9 September 2024

Apple Pty Ltd

Submission in response to the Digital Platform Services Inquiry Discussion Paper

The Australian Competition and Consumer Commission (**ACCC**) has invited stakeholder views on recent overseas legislative and regulatory developments in markets for digital platform services and the impact on competition and consumers, major developments and key trends in certain markets for digital platform services, and potential and emerging competition and consumer issues which relate to digital platform services.

Apple Pty Limited (**Apple**) welcomes the opportunity to provide written feedback in response to these and other matters raised in the ACCC's issues paper for the Digital Platform Services Inquiry - March 2025 - Final Report, dated 25 July 2024 (**Issues Paper**).

1. Executive Summary

1. Apple acknowledges the importance of ensuring that digital platform operators—like all firms—operate within fair and competitive markets, and that appropriate legal frameworks and regulatory oversight can address market failures where they arise and otherwise guard against threats to consumers.

2. As Apple has articulated in prior submissions to the ACCC and separately to Treasury[1], Apple believes that the investigative and public enforcement tools available under the current competition and consumer protection regulatory regime in Australia are effective to address competition issues and to protect consumers, including with respect to issues unique to digital platforms.

3. Insofar as Apple's products and services are concerned, there is no objective credible evidence of a market failure which requires a regulatory response directed specifically at Apple as a digital platform operator, nor should sweeping changes be implemented

[1] See, in particular, Apple submission to DPSI, 1 April 2022 (https://www.accc.gov.au/system/files/Apple.pdf?ref=0&download=y) and Apple submission to Treasury, February 2023 (https://treasury.gov.au/sites/default/files/2024-01/c2022-341745-apple_pty_ltd.pdf)

simply on the basis that particular products or services are popular with Australian consumers. To do so risks harming both competition and consumers, including by chilling innovation and increasing security and privacy risks.

4. This submission is not intended to revisit in detail the bases for Apple's views as to the adequacy of the existing competition law framework in Australia and Apple's serious concerns about the risk and downsides of an ex ante framework, especially if crafted or implemented in the wrong way.

5. As described in previous submissions, Apple continues to believe that the existing competition law framework is adequate to protect both competition and consumers, and that the proposed reforms would risk leaving Australian consumers worse off. Even the Government, in its 8 December 2023 *Response to ACCC Digital Platform Services Inquiry*, acknowledged that *"the introduction of any new ex ante regime would be a significant undertaking and it would be critical to develop a framework that ensures Australians continue to enjoy the benefits of the best technology in the world"* and that *"international experience has demonstrated the complexities in achieving the appropriate and effective regulatory approach"*.[2]

6. To that end, and noting the ACCC's invitation for stakeholder views on recent regulatory developments in other jurisdictions, Apple seeks in this submission to highlight the very real risks to consumer welfare from forms of ex ante regulatory intervention which seek to heavily prescribe market outcomes. This can include unintended negative consequences, including the removal of existing platform structures and policies directed at privacy, security and general consumer protection, or through a similarly unintended chilling of market dynamism and innovation. Given the Australian Government's focus on cyber security, privacy, online safety and combatting scams, ex ante regulatory intervention for app distribution services could inadvertently undermine the Government's progress on these important issues.

7. Because the risk of regulatory error is high, and the adverse consequences of any regulatory error in this sector for innovation, the online economy, regulatory burden and the safety, security and privacy of consumers are substantial, the timing and scope of any ex ante regulation should therefore be calibrated with corresponding caution.

8. Based on its experience to date of the nascent reforms introduced in other jurisdictions, Apple submits that:

   (a) the impact of reforms in other jurisdictions on consumers and competition is uncertain. Therefore, any regulatory reform in Australia would benefit from an assessment of whether those reforms have achieved their goals—including considering any unintended negative consequences (such as potential anticompetitive effects)—after sufficient time has been allowed for careful and thorough observation;

   (b) overseas regulation which has taken a very prescriptive form, in particular the Digital Markets Act (**DMA**), demonstrates the risk that regulation can degrade consumer experiences, including by introducing safety, security and privacy risks, by having a chilling effect on innovation, as well as potentially curtailing

[2] See Government Response to ACCC Digital Platform Services Inquiry at page 4 (https://treasury.gov.au/sites/default/files/2023-12/p2023-474029.pdf)

the suite of services available to Australian businesses and consumers due to regulatory aversion or uncertainty (as has already been observed in Europe); and

(c) if Australia does pursue regulatory reforms at this time, it should ensure that purported pro-competitive changes do not impair Apple's ability to continue safeguarding user security, online safety and privacy and to provide Australian consumers with new Apple products and services available elsewhere in the world. Furthermore, incentives to innovate and develop new technologies should not be eroded by a regulatory framework that discounts the value of IP in new technologies and risks removing "*first mover*" advantages.

9. With respect to the ACCC's request for input 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, Apple observes that:

(a) as previously submitted to the ACCC, existing competition in app marketplaces is sufficient to constrain any purported exercise of market power by Apple having regard to the currently observable fee benchmarks and fee structures across platforms;

(b) in gaming, one of the major use cases relevant to app marketplaces, the dynamic nature of the market is reflected in continuing innovations in cross platform play, progression and wallets, and the increasing availability of cloud gaming / game streaming; and

(c) efforts by bad actors have continued to intensify, requiring corresponding vigilance and heavy investment on the part of platform and app store operators to safeguard consumers, with centralised distribution of apps through curated app stores proving more effective at protecting user security and online safety and privacy than systems that permit sideloading or place less emphasis on malware and social engineering detection.

10. With respect to the ACCC's request for interested parties to identify potential or emerging competition and consumers issues in relation to online gaming, cloud computing or generative artificial intelligence (**AI**), Apple submits that:

(a) generally, there is no indication of competition market failure related to online gaming in Australia, and developers have a wide variety of platforms through which to distribute their apps;

(b) online games may employ manipulative or deceptive design elements, giving rise to consumer concerns which illustrate the need for thorough app review, fraud detection and parental controls, rather than ex ante reforms which could reduce digital platform operators' ability to maintain and further improve such measures; and

(c) generative AI is an emerging and extremely dynamic area, and it would be premature to introduce ex ante competition regulation in relation to AI alone, which could have the unintended consequences of stunting further development and the rollout of AI technologies.

2. International Regulatory Developments

11. The ACCC has invited 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.

12. As the ACCC has acknowledged, in most cases, legislation has only recently been enacted and the full impact of recent international regulatory developments cannot yet be observed. Noting this, the ACCC has invited parties to provide their views on these developments more broadly, including views on potential or anticipated impacts on competition and consumers.

13. There has been a recognition in jurisdictions seeking to establish appropriately balanced regimes that there can be a tension between introducing ex ante reforms which purport to promote competition, while at the same time ensuring protection of consumers' privacy, security, and safety in a sector where actual harm from bad actors is rife. One such example is a pilot assessment being conducted by the Singapore Cyber Agency by agreement with Google to no longer permit sideloading in Singapore owing to the consumer harm correlated to this practice[3].

14. For the reasons set out in more detail below, Apple submits that:

    (a) recent international regulatory developments, in particular the highly prescriptive (but also vague) terms of the DMA, demonstrate that ex ante reforms with the stated purpose of improving competition can risk poor consumer and market outcomes if there is insufficient consideration of consumer interests, including by:

        (i) introducing safety, security and privacy risks that may make consumers more vulnerable; and

        (ii) having a chilling on innovation and the availability of the most up to date services and features.

    (b) if Australia does pursue regulatory reforms, it should ensure that any changes do not prevent or discourage companies like Apple from continuing to safeguard user security, online safety and privacy, and that incentives to innovate and develop new technologies for Australian users are not reduced by a regulatory framework that discounts the value of intellectual property in new technologies and potentially removes "*first mover*" advantages.

2.1 Regulatory reform in Australia would benefit from further assessment of the efficacy of reforms in other jurisdictions

15. Apple has concerns about the implementation of regulatory reforms in circumstances where:

---

[3] https://techcrunch.com/2024/02/07/google-starts-blocking-users-from-sideloading-certain-apps-in-singapore/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGkoUf1gfIkt3-OnNUXVZh0HqMZBlF0s4YCXCDkkpB5D1fe1Z1KJ4iiJebjz1jHwWx

(a) reforms would be directed at addressing hypothetical (rather than documented and evidence-based) problems insofar as conduct attributable to Apple is concerned; and

(b) there is no evidence that the existing competition and consumer law regulatory framework is insufficient to address the issues of concern identified by the ACCC in the DPSI, insofar as those concerns are relevant to Apple and to the extent that those issues might in fact materialise in the future.[4]

16. To the extent that regulatory reforms in Australia might seek to draw upon lessons from recent international regulatory developments, most of those developments are at an early stage of implementation, and, as a result, the efficacy of these reforms cannot yet be adequately assessed. What can be observed already is that where a new regulatory regime has been highly interventionist (such as in the EU), it has been led to regulatory uncertainty, and unintended negative consequences (including potential anticompetitive effects, reduction to consumer protections and chilling of innovation).

2.2 International regulatory developments demonstrate the risks to consumer welfare (including privacy, security, and safety) that regulation can pose

17. When Apple first launched its software development kit (**SDK**) in 2008 to enable third parties to develop software for Apple's proprietary iOS operating system, leading to the introduction of third-party apps and eventual development of the App Store, Steve Jobs stated:

> *"It will take until February to release an SDK because we're trying to do two diametrically opposed things at once - provide an advanced and open platform to developers while at the same time protect iPhone users from viruses, malware, privacy attacks, etc. This is no easy task."*[5]

18. Apple remains committed to balancing these two principles, which are inherently in tension; that is, providing an advanced and open platform to developers, and protecting iPhone users from viruses, malware, privacy attacks and other security and safety threats.

19. The overall expressed policy objectives of ex ante regulation of the technology sector are not dissimilar to these two objectives that Apple has worked hard to balance effectively for over 15 years. But it is no easy task to legislate to achieve these market outcomes, and the risk of regulatory error is high.

20. Moreover, the threats from bad actors continue to multiply. Sideloading security threats are increasing[6]. Bad actors create malicious apps that can alter user data, hold it hostage for ransom, or leak it to the entire web. They can engage in deceptive or fraudulent activity, seek to track users without their consent, or compromise the functionality of devices. They can build sham websites and send phishing emails

---

[4] Apple submission to DPSI, 1 April 2022, paragraphs 1(a) - 1(b).

[5] Apple SDK announcement, 17 October 2007.

[6] https://arstechnica.com/security/2024/08/novel-technique-allows-malicious-apps-to-escape-ios-and-android-guardrails/

designed to trick users into giving away sensitive data, convince users to download dangerous software, or even attack web browsers. Cybercriminals can also attempt to steal users' information by accessing their devices without their knowledge or consent, using Bluetooth accessories and open network connections—or just getting physical access to a device. Bad actors can even try to hack users' information and messages while they're in digital transit to and from a device.[7]

21. Apple built the iPhone to protect users against these kinds of risks, combining hardware, software, and services designed to work together for maximum security and a transparent user experience, in service of the ultimate goal of keeping personal information safe.[8] Apple is committed to the following standards:

    (a) **Security:** Users trust their iPhones with their most sensitive data. Apple builds industry-leading security protections to help prevent anyone but the user from accessing the data on their iPhone.[9]

    (b) **Privacy:** Users should not be exposed to software or websites that collect, use, or share their information without their informed permission. Apple builds its products and services to give users control over their data and help protect them against the collection, use, or sharing of their information without their permission, and to make sure users know what data of theirs is being shared and how it is used, and that they can exercise control over it.[10]

    (c) **Safety:** Users should not be exposed to physical harm through iOS, including through apps that advocate for or cause harm. [11]

22. Users in Australia and elsewhere choose iPhone because of this commitment, which is differentiated from and competes with other smartphones on security, privacy, and safety protections.

23. Regulatory developments aimed at improving competition outcomes with respect to markets for digital platforms can have the unintended consequence of making it more difficult for Apple to safeguard the security, privacy and safety of its users and developers—attributes that set iPhone apart in the marketplace and which attract Australian consumers who prioritize those features. These types of ex ante regulations can have the perverse effect of *weakening* competition by diminishing features (including privacy and security features) that consumers value.

24. The DMA is a salient example of a recent international regulatory development which has imposed very prescriptive regulations aimed at improving competition in digital markets—while also creating uncertainty as to how Apple adequately comply due to vagueness—and has, in Apple's view, resulted in increased risk of adverse consequences when it comes to privacy, security, and safety for both consumers and developers, and has also already had a chilling effect on innovation.

---

[7] Complying with the Digital Markets Act, Apple's Efforts to Protect User Security and Privacy in the European Union, March 2024 (**DMA White Paper**), page 3.

[8] DMA White Paper, page 4

[9] DMA White Paper, page 4

[10] DMA White Paper, page 4

[11] DMA White Paper, page 4

European Union's new Digital Markets Act (DMA)

25. The DMA went into effect on March 6, 2024. Following designation of certain Apple services, Apple has implemented changes to iOS, Safari and the App Store, in attempts to comply with the requirements of the DMA.[12] The DMA requires designated providers like Apple to:

    (a) allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that provider;[13]

    (b) allow business users, free of charge, to communicate and promote offers, including under different conditions, to end users acquired via its core platform service or through other channels, and to conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the provider;[14] and

    (c) not require end users to use, or business users to use, to offer, or to interoperate with, an identification service, a web browser engine or a payment service, or technical services that support the provision of payment services, such as payment systems for in-app purchases, of that gatekeeper in the context of services provided by the business users using that gatekeeper's core platform services.[15]

26. The DMA required Apple to change the uniquely successful approach that it has employed to protect users' security and privacy, bringing greater risk to both consumers and developers.[16] Apple nevertheless has worked hard to provide users new options within the DMA framework that were as protective of security, privacy, and safety as possible, even though many risks remain. Apple has now introduced changes in Europe that include more than 600 new APIs, expanded app analytics, functionality for alternative browser engines, and options for distributing iOS apps and for payments.

27. Although Apple has worked hard to continue protecting user security, privacy, and safety within the DMA framework, the new options Apple introduced to comply with the DMA necessarily mean that Apple cannot protect users in the same way.

28. Two already observable negative consequences of the DMA are:

    (a) **increased privacy and security risks**: The DMA required changes to Apple's ecosystem that bring greater risks to users and developers. This includes new avenues for malware, fraud and scams, illicit and harmful content, and other privacy and security threats. These changes also compromise Apple's ability to detect, prevent, and take action against malicious apps on iOS and to

---

[12] https://www.apple.com/legal/dma/

[13] DMA Art. 6(4).

[14] DMA Art. 5(4).

[15] DMA Art. 5(7).

[16] DMA White Paper, page 5.

support users impacted by issues with apps downloaded outside of the App Store;[17] and

(b) **chilling effect on innovation**: The interoperability requirements of the DMA could force Apple to compromise its products in ways that risk user privacy and security. This has resulted in Apple delaying the rollout of new AI technologies on its iOS devices in the European Union (**EU**)[18].

DMA: Increased privacy and security risks

29. The DMA appears to require that Apple, among other things, provide for third-party app marketplaces or third-party app distribution on iOS devices and allow developers to use third-party payments processing services on iOS devices.

30. Centralised distribution for native apps means that the operating system is required to go to a single approved location to download native apps, which allows for a single point of review and enforcement. To date, there has never been a widespread consumer malware attack on iOS—which is exceptional for a modern computing platform.[19]

31. The DMA obligations undercut Apple's centralised distribution philosophy, and the new options for processing payments and downloading apps on iOS open new avenues for malware, fraud and scams, illicit and harmful content, and other privacy and security threats.[20]

32. The benefits of Apple's centralised app distribution are apparent when its security outcomes are compared with mobile platforms that do allow sideloading. Threat analyses of sideloading have repeatedly illustrated these real world impacts:

(a) Nokia Threat intelligence Reports have consistently found that Android devices (which support sideloading) are susceptible to exponentially higher malware infections than iPhone - the most recent 2023 Nokia Threat intelligence Report attached demonstrates (at page 15) the increasing (year on year) risks associated with sideloading apps to Android devices;[21]

---

[17] Apple's Non-Confidential Summary of DMA Compliance Report, https://www.apple.com/legal/dma/dma-ncs.pdf, page 1

[18] Core product re-design and curtailment of services have been announced and deployed by other gatekeepers such as Meta and Google by reason of the DMA.

https://about.fb.com/news/2024/01/offering-people-more-choice-on-how-they-can-use-our-services-in-the-eu/

https://blog.google/around-the-globe/google-europe/complying-with-the-digital-markets-act/

[19] DMA White Paper, page 5.

[20] Apple announces changes to iOS, Safari and the App Store in the European Union, https://www.apple.com/au/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/#:~:text=The%20changes%20include%20more%20than,DMA%20poses%20to%20EU%20users.

[21] Apple, Building a Trusted Ecosystem for Millions of Apps, A threat analysis of sideloading, October 2021, page 2

(b) Kaspersky Lab, Europe's largest cybersecurity services provider, estimated that in 2020, nearly 6 million attacks per month affected Android mobile devices owned by its clients;[22]

(c) Ponemon Institute estimated that a single mobile device infected with malware costs an organisation an average of nearly $10,000.[23]

33. In contrast, there has never been a widespread consumer malware attack on iOS users,[24] largely thanks to its security architecture, underpinned by the App Store, which provides for centralised app distribution through a single, trusted source.

34. The DMA compels Apple to significantly alter its approach to app distribution in the EU, and open its platform to allow third-party distribution and third-party payment processing, which increases risks to both consumers and developers.

35. This necessarily means Apple will not be able to protect users in the same way.[25] Apple has introduced new safeguards that reduce — but don't eliminate — new risks the DMA poses to EU users.[26] Users' experiences will vary significantly based on how each marketplace, app developer, and payment provider chooses to conduct their business, as Apple is not able to carry out on its own user protection functions, such as reviewing apps for a fuller slate of possible harms and requiring transparency features such as Privacy Nutrition Labels, in third-party distribution.

36. Consumers in Europe will need to recognize and protect against privacy, safety and security threats not present in other jurisdictions (because the DMA limits what protections Apple may provide), including:

(a) apps that contain scams, fraud and abuse, or that expose users to illicit, objectionable or harmful content or negatively affect the user experience, as Apple will not be able to prevent such apps from being distributed outside of the App Store[27]

---

[22] Apple, Building a Trusted Ecosystem for Millions of Apps, A threat analysis of sideloading, October 2021, page 7

[23] Apple, Building a Trusted Ecosystem for Millions of Apps, A threat analysis of sideloading, October 2021, page 8.

[24] DMA White Paper, page 5.

[25] DMA White Paper, page 5.

[26] Apple announces changes to iOS, Safari and the App Store in the European Union, https://www.apple.com/au/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/#:~:text=The%20changes%20include%20more%20than,DMA%20poses%20to%20EU%20users.

(a) Notarization — baseline review of all apps using automated checks and human review.

(b) App installation sheets providing descriptions of apps and functionality before download.

(c) Authorisation for marketplace developers.

(d) Additional malware protections preventing iOS apps from launching after installation.

[27] Apple announces changes to iOS, Safari and the App Store in the European Union, https://www.apple.com/au/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/#:~:text=The%20changes%20include%20more%20than,DMA%20poses%20to%20EU%20users.

(b) apps targeting children, as features designed to protect children, such as Family Purchase Sharing and Ask to Buy, will not be compatible with apps downloaded from outside of the App Store.[28]

(c) apps that use alternative payment processing, payment scams or fraud, as Apple will not be able to issue refunds, and will have less ability to support customers encountering issues, scams or fraud. Helpful App Store features — like Report a Problem, Family Sharing and Ask to Buy — will also not reflect these transactions.[29]

37. The DMA will thus likely result in compromised privacy, security, and safety outcomes for users and developers, such as:

(a) unvetted marketplaces that offer socially engineered messages to users, including children, to persuade them to permit malicious interference with their devices and data;

(b) a loss of protective features like reviews, which are an important signal to Apple and users to keep data and devices secure;

(c) forged reviews to maximise the chance of download;

(d) a loss of transparency about apps' access to and use of data, which Apple currently provides on the App Store through the requirement that all apps include a Privacy Nutrition Label;

(e) a proliferation of operators with permissive privacy policies that don't highlight their data use and disclosure practices available from marketplaces that either don't enforce privacy guidelines or don't make users aware of their practices;

(f) a proliferation of pornographic or hateful material, with users being socially engineered toward it;

(g) a lack of choice for users who may wish to only download apps from the App Store, but who need to stay in touch with friends via third-party apps, or use certain apps professionally, which are only made available on third-party app marketplaces;

(h) there is an acclimatisation effect – once using third-party marketplaces or third-party distribution becomes ordinary practice, as with web downloading on the Mac, it is much easier to socially engineer an app user to convince them to go to a particular site to access an app. When users are accustomed to going to lots of different places, it is much easier to social engineer them to act against their own interest;

---

[28] Apple announces changes to iOS, Safari and the App Store in the European Union, https://www.apple.com/au/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/#:~:text=The%20changes%20include%20more%20than,DMA%20poses%20to%20EU%20users. This will cause major issues for online safety regulation in Australia if applicable in Australia

[29] Apple announces changes to iOS, Safari and the App Store in the European Union, https://www.apple.com/au/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/#:~:text=The%20changes%20include%20more%20than,DMA%20poses%20to%20EU%20users.

(i) slower response time to threats and other problematic activity regarding an app on third-party marketplace, which gives bad actors the incentive to attempt attacks in the first place.

38. Government agencies, both in the European Union and outside of it, have been quick to recognize the risks created by alternative distribution and the need for protective measures.[30] These agencies—especially those serving essential functions such as defence, banking, and emergency services—have reached out to Apple about the changes that Apple has made as a result of the DMA in the EU, seeking assurances that they will have the ability to prevent government employees from sideloading apps onto government-purchased iPhones. Several have told Apple that they plan to block sideloading on every device they manage.[31]

39. Overall, the changes as a result of the DMA have altered the threat profile for iOS users and increased the risk of attacks. Developers and users who do not use third-party app marketplaces or third-party payment processing may also become vulnerable, even without themselves downloading a malicious app. Whereas before cybercriminals viewed iPhone as an unattractive target because of its integrated approach to platform security and proactive and ongoing monitoring, with easier access to iPhone users through alternative app download channels, the return on cybercriminals' investment increases, making attempts to target iPhone relatively more lucrative overall. This newly incentivized level of criminal investment in building tools, services, and infrastructure to target iOS users risks spilling over and lowering the cost of attacking even those users who only use the App Store or do not download a malicious app. The introduction of these vulnerabilities reduces the security and safety of the platform overall.

40. As the ACCC notes in the Issues Paper, in most cases, legislation has only recently been enacted and the full impact of recent international regulatory developments cannot yet be determined. But even at this early stage it is clear that the DMA has diminished the iOS platform's overall level of safety, privacy, and security even as Apple continues to work to protect those principles to the extent possible within the framework of the DMA.

41. By contrast, it is too early to tell if there have been any pro-competitive benefits from the introduction of the DMA.

DMA: Chilling effect on innovation

42. In previous submissions to the ACCC, Apple forewarned that there is a significant risk that increased regulation will be disproportionate and chill innovation in relevant markets.[32]

---

[30] DMA White Paper, page 15.

[31] These concerns are consistent with the express advice to consumers by Australian cyber security agencies to never sideload and only use official app stores to download apps to their devices: https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-device/secure-your-mobile-phone

[32] Apple submission to DPSI, 1 April 2022, paragraph 7(b)

43. The potential chilling effects of regulation are currently playing out in the DMA context. On 21 June 2024, Apple announced that it will delay launching new AI features, including Apple Intelligence, to EU users because of regulatory uncertainties due to the DMA.[33]

44. Apple Intelligence is a personal intelligence system for iPhone, iPad, and Mac that combines the power of generative AI models with personal context to deliver intelligence that's incredibly useful and relevant.[34]

45. A cornerstone of Apple Intelligence is on-device processing, and many of the models that power it run entirely on device. To run more complex requests that require more processing power, Private Cloud Compute extends the privacy and security of Apple devices into the cloud to unlock even more intelligence. These features set a new standard for privacy in artificial intelligence.

46. However, Apple is concerned that the interoperability requirements of the DMA, if applied to Apple Intelligence, could put user privacy and data security at risk. As a result, Apple Intelligence features will not be made available for users in the EU when the technologies are first rolled out this year.[35]

47. This demonstrates the very real unintended risks posed by introducing regulation that could compromise or constrain the ability of companies like Apple to innovate in a safe and secure manner.

48. Moreover, if Australia introduces ex ante legislation with similar effects as the DMA, this may result in preventing or delaying the implementation of new features by Apple or other companies in Australia due to concerns that its requirements could force companies to compromise their products in ways that harm consumers.

49. Finally, the lack of certainty arising from the "free of charge" interoperability and access obligations will lead to a lack of investment over the medium and longer term by platform operator who will fear free riding by competitors. Ultimately, this lack of investment will be to the detriment of consumers. In setting the parameters of ex ante regulation, Australia should protect IP rights and companies' ability to earn an appropriate rate of return commensurate with the high risks of investment in innovation in the sector. These safeguards will ensure that Australians continue to benefit from the most advanced technological innovation.

The importance of balancing purported pro-competitive benefits of regulation with security concerns

50. Ex ante regulation carries a high risk of regulatory error as it seeks to achieve several very difficult simultaneous objectives, including balancing purported pro-competitive benefits and enabling companies like Apple to continue protecting user security, privacy,

---

[33] Reuters, Apple to delay launch of AI-powered features in Europe, blames EU tech rules, https://www.reuters.com/technology/artificial-intelligence/apple-delay-launch-ai-powered-features-europe-blames-eu-tech-rules-2024-06-21/

[34] Apple, Introducing Apple Intelligence, the personal intelligence system that puts powerful generative models at the core of iPhone, iPad, and Mac, https://www.apple.com/au/newsroom/2024/06/introducing-apple-intelligence-for-iphone-ipad-and-mac/

[35] Reuters, Apple to delay launch of AI-powered features in Europe, blames EU tech rules, https://www.reuters.com/technology/artificial-intelligence/apple-delay-launch-ai-powered-features-europe-blames-eu-tech-rules-2024-06-21/

and safety; enhancing incentives for businesses to develop new technologies; and maintaining and promoting the value of intellectual property in new technologies and not removing "first mover" advantages through product differentiation through innovation.

51. As discussed above, there are early signs that the DMA fails to strike this balance, and may fail to realise the objectives it seeks to achieve.

52. Regulatory reforms recently implemented in some jurisdictions, although in their early days, have been less prescriptive in approach, and have arguably achieved a better balance in the pursuit of the multiple policy objectives. Act on Promotion of Competition for Specified Smartphone Software (**SSCPA**), which was passed in Japan in June 2024 and enters into force in 2025, serves as an example of a recent international regulatory development that seeks to strike a balance between such competing goals and permits service providers to take into account security and privacy as an equally important goal when complying with the obligation to provide access to their systems[36].

53. But it should be emphasized that regulatory reforms in virtually all jurisdictions that have undertaken these efforts are at a very early stage. It cannot yet be ascertained whether they will be able to achieve their policy objectives, while it is already clear is that highly prescriptive regimes which seek to legislate market outcomes by mandating highly detailed specific access to technologies and services—in at least some cases free of charge—have already given rise to serious adverse consequences.

3. Major developments in digital platform markets

54. The ACCC has invited 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. Apple welcomes the opportunity to provide its views.

3.1 Existing competition in app marketplaces remains robust

55. The App Store is a two-sided transaction platform. It exists to facilitate transactions between developers of apps and app users. Apple faces strong competition on both sides of the App Store, and has strong incentives to maximise third-party apps on iOS.[37]

56. Apple differentiates itself and competes on the basis of its continuing commitment to security and privacy policies that protect the value that both consumers and developers derive from the two-sided platform. This has, from the outset, been at the heart of Apple's value proposition to consumers and has significant benefits in relation to consumer protection, privacy, device and data security, and child safety. In addition to forming a core feature of how its products compete, it also supports a vibrant, healthy, competitive market in which small developers have an opportunity to be found by consumers and compete with established developers on a trusted platform.[38]

---

[36] for example, permitting platform operators to take steps to protect the platform and its users so long as those measures are "*necessary for ensuring cybersecurity, protecting privacy, or youth*."

[37] Apple submissions to DPSI, 1 April 2022, [2.1]

[38] Apple submissions to DPSI, 1 April 2022, [13]

57. The pro-competitive effects of the terms by which developers distribute, and users download, apps through Apple's App Store can be observed from the history of the App Store itself:

    (a) Since its introduction, 37.6 million developers have registered with Apple.

    (b) Around 657 million people visit the App Store each week worldwide.

    (c) The number of apps on the App Store has increased from 500 in 2008 to over 1.8 million apps.

    (d) By 2016, developers had earnt USD44 billion from sale of apps on the App Store, increasing to more than USD260 billion by 2022 (i.e. developer revenue increased by USD216 billion in just six years).

    (e) Over what is now some 15 years, the Apple ecosystem and the App Store, have enabled highly rewarding business opportunities for literally millions of developers.

58. Other app transaction platforms compete with Apple's App Store. The close substitutability of rival app transaction platforms is evidenced by the ability of such platforms to expand quicky and easily to serve additional users at low marginal cost.

59. The following platforms are available in Australia, and compete with Apple's App Store:

    (a) PC platforms such as Steam, Microsoft Store and the Mac App Store;

    (b) device-specific platforms for smartphones and tablets such as the App Store, Google Play, Huawei AppGallery and Samsung Galaxy Store;

    (c) console-specific platforms such as the Sony PlayStation Store, the Microsoft Store for Xbox and the Nintendo eShop;

    (d) web browsers accessing publisher-owned stores such as Epic Games, CD projekt and Electronic Arts where transactions occur through the developer's website;

    (e) web browsers accessing indie game stores, e.g. Green Man Gaming, Humble Bumble, Indie Gala, itch.io;

    (f) web portals, e.g. Agame, Big Fish Games and Crazy Games;

    (g) games subscriptions services where games may be downloaded for a monthly price, e.g. Apple Arcade, Netflix Games;

    (h) cloud gaming services, where app users can live stream games via remote servers, such as Xbox Cloud Gaming (XCG), Nvidia GeForce Now, PlayStation Plus Premium and Amazon Luna; and

    (i) social media platforms, e.g. Meta and Twitch.

60. A critical characteristic of app users and developers is that they engage in multi-homing (i.e. they make transactions facilitated by many platforms across a range of devices). Recognition of the prevalence of multihoming and the increased availability from developers of cross platform play, wallet and progression are crucial to the definition of the relevant markets and the associated competition analysis. This further enforces the ability and tendency of app users and developers to substitute transactions across platforms and is evidence of the competition that exists between the aforementioned app marketplace platforms.

61. Developers almost invariably develop apps on multiple platforms. For example:

    (a) in June 2021, 97% of the top 100 downloaded iPhone game apps were also available on Google Play;

    (b) Minecraft, one of the best-selling video games of all time, is available on the App Store, Google Play, Microsoft Store, Amazon Appstore, Nintendo eShop, PlayStation Store and directly from Minecraft's website; and

    (c) Roblox, with 202 million active users in July 2023, is available on the Microsoft Store, App Store, Amazon Appstore, Google Play, PlayStation Store and Quest Store.

62. In the case of app users, they too make use of multiple platforms:

    (a) many iOS users have access to devices with other game app transaction platforms. For example, an Apple survey of iPhone owners in October 2020 found that 46% owned a Mac notebook or desktop, 56% owned a Windows PC laptop or desktop, 25% owned a gaming console and 9% owned a non-iPad tablet. An Apple survey of iPad buyers in June–September 2021 found that 58% owned a Windows PC laptop or desktop, 19% owned a gaming console and 17% owned a non-iPhone smartphone; and

    (b) the ability to transact through a web browser or a game streaming service, as an alternative to transacting within a native app, means that alternative platforms can be available even on the same device (including on an iOS device).

63. The level of competition in app marketplaces summarised above has only grown as technology has improved. A key development in markets for the distribution of apps demonstrating this is the rise of cloud gaming (or game streaming). This is a clear example of firms in a competitive market innovating to win market share against competitors. The existing competition law framework in Australia empowers the ACCC to investigate and bring an enforcement action against parties whose conduct inhibits innovation and competition. To address unlawful conduct, the ACCC is allowed to use an array of existing tools at its disposal (see, e.g., recent ACCC actions against three Australian mobile network carriers in response to an ACCC investigation), or to commence proceedings in court in the same manner as a private litigant (see, e.g., the Epic Games proceedings currently before the Federal Court).

3.2 Innovations in Apple's development and distribution of apps through the App Store is reflective of a highly competitive and dynamic market

64. Apple has invested and continues to invest billions of dollars in the App Store and app distribution to provide developers with the latest tools and technologies to effectively build update their apps. This constant innovation and investment is reflective of a highly competitive and dynamic market.

65. Apple has also modified its rules over time in an effort to offer better terms to developers to attract and retain their business, in the face of existing and potential competitive threats.

66. At the same time as Apple has continued to invest billions in improving its hardware, software and services, offering more and more features to developers such as the current

catalogue of hundreds of thousands of APIs which allow developers to offer an ever increasing array of new features to make their apps even better; over time Apple has allowed more developers to choose to monetise in ways which reduce or avoid altogether paying a commission to Apple, such that in 2024 more than 90% of developers pay no more than 15% commission to Apple. These changes include:

(a) **The reader rule** - in 2011, Apple introduced the reader rule, which removed developers' obligations to pay any commission for app users to access digital content viewed on iOS devices but purchased elsewhere, including for magazines, newspapers, books, audio, music and video.

(b) **Reduced commission on subscriptions** - In 2016, Apple reduced the commission for subscription renewals after the first year to 15%.

(c) **Video Partner Program** - In 2016, Apple formally introduced its Video Partner Program, which reduces the commission for eligible developers from 30% to 15%.

(d) **Multiplatform Rule** - In 2017, Apple introduced the multiplatform rule, which allows users of apps that operate across multiple platforms to access content, subscriptions, or features which were acquired in another platform in their iOS app, provided those items are also available as in-app purchases in the iOS version of the app.

(e) **Small Business Program** - In January 2021 Apple launched the Small Business Program which reduced the commission rate charged to developers to 15% for those developers who earn less than USD1 million in proceeds in the previous year across all apps.

(f) **News Partner Program** - In about August 2021, Apple introduced the News Partner Program, which reduced the commission on subscriptions to 15% (including in the first year) for news publications that provide access to their content in Apple News

67. Apple invests heavily in creating tools and services to enable app developers to provide high-quality apps on iOS. Recent innovations include the creation of new ways for developers to market their apps and content features, enhancements to StoreKit views to give developers more options when building customisation experiences, improvements to StoreKit testing in Xcode and the Apple sandbox environment to help test additional purchase scenarios to ensure they work properly, and expansion of analytics in developers' apps to help them get more insight into their business and apps' performances.

68. Even more recently, starting with iOS 18.1, developers will be able to offer near field communication (NFC) contactless transactions using the Secure Element from within their own apps on iPhone, separate from Apple Pay and Apple Wallet. Using the new NFC and Secure Element APIs, developers will be able to offer in-app contactless transactions for in-store payments, car keys, closed-loop transit, corporate badges,

student IDs, home keys, hotel keys, merchant loyalty and rewards cards, and event tickets, with government IDs to be supported in the future.[39]

69. These changes and innovations, along with countless others, are reflective of the competition that exists between app marketplaces, and within related markets. Apple is constantly innovating to attract and retain both developers and customers. This is also the kind of innovation that could potentially be stymied by unnecessary or ill-conceived ex ante regulation.

3.3 Cloud gaming (or game streaming) is an emerging option for gamers on a range of devices

70. Game streaming services enable users to play games on a device (including a PC, gaming console, smartphone or tablet) that is connected to the internet, without the games in question being installed as apps on the user's device. Processing of the game occurs remotely, on servers accessed by the internet which receive and send signals from the user, with video of the game streamed to the user's device.

71. Apple continues to support cloud streaming on its platform, helping developers to create new cloud gaming apps, and introducing users to cloud gaming's unique benefits. Although a growing segment of gaming, adoption has been relatively slow to date, given technical challenges. As Microsoft has noted, "cloud gaming is small and uncertain to succeed. It is a new and immature technology which faces significant challenges."[40] In order to further promote streaming game services, Apple earlier this year announced new options for streaming games services, offering developers the ability to submit a single app to the App Store from which users can stream all of the games in the developer's catalogue.[41]

72. The offerings available on computer, console and mobile apps, game streaming services and websites have evolved over time and continue to do so. The trend is towards improvements in the performance and popularity of game streaming services through technological improvements in the capabilities of remote servers, continued advancements in internet speeds and reduction in costs as scale increases.

73. The most popular cloud gaming services are:

(a) **Amazon Luna** – available on Windows PCs, Amazon Fire tablets, Chromebooks, as a web app within web browsers on iOS and Android devices, and on certain smart TVs. Amazon Luna offers access to a library of third-party titles (including Fortnite) and titles available through Ubisoft+, Jackbox Games or Amazon's Luna+ catalogue.

(b) **Nvidia GeForce Now** – available on Windows and Mac PCs, Android TV, Shield TV (a streaming device for TVs), Google Chrome, iOS (via a web

---

[39] Apple Newsroom, Developers can soon offer in-app NFC transactions using the Secure Element, https://www.apple.com/newsroom/2024/08/developers-can-soon-offer-in-app-nfc-transactions-using-the-secure-element/

[40] Microsoft's Response to the CMA's Issues Statement on its acquisition of Activision-Blizzard, https://assets.publishing.service.gov.uk/media/637cec9dd3bf7f5a0b33f881/MICROSOFT_S_RESPONSE.pdf

[41] https://developer.apple.com/news/?id=f1v8pyay

browser) and Android. Users can access games that they have previously purchased (such as via Steam or the Epic Games Store) or which are available under a compatible game subscription service (currently Ubisoft+). Nvidia and Microsoft recently announced that some games available via PC Game Pass / Game Pass Ultimate will be streamed on GeForce Now.

(c) **PlayStation Plus** - subscribers to the highest tier of Sony's PlayStation Plus can remotely stream certain games from its library of first-party and third-party titles to their PlayStation 5 console.

(d) **Xbox Cloud Gaming (xCloud)** - subscribers to Microsoft's Game Pass Ultimate subscription tier can stream a wide library of games to their Xbox, Windows PC, iOS device (via a web browser), Android device and certain smart TVs.

74. The recent developments in game streaming demonstrate that the market or markets for app distribution are a continued focus by the gaming industry for innovation and growth. This demonstrates that such markets are both dynamic and competitive, and any market leaders need to consistently innovate to incentivise developers and end-users to transact on their platforms.

4. Identifying potential or emerging issues

75. The ACCC has invited interested parties to:

(a) share their views on potential or emerging competition and consumer issues in relation to online gaming in Australia;

(b) share their views on potential or emerging competition and small business issues in relation to cloud computing in Australia; and

(c) share their views on potential or emerging competition issues in relation to generative AI in Australia.

76. Apple welcomes the opportunity to provide its views. For the reasons set out in more detail below, Apple submits that:

(a) there is no market failure related to online gaming in Australia, and developers have a wide variety of platforms through which to distribute their apps as set out in more detail in section 3.1;

(b) online games may employ manipulative or deceptive design elements, giving rise to consumer concerns. The increasing prevalence of online scams and malware demonstrates the importance of responsible app distribution and thorough review, and platforms that focus on security, privacy and safety;

(c) Apple provides an easy and secure means for iCloud users to transfer a copy of their stored data to other cloud store providers; and

(d) as an emerging technology, it would be premature to introduce ex ante competition regulation targeting generative AI.

4.1 Online games may employ manipulative or deceptive design elements, giving rise to consumer concerns

77. As the ACCC notes in its Issues Paper, online games may employ manipulative or deceptive design elements, giving rise to consumer concerns. A prominent example of such conduct was, as alleged by the Federal Trade Commission (FTC), Epic Games, Inc's (Epic's) use of design tricks known as "*dark patterns*" to charge consumers for items without first obtaining their express informed consent. As a result of the FTC complaint and investigation, Epic paid $245 million USD to the FTC to refund customers, and a further $275 million USD in a settlement to resolve concerns relating to children's privacy in Epic's game, Fortnite.

78. Such tactics are often employed against children and teenagers, who the ACCC notes may be particularly susceptible to such practices given they are often less aware than adults of commercial practices and messaging.

79. This prevalence of such conduct demonstrates the importance of thorough App Review, fraud detection tools and other features like Parental Control.

(a) **App Review** - Apple's App Review process works through a combination of automated scanning and human review, with the human review assisted by automated tools to facilitate the review process. It is a multi-stage process that seeks to ensure that all apps made available on the App Store comply with Apple's published technical, content and design criteria, as well as the terms of Apple's DPLA. Apple's mission in its app review process is to hold apps to clear, published, and high standards for privacy, security, and safety, to assure iOS Device users that they can expect to go to the App Store and get safe and trusted Apps whose content and software have been reviewed.

(b) **Parental Controls** - Apple's Parental Controls are important tools that allow parents to choose how — and how often — their children can use their devices. Parental controls are built right into each iPhone, iPad and Mac. Parental Controls can be used to prevent App Store purchases and prevent children being exposed to explicit content.[42]

(c) **Fraud detection tools, and other features of IAP** - Apple's IAP has functionality that includes fraud detection tools, verification of delivery of goods, and refund processing for accidental or unwanted purchases. From 2020 through 2023, Apple prevented a combined total of over $7 billion in potentially fraudulent transactions.[43]

80. These features rely on Apple's centralized app distribution method. In the EU under the DMA, apps that are distributed through third-party channels on iOS are not subject to Apple's App Review. This is problematic when low quality app marketplaces like itch.io are known to distribute games with graphic violence, blood and gore; murder; sexual assault and implied child neglect. For example, itch.io distributes games such as "baby shooter" and "Isis Hunter" that have been banned in three countries.

---

[42] https://support.apple.com/en-au/105121

[43] https://developer.apple.com/in-app-purchase/

81. Furthermore, if developers can avoid using Apple's IAP, and instead engage a separate service provider to process in-app transactions, a user's security cannot be guaranteed and their experience in acquiring in-app digital content is fundamentally altered. The content acquired will no longer form part of the user's centralised repository of content to be managed, including through family sharing and ask-to-buy Parental Controls. Apple will no longer be able to address user's complaints, requests for support, or requests for a refund.

82. The prevalence of manipulative or deceptive design elements that can be employed in apps, and more generally the prevalence of malware, demonstrates the importances of the security features employed by Apple. As noted in these submissions, such features could be undermined by prescriptive ex ante regulations.

4.2 Apple provides an easy and secure means for iCloud users to transfer a copy of their stored data to another cloud storage provider

83. In its September 2023 report, the ACCC examined consumer cloud storage as an example of the expanding ecosystems of digital platforms. Given this past focus, the ACCC states in the Issues Paper that it does not intend to revisit consumer cloud storage as part of the current chapter of the Inquiry.

84. Apple notes that it provides an easy and secure means for iCloud users to transfer a copy of their stored data to another cloud store provider in just four steps:

    (a) sign in with Apple ID at privacy.apple.com, and complete two-factor authentication;

    (b) select Request to transfer a copy of your data;

    (c) to start the transfer, sign in with incoming provider login details (for example, sign in to Google Account to transfer to Google Photos); and

    (d) to finish the request, follow the on-screen instructions.[44]

85. The transfer process takes between three and seven days, so that Apple can appropriately verify that the request was made by the user, and to make the transfer.[45]

86. Third-party cloud storage providers also offer resources to facilitate consumer switching and data migration from one provider to another. There are also a number of third-party migration tools for consumer and business / enterprise - including free services - to further assist users.[46]

4.3 Ex ante economic regulation targeting generative AI would be premature

87. As the ACCC notes in its Issues Paper, recent developments in, and adoption of, generative AI have been extensive, and this technology continues to expand and develop at a rapid pace.

---

[44] Apple submissions to DPSI, 14 April 2023 [54]

[45] Apple submissions to DPSI, 14 April 2023 [55]

[46] Apple submissions to DPSI, 14 April 2023 [56]

88. Generative AI is an emerging technology, and it would be premature to introduce targeted ex ante economic regulation at this stage, when no specific harms have been identified.

89. Any such regulation, at this stage, could have the effect of chilling further innovation in this field. An explicit example of this is the chilling effect attributable to the DMA, which has delayed the rollout of Apple Intelligence in the EU. Any targeted regulation directed at addressing hypothetical (rather than existing) competition concerns in relation to generative AI would run the risk of causing a similar chilling effect on innovation and development.

90. There is no objective credible evidence that there is a relevant market failure arising from any firm's market power in relation to generative AI which would require a regulatory response directed specifically to target this emerging technology. Accordingly, Apple submits that existing competition law in Australia is effective to address any competition concerns relating to generative AI, as or when they arise.

91. To the extent that the ACCC is concerned about companies with dominant market positions acquiring start-up companies providing generative AI technology, the new mandatory merger control regime that will come into effect on 1 January 2026, which includes targeted mandatory notification thresholds and targets serial / creeping acquisitions, should be sufficient to address any competition concerns of this nature.

5. Conclusion

Ex ante regulation of digital platforms seeks to achieve a number of complex and potentially competing policy objectives which appropriately balance the interests of all participants in the sector.

It is exceedingly difficult for any ex ante regime to simultaneously:

- address alleged market power of platforms
- encourage competition between platforms and with business users who want to compete with the platforms
- maintain user security and privacy
- protect consumers from bad actors, whose entire purpose in seeking access to the platform is to exploit consumers
- ensure that innovation is encouraged and not chilled or delayed; and
- protect, and permit an appropriate return on, intellectual property rights.

The ex-ante approach the legislature has adopted in Europe has given rise to substantial complaints, investigations and disputes about whether and what services ought be subject of access; whether the terms of access offered by platforms are compliant with the regulations; whether the platforms' compliance with consumer protection exceptions within the regulations is correct; whether pricing terms are compliant. It is highly unlikely that a resolution of these issues will be achieved in the short or even medium term.

Moreover, there are early signs that certain platform services in EU and the introduction of the latest technologies are being curtailed by platform operators because of compliance concerns and that security of consumers is being compromised.

Apple would welcome a discussion with Commission staff about the risks of regulatory error which can arise from an ex ante regime which seeks to intervene in a highly

innovative sector and determine market outcomes which are emerging in some jurisdictions which have adopted that approach. Because the adverse consequences of which are potentially significant, so that Australia, in designing an optimal regime, can benefit from the initial learnings once enough time has passed to better-understand those consequences.