind* (Web Page).
[194] See Frontier Model Forum, 'Frontier Model Forum, Advancing frontier AI safety', *Frontier Model Forum* (Web Page, 2024).
[195] Google, 'Responsible AI practices', *Google AI* (Web Page).
[196] Google, 'Our Principles', *Google AI* (Web Page).

training and monitoring; directly examining the raw training data when possible; understanding and disclosing the limitations of a model; conducting rigorous testing; and continuing to monitor and update the system after deployment. We are proud to have joined other leading AI developers in making commitments to heightened safety and security practices for our most advanced models.

b. **We help third-party developers mitigate risks to users.** For example, we provide to developers and publishers the open-source Perspective API, which helps detect and filter out potentially toxic comments in training datasets and can reduce the chance that a generative language model will produce toxic text.

c. **We invest in AI safety research that guides and enables our Responsible AI efforts.** Our dedicated research teams are working on various research programmes from foundational questions (e.g., how to make AI evaluation standards more robust), socio-technical issues (e.g., how to strengthen the involvement of under-represented or vulnerable communities), and on specific products (e.g., DeepMind's research into useful and safe dialogue agents that led to the experimental Sparrow[197]).

d. **We have launched and support a number of proactive safety and security initiatives to improve accountability and responsibility throughout the AI supply chain**. Beyond the Frontier Model Forum,[198] Google is a founding member of the Partnership on AI[199] and actively contributes to safety benchmarking of AI systems via the ML Commons.[200] In June 2023, Google also launched our Secure AI Framework, which offers best security practices for the development and deployment of AI systems across the public and private sectors.

Dynamism at every layer of the AI value chain

150. As discussed in our DPSI 9 response,[201] we have observed — and fostered — increasing dynamism throughout the AI industry at every layer of the AI value chain. This dynamism coupled with ready and sustained access to key inputs for AI model development and deployment is driving intense competition between a variety of companies including a host of new AI developers and providers. The result is a thriving and growing market that is delivering innovative products and services for both existing and new use cases.

151. The Issues Paper cites a Digital Platform Regulators Forum paper from October 2023 which suggests that "*Developing and operating LLMs requires a large financial investment upfront, access to vast datasets, long development lead times, access to sophisticated AI systems and talent, and substantial ongoing computing costs and access to computing resources (such as cloud storage), which together create high barriers to entry.*" We consider that these barriers to

---

[197] Google, 'Building safer dialogue agents', *Google DeepMind* (Web Page, 22 September 2022).
[198] See Frontier Model Forum, 'Frontier Model Forum, Advancing frontier AI safety', *Frontier Model Forum* (Web Page, 2024).
[199] See 'Partnership on AI', (Web Page, 2024).
[200] See ML Commons, 'Benchmark for general purpose AI chat model', *ML Commons* (Web Page, 2024).
[201] Google, 'September 2024 report on "revisiting general search services": Google's Response to ACCC Issues Paper', *ACCC Digital Platforms Services Inquiry* (3 May 2024), 3 - 5.

entry are overstated.

152. There are several factors which are lowering barriers to entry and enabling access to economies of scale in the AI space so that it is easier to develop, train and deploy AI models.[202] These factors include:

a. A maturing cloud infrastructure market that offers a range of infrastructure options to AI companies.[203]

b. A pivot in FMs from size to quality and efficiency demonstrated by, amongst other things, increasing focus on model architecture, reliance on datasets available from public sources such as GPT-3,[204] and the open models LLaMA[205] and Vicuna 13-B,[206] and declining costs for high quality datasets for AI model fine-tuning. For example:

i. **Model architecture:** Several of Google's top models (e.g., Gemini or PaLM 2) have focused on developing more efficient model architectures, which has resulted in much smaller models (requiring less compute resources to train and serve) with better overall performance and efficiency than their comparators.

ii. **Datasets for genAI model pre-training:** Model pre-training relies heavily on datasets from public sources. This is particularly the case for general purpose genAI models (e.g., a large language model). Many of these data sets are naturally high-quality, and there are a large and growing number of open source data sets curated and processed specifically for genAI model training. Many notable FMs are trained using entirely public or open source data (e.g., large textual datasets). This includes GPT-3, 21 and the open models LLaMA 22 and Vicuna 13-B.

iii. **Datasets for genAI model fine-tuning:** High-quality data such as Reinforcement Learning from Human Feedback (**RLHF**) is an important source for training and fine-tuning AI models. While more costly than other sources (e.g., those produced using public sources) due to its use of human "raters" or "participants", the cost for RLHF is by no means prohibitive for the many VC-backed, well-funded AI start-ups. These costs are also expected to decline further as a result of an emerging industry of outsourced RLHF services, increased automation and innovation in synthetic data curation techniques.

c. Dynamic financing and incubation infrastructure available to fund and support

[202] See also Google, 'September 2024 report on "revisiting general search services": Google's Response to ACCC Issues Paper', *ACCC Digital Platforms Services Inquiry* (3 May 2024), section 2.2.
[203] Certain practices in the cloud infrastructure market may jeopardise its competitiveness, as discussed above at Topic 1.3.2.
[204] See Tom B Brown et al, 'Language Models are Few-Shot Learners', *Open AI,* (Proceedings of the Conference on Neural Information Processing, 22 July 2020).
[205] See Meta, 'Introducing Meta Llama 3: The most capable openly available LLM to date', *Meta Blog* (Blog Post, 18 April 2024).
[206] The Vicuna Team, 'Vicuna: An Open-Source Chatbot Impressing GPT-4 with 90%* ChatGPT Quality', *LMSYS Org* (Blog Post, 30 March 2023).

innovation in training new AI models.

d. A growing pool of talent in the AI sector both globally and in Australia, which Google is itself contributing to, through its free genAI courses available on Google Cloud.[207]

153. The ready availability of key inputs to AI development is enabling an ever-growing variety of use cases from established industry players (e.g., Microsoft, Amazon, Google, Meta) to agile and well-funded start-ups (e.g., Anthropic, Cohere, AI21 Labs, stability.ai) and academic and open-source institutions (e.g., Together, Stanford CRFM). Most recently in Australia, Leonardo.Ai — a genAI content creation platform — released its own AI FM, Phoenix, after previously using a modified version of Stable Diffusion by stability.ai.[208]

Dynamism and innovation means new entrants can—and do—compete across the AI value chain

154. It is easier than ever before for a developer— even one without extensive AI/ML experience — to start making and offering new AI-powered products and solutions, or to transform existing products and solutions with AI-powered features.

155. Advances in AI model capabilities have enabled brand new use cases and new classes of products, including generative dialogue agents/assistants, image/art generators, and virtual mental health support/companions. More established AI model developers are facing competition from innovative developers who have created specialised models[209] and genre-defining new products, including apps (often using AI models from third parties), which now populate the top charts across different app stores.

156. For existing use cases, AI models have created brand new possibilities that have shifted the paradigms. Consumers and businesses alike are expecting new and enriched experiences on these products, as developers race to introduce new AI-powered features to their existing products, and new players take advantage of the opportunity created by this shifting demand to enter the market. **Annex B** is a snapshot as of September 2023 showing a non-exhaustive sample of the wide variety of genAI players that have emerged at the global level, driving dynamism and innovation in the market.

157. We believe that ensuring the full potential of AI is realised requires a collective effort by researchers, developers, deployers, academics, businesses, consumers and governments. We are seeing innovation in genAI unfold at pace in Australia and across the globe and there are no signs that this dynamism is slowing. To the contrary, we are seeing a growing number of genAI startups and new entrants creating new models and use cases for genAI. In this context, Google has strong incentives to keep innovating its genAI offerings.

---

[207] See for example Google Cloud, '12 days of no-cost training to learn generative AI this December', (Blog Post, 2 December 2023) and Google Cloud, 'Generative AI on Google Cloud: New training content, from introductory to advanced', (Blog Post, 13 September 2023).

[208] See Phoenix by Leonardo.Ai, 'Phoenix by Leonardo.Ai - meet the future of AI image generation', (Web Page).

[209] For instance, Runway's "Customer stories" indicates its genAI video and image models are innovating to meet the demands of creatives such as filmmakers and advertisers. See Runway, 'How the world's top creatives are using Runway', *Runway* (Web Page, 2024).

158. To preserve and foster this level of innovation and dynamism requires all stakeholders to work together to find solutions that strike a careful balance which recognises the great potential of AI to benefit people, society and humanity, encourages innovation and safe and beneficial use of the technology, while avoiding misapplication, misuse and harmful uses.

CONCLUSION

159. Google appreciates the opportunity to comment on the ACCC's consultation on DPSI 10. We look forward to working constructively with the ACCC as it consults with market participants and prepares its report.

Annex A
Google's messaging and video conferencing products

Google Messages	The Google Messages app enables users to send and receive text messages, photos, voice messages and videos.[210] The app is available on Android devices (but not iOS devices); users can also check messages via a web browser. Google Messages' features include: ● Support for RCS which:[211] – Show the user when someone is typing. – Offer read receipts, which show when someone has read or received a message. – Send messages over mobile data and Wi-Fi. – Let users share files and high-resolution photos. ● Technology that keeps conversations private. For example: – Conversations that use RCS in Google Messages are upgraded to **end-to-end encryption** by default. With end-to-end encryption, no one can read the content sent between those users.[212] – Google Messages **creates suggestions** with technology that's built into the user's device. Users' conversations stay in the Google Messages app, and aren't sent to the Google Assistant or Google servers.[213] – Google Messages can provide **automatic previews** for links, places and other types of content. Automatic previews only use select information (like addresses and links), without saving them to the user's Google Account or Location History or linking them to identifiers like the user's name or phone number. Users can disable automatic previews.[214] – Google Messages has **spam detection** features by default. Users can disable spam detection.[215]

[210] Google, 'Get started with the Google Messages app', *Google Messages* (Web Page, 2024).
[211] Google, 'Turn on RCS chats in Google Messages', *Google Messages* (Web Page, 2024); Google, 'RCS chats by Google FAQ', *Google Messages* (Web Page, 2024).
[212] Google, 'Understand the basics of privacy in Google Messages', *Google Messages* (Web Page, 2024).
[213] Google, 'Your chats stay private with Google Assistant in Google Messages', *Google Messages* (Web Page, 2024).
[214] Google, 'Your chats stay private with automatic previews', *Google Messages* (Web Page, 2024).
[215] Google, 'Your chats stay private with spam detection', *Google Messages* (Web Page, 2024).

	Google Messages collects performance data, crash logs and diagnostics. We also use this information to help prevent abuse of our services.[216] However, we don't use information collected in the Google Messages app for advertising purposes.[217]
Google Meet	Google Meet is part of our Google Workspace product suite.[218] The Google Meet app enables users to make video calls and meetings. The app is available on Android devices, iOS devices and on web browsers.[219] Meet users can communicate using either: ● **1:1 and group video calling**: Involves ringing a number or group directly. Users can make unlimited video calls with no time limits. All calls are end-to-end-encrypted.[220] ● **Meetings**: Users signed in with a Google Account can create or join a Google Meet meeting with a link. Additional meeting features (not available in calls) include: in-meeting chat, reactions, add-ons, polls and Q&A; the ability to report abuse; live closed captions in a video call; virtual backgrounds and visual effects; meeting scheduling; and larger groups of up to 100 people in a meeting.[221] ● Meetings are cloud-encrypted, which means that the user's information is encrypted in transit and when stored in Google's data centres, as are any call recordings stored in Google Drive.[222] We process some data to offer users better experiences in the product, and to provide features like Smart Reply and spam detection. Users can control their privacy settings in Google Account.[223] However, we don't use information in Google Meet for advertising purposes.[224]
Google Chat	Google Chat is part of our Google Workspace product suite. The Google Chat app enables users to use Google Chat to message and collaborate with others. The app is available on Android devices, iOS devices and on

216 Google, 'Understand the basics of privacy in Google Messages', *Google Messages* (Web Page, 2024).
217 Google, 'Understand the basics of privacy in Google Messages', *Google Messages* (Web Page, 2024).
218 Google, 'Google Meet: Video calls with anyone, anywhere', *Google Workspace* (Web Page, 2024).
219 Google, 'Download the new Google Meet app', *Google Messages* (Web Page, 2024).
220 Google, 'Learn about the new Google Meet app', *Google Messages* (Web Page, 2024).
221 Google, 'Learn about the new Google Meet app', *Google Messages* (Web Page, 2024); Google, 'Learn about call and meeting encryption in Google Meet', *Google Meet Help* (Web Page, 2024).
222 Google, 'Learn about call and meeting encryption in Google Meet', *Google Meet Help* (Web Page, 2024).
223 Google, 'Understand the basics of privacy in Google Meet', *Google Meet Help* (Web Page, 2024).
224 Google, 'Understand the basics of privacy in Google Meet', *Google Meet Help* (Web Page, 2024).

web browsers. Users can also use Chat directly in Gmail (on Android devices, iOS devices and on web browsers).[225]

Google Chat can be used to:[226]

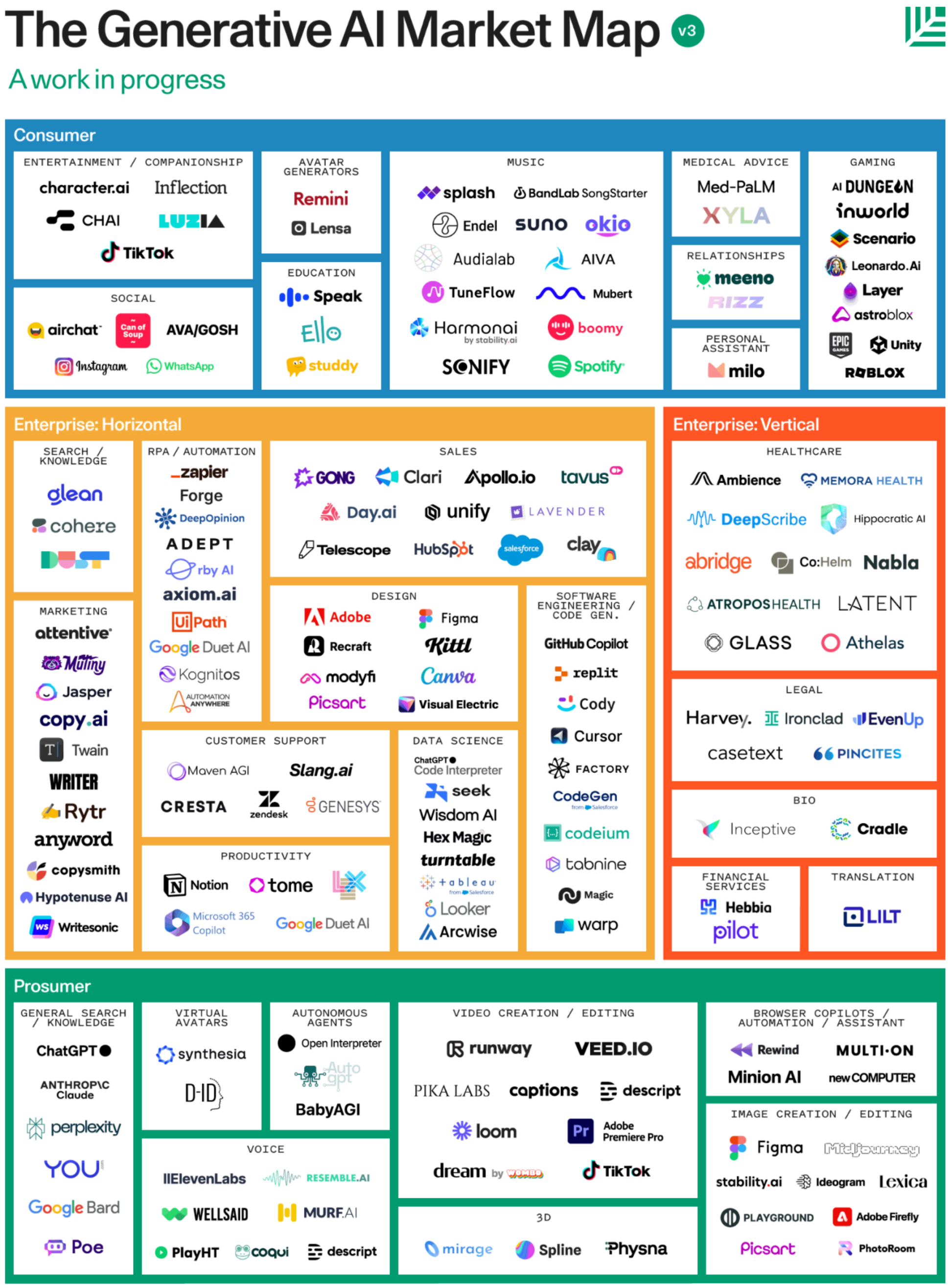
- Message people directly or in small group messages.
- Collaborate in large, named groups called spaces.
- Send and share files from Google Docs, Slides and Sheets.
- Set up tasks and meetings, and add apps to enhance productivity.

All messages and attachments sent in Google Chat are encrypted in-transit and when stored in Google's data centres.[227]

We process some data to offer users better experiences in the product, and to provide features like Smart Reply and spam detection. Users can control their privacy settings in Google Account.[228] However, we don't use information in Google Chat for advertising purposes.[229]

[225] Google, 'Get started with Google Chat', *Google Chat Help* (Web Page, 2024).
[226] Google, 'Get started with Google Chat', *Google Chat Help* (Web Page, 2024).
[227] Google, 'Understand the basics of privacy in Google Chat', *Google Chat Help* (Web Page, 2024).
[228] Ibid.
[229] Ibid.

Annex B
A snapshot of genAI players[230]



[230] See Sequoia Capital, '[Generative AI's Act Two]', (Web Page, 20 September 2023). Please note that the genAI landscape is developing quickly and that this snapshot is non-exhaustive even as at 20 September 2023. Please also note that Bard is now known as Gemini, and Duet AI as Gemini for Google Cloud (a portfolio of products that includes Gemini Code Assist). See also Antler, '[Mapping the Generative AI landscape]', (Blog Post, 20 December 2022), and [underlying data] with funding round information, for a snapshot of the global genAI startup landscape as of December 2022.