



Confidential

Government consultation on ACCC's regulatory reform recommendations – Submission by Apple Pty Ltd in response to Consultation Paper

Apple Pty Limited (**Apple**) welcomes the opportunity to comment on the matters raised in the consultation paper published by Treasury on 22 December 2022 (**Consultation Paper**) in relation to the recommendations made by the Australian Competition and Consumer Commission (**ACCC**) in its fifth interim report in the ACCC's Digital Platform Services Inquiry (**DPSI**) published on 11 November 2022 (**DPSI Report**).

A. Executive summary

1. As Treasury is aware, the list of competition and consumer issues the ACCC has identified in its DPSI Report include:
 - (a) the large volumes of unique, highly sensitive and personal individual-level user data that is collected and controlled by digital platforms, and the way in which this information is used (including the monetisation of users' personal information by certain platforms);
 - (b) a significant and sustained prevalence of scam activity on certain digital platforms, including harmful apps (such as malware), and fake reviews, which mislead consumers, distort competition, reduce trust in platforms, and harm businesses;
 - (c) substitutability between app marketplaces, and the ability of app developers to bypass a particular app marketplace;
 - (d) terms, conditions and fees imposed on businesses to place apps (including in-app purchases (**IAP**)) on app marketplaces and the effect of these on an app's commercial viability;
 - (e) the effect of app marketplace providers competing downstream with app developers for the distribution of apps to consumers, and whether this creates the ability and/or incentive for app marketplaces to foreclose competing developers' apps (for example, by 'self preferencing' marketplace platforms' own apps); and
 - (f) the process for determining whether apps are permitted on an app marketplace and whether this could negatively affect developers' ability to reach consumers with their apps.
2. Apple is concerned that much of the DPSI Report proceeds on the assumption that *ex ante* regulation targeted at specific designated market participants in relation to competition aspects of app marketplaces is necessary to address hypothetical future competition concerns. Apple disagrees that the current provisions of the Australian competition law cannot adequately address any concerns which might arise.
3. Insofar as **Apple's products and services** are concerned, there is no objective credible evidence that there is a relevant market failure arising from Apple's purported market power which requires a regulatory response directed specifically at Apple by designating Apple as a digital platform to which *ex ante* regulation should apply simply on the basis of the popularity of its products.



4. The available objective credible evidence is to the contrary: app marketplaces, even the mobile segment alone, have over time since 2008 (when the App Store launched in Australia) been consistently characterised by massively higher output (increasing from a few hundred to millions of apps and billions of app downloads per annum), decreasing prices to developers (that is, lower commissions, with zero commission on more than 80% of apps), no charges levied on consumers by the platform operator, and with the most popular and successful apps in every genre originating from third party developers, not Apple.
5. These characteristics are indicia of dynamic, healthy, competitive markets and it is only through constant innovation and improvement year on year that Apple products and services can remain popular within the ferociously competitive global markets in which Apple offers its products and services.
6. The reforms canvassed by the ACCC in the DPSI Report are based on a fundamental misconception as to the different business models, incentives, user experiences and characteristics falling within the umbrella term “digital platform services”. For example, the concerns identified in the DPSI Report with respect to data protection, privacy and security, as well as scams and harmful apps, are well-founded insofar as data-driven businesses which sell their customers’ to advertisers are concerned.
7. But Apple’s business is not dependent on the commercialisation of user data. Privacy is embedded in the DNA of Apple’s products and the App Review process. Apple believes privacy is a fundamental right, and privacy has long been an integral part of Apple’s brand.
8. For the reasons set out in this submission, Apple does not agree that there is a market failure that requires entity-specific *ex ante* regulatory intervention or legal action directed at Apple to address.
9. Apple has serious concerns about the implementation of the regulatory reforms proposed by the ACCC in the DPSI Report in circumstances where:
 - (a) those reforms are directed at addressing hypothetical (rather than existing) problems insofar as conduct attributable to Apple is concerned;
 - (b) it is not clear why the existing competition and consumer law regulatory framework is insufficient to address the issues of concern identified in the DPSI Report, to the extent that those issues might in fact materialise in the future;
 - (c) the real-world market outcomes which will result from many of the proposed “reforms”, if they are implemented in the form proposed, would reduce incentives for dynamic firms like Apple to innovate and develop new and differentiated products, and would force Apple to redesign its products (including the iPhone) in a manner which would ultimately benefit only:
 - (i) a handful of powerful developers whose primary goal is to remove the highly effective security, privacy, scam and content protections for consumers that Apple has built from its experience into its integrated platform; and
 - (ii) expose consumer, business and government users of Apple devices and services to the far less secure and private environment found on the web and to a lesser extent Android devices in which scams and malware proliferate daily.

The weakening of Apple’s integrated security, privacy, scam and content control will result in significant consumer detriment – not only in the form of a reduction in



consumer choice as a result of the homogenisation of competing digital platform business models and product offerings, but also a reduction in key protections for consumers to which they entrust their personal and financial data. It would also be contrary to recent reforms to Australian data protection laws, which have sought to strengthen, not weaken, the privacy protections afforded to Australian consumers.¹ The recent spate of sophisticated and large-scale cyberattacks which have affected millions of Australian consumers demonstrate that these concerns are not academic or trivial;²

- (d) as Treasury has acknowledged, “[n]o platform specific regulatory approach has been established for a significantly long enough period to provide a proven regulatory template to draw on”; and
 - (e) contrary to the analogies drawn by the ACCC to other sector-specific regulation in the context of essential infrastructure, the reforms canvassed in the DPSI Report would be unprecedented in the Australian economy. Australia is currently in a unique position in which it can “leverage international regulatory approaches and industry undertakings overseas as they are developed, better aligning Australia with larger markets and benefiting from the rules implemented in other jurisdictions”.
10. Apple is concerned that the recommendations in the DPSI Report prioritise purported competition concerns which lack cogent evidence of harm, over clear and present severe damage to users that they experience every day. That is not what consumers want to see as outcomes of legislative reform - they want stronger, not weaker, protection - from the unlawful conduct which affects the hundreds of thousands of Australians every year whose information is stolen, scammed, traded and exploited to their detriment.
11. Apple has intentionally designed its products to ensure that its products are simple, private and secure for users. The regulatory interventions proposed in the DPSI Report would fundamentally change the iPhone and related Apple services (including iOS and the App Store) in what are already vigorously competitive and dynamic markets, and would have substantial implications for consumers, including in terms of Apple’s industry-leading privacy and security standards. They would also reallocate the distribution of benefits of the app economy from the broadest set of developers to a small set of successful incumbents.
12. It is well established that interventions under competition policy can improve competition on a range of indicators - but can equally have detrimental effects on consumer protection.³ The reform proposals in the DPSI Report fail to grapple with this fundamental tension in competition and consumer protection policy. The proposed reforms, if made law so as to apply to Apple products and services as proposed, therefore fail their key test: Australian consumers will be net worse off.
13. For the reasons set out in this submission, Apple considers that the current regulatory regime in Australia is sufficient to address issues unique to digital platforms, particularly in

¹ See *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022*.

² ‘Hacks expose Australia as years behind on cybersecurity’ *The Sydney Morning Herald* (online, 10 November 2022) <https://www.smh.com.au/technology/hacks-expose-australia-as-years-behind-on-cybersecurity-20221110-p5bx9n.html>; Josh Taylor, ‘Medibank reveals hack could affect all of its 3.9 million customers’, *The Guardian* (online, 25 October 2022) <https://www.theguardian.com/australia-news/2022/oct/25/medibank-reveals-hack-has-affected-more-customers-than-first-thought>; -

Leigh Tonkin, ‘Optus’s week of hell: How nine days of confusion left 9.4 million Australians waiting for answers’, *ABC News* (online, 1 October 2022) <https://www.abc.net.au/news/2022-10-01/optus-data-hack-australians-waiting/101486874>; Sam McKeith, ‘Australia’s Telstra suffers privacy breach, 132,000 customers impacted’, *Reuters* (online, 13 December 2022) <https://www.reuters.com/technology/australias-telstra-suffers-privacy-breach-132000-customers-impacted-2022-12-11/>.

³ See eg Louise Sylvan, ‘Activating competition: The consumer – competition interface’ (2004) 12 *Competition and Consumer Law Journal* 191, 198; Max Huffman, ‘Bridging the divide? Theories for integrating competition law and consumer protection’ (2010) 6(1) *European Competition Journal* 7.



circumstances where the ACCC has not sufficiently identified a relevant market failure arising from Apple's purported conduct. Specifically, Apple submits that:

- (a) **a sweeping, "one size fits all" approach to regulation is inappropriate and poses a substantial risk of type I ('false positive') regulatory error** given the dynamic and rapidly advancing nature of the various markets in which digital platforms operate.⁴

As the DPSI Report acknowledges, the broad conduct attributed to "digital platforms" and "digital platform services" by the ACCC can take different forms and have different competitive and consumer welfare effects when conducted by different types of digital platforms and for different services and consumer groups. The ACCC also recognises that there are legitimate justifications and efficiency-enhancing effects for given conduct (eg, promoting efficiency or addressing security or privacy concerns) in different platform contexts.

Sector-wide regulation poses a significant risk of chilling these procompetitive and welfare enhancing effects, and should be discounted as fundamentally inconsistent with the underlying goal of Australia's fair trading laws to enhance the welfare of Australians,⁵ and to promote economic efficiency, thereby promoting effective competition in upstream and downstream markets.⁶ Although the ACCC proposes 'service-specific' regulatory schemes, including by way of mandatory codes of conduct for single digital platform services, such an approach would fail to take account of the stark differences in the business models and user experience between different platforms offering the same ostensible service (for example, the competing app stores operated by Apple and Google).

The ACCC proposes that quantitative (e.g, number of monthly active Australian users, or revenue) and/or qualitative ("*whether [a platform] has substantial market power*") criteria be used to 'designate' a digital platform service for the purpose of a mandatory industry code.⁷ Insofar as quantitative metrics are concerned, the effect of the proposed scheme would be to subject digital platform services to additional regulatory burden simply as a result of their success and popularity with consumers – thereby disincentivising innovation, growth and the development of products which meet consumer needs and preferences. It ignores the fact that even small companies can wield enormous market power. It also ignores the well-established principle that the mere possession of market power is not, of itself, detrimental to competition. Rather, the *misuse* of market power (or 'abuse of dominance') has the potential to cause anticompetitive harm under certain market conditions and competitive dynamics. The assessment of whether a platform service should be subject to 'designation' must therefore be undertaken on a case-by-case basis having regard to the facts and market dynamics in issue. An indiscriminate approach which punishes successful platforms risks chilling the efficient use of, and investment in, the digital economy.

Insofar as qualitative criteria are concerned, the application of *ex ante* 'designation' criteria for digital infrastructure providers is liable to give rise to substantial disputation, which creates further uncertainty and disincentives to investment (for example, the subjective determination of whether a digital platform has "substantial market power"). These concerns are particularly acute in the context of dynamic, innovate digital platform services, and the significant uncertainty that the implementation and enforcement of blanket obligations (such as a general

⁴ See further Consultation Paper Q11.

⁵ *Competition and Consumer Act 2010* (Cth) (CCA) s 2.

⁶ See eg CCA s 44AA.

⁷ DPSI Report, p 114.



prohibition on “anti-competitive self-preferencing” or “tying”) will create. As Treasury has acknowledged, “[a]n important risk to manage is how to achieve sufficient regulatory certainty and timeliness of the designation process (which might suggest prescriptive quantitative designation criteria) while retaining the flexibility to accurately target the right entities (which would require some qualitative assessment and discretion by the decision maker)”;⁸

- (b) there is a significant risk that **the proposals will be disproportionate and chill innovation** in the relevant markets. Clearly, the more intrusive the remedy being considered and the wider the effect that the remedy could have, the stronger the evidence base underpinning the need for the remedy must be. The evidence base justifying regulatory intervention set out in the DPSI Report is scant.

Further, Apple’s ecosystem operates on a centrally-run, worldwide basis. Unique regulation imposed in Australia could potentially require that Apple restrict its product and service offering as available to Australian consumers, with the result that Australian consumers could receive a lower quality offering relative to other markets. Again, the potential for remedies to have such wide-ranging effects indicates that a particularly strong evidence of market failure is required - which to-date has been wanting; and

- (c) **the ACCC’s proposals run the risk of sacrificing user security and privacy, leading to net consumer welfare detriments.** It is a key driver for Apple - and always has been - to ensure that users’ data and information is private and secure and that consumers only share what they want to share when they wish to share it. It is essential to Apple’s business that users are confident when using Apple’s products that they are not being subject to poor data practices. Apple has serious concerns that some of the measures proposed in the DPSI Report - in particular, mandatory access for third-parties to Apple hardware and software - will significantly undermine users’ privacy and security, and Apple’s integrated and carefully-designed efforts to protect these. Moreover, as the ACCC concluded in its earlier report regarding app marketplaces,⁹ immediate and severe consumer harm is occurring by reason of scams directed at consumers, yet the ACCC’s proposals run the risks of increasing this risk.

14. Apple submits that any response to the ACCC’s recommendations in its DPSI Report cannot rely on hypothetical considerations to the exclusion of positive evidence submitted by Apple, app developers and other interested parties. Apple urges the Treasury to undertake a more fulsome analysis of the benefits that Apple’s ecosystem brings to both consumers and developers, and to consider objectively the ramifications of any proposed interventions on consumers and competition in the various markets that would be affected by the regulatory proposals in the DPSI Report were they applied to a digital platform such as the Apple App Store without assessing the net overall consumer benefit question.

15. If Treasury ultimately considers that regulatory reform is necessary to address a perceived market failure (a position with which Apple does not agree), it would be important to ensure that any such measures – for example, the making and enforcement of industry codes canvassed by the ACCC – are subject to appropriate regulatory oversight so as to minimise in particular the risk of type I error. Specifically, the process of ‘designation’ should be subject to objective qualifying criteria and merits review of a designation decision in accordance with those criteria to safeguard the quality and consistency of designation decisions and ensure that such a decision is warranted in each case - and designation decisions should be

⁸ Consultation Paper p 10.

⁹ ACCC, DPSI Interim Report No. 3 - App Marketplaces (March 2021), [6.2.3].



determined (and reviewed) by a specialist and impartial body separate to the ACCC as the body responsible for enforcement.

16. Apple does not propose to provide feedback in response to all of the questions raised in the Consultation Paper.¹⁰ For the avoidance of doubt, where Apple has not addressed a specific question or topic in the Consultation Paper, Apple should not be taken to agree with or acquiesce to the proposals canvassed or views expressed in the Discussion Paper. However, if Treasury has any specific questions to ask Apple in relation to any topics it has not addressed in this submission, Apple would be happy to assist.

B. No basis for any requirement that Apple provide “increased access” to iPhone hardware or iOS¹¹

17. The DPSI Report expresses a concern that digital platform service providers are engaging in self-preferencing conduct which can distort competition and decrease consumer welfare, or restricting interoperability of service outside a platform's ecosystem. To the extent that these concerns relate to Apple, they are misconceived.
18. As a preliminary matter, Apple notes that it makes technologies available to third-party developers including software tools which safely interact with device features - and has a strong track record of doing so. It is in Apple's interests to do so, as the greater the range of high-quality apps available on the App Store, the more attractive the overall iPhone experience will be for users and the better it is able to compete against other devices. Apple's platforms are not 'essential facilities' or otherwise analogous to natural monopoly (or bottleneck) infrastructure assets. The DPSI Report fails to take into account the two-sided nature of app marketplaces and the fact that the availability of a broad selection of innovative and popular apps helps Apple sell iPhones. Apple has strong incentives to, and does, provide access to app developers to features and functionality within the device – such as the camera, sensors or GPS technology – as these apps then serve to improve the quality and experience of Apple's mobile ecosystem.
19. There can be no suggestion that Apple is withholding or limiting access to its products and services (including device hardware) for developers. Apple has invested significant engineering time and resources to make more developer tools such as APIs available to third-party developers, and each year Apple has opened more and more APIs to developers. Today, there are more than 150,000 APIs available to developers, and that number continues to grow. This is clear evidence of Apple fostering competition by developers, rather than restricting or distorting it.
20. Developers have benefitted enormously from Apple's approach and provision of access to Apple's investments in R&I. Apple has made it easy for developers to create applications using Apple's proprietary technologies and intellectual property. And Apple has made it easy for developers to access customers around the world. Apple gives developers access to customers in 175 countries worldwide, with consistent rules, pricing and guidance across the globe, reducing costs and making it easier for developers to succeed across borders and to enter new markets.
21. The assumption underlying the ACCC's concerns (that Apple would want to disadvantage third-party apps) is flawed. Apple's incentives are driven by its overall business model, which remains that of selling mobile devices; the more attractive the device, the greater Apple's sales. Apple does not sell its consumers' personal information to advertisers or others. Apple generates the vast majority of its revenue from the sale of products like the iPhone and iPad.

¹⁰ For ease of reference, this submission includes footnote references to the relevant questions in the Consultation Paper.

¹¹ See generally Consultation Paper Q7.



A greater choice of features and functionality that users desire is key to ensuring the attractiveness of Apple's devices.

22. Apple wants developers to create applications using the new technologies and innovations it introduces with every new device generation. Apple's incentives are reflected by the fact that Apple is constantly investing in its developer community by providing new tools, more flexible monetisation rules and other benefits for developers. Apple must compete, and innovate, to ensure that developers focus on developing innovative features for their iOS apps so that they are available on a timely basis and the iPhone maintains its reputation as delivering cutting edge performance. The DPSI Report ignores Apple's incentives to ensure that it can offer a broad selection of innovative and high-quality apps on the App Store.
23. By way of example, whilst Safari is pre-installed on iOS devices in order to provide a seamless out-of-the-box experience for users (who expect to be able to immediately access the internet when they power on their Apple device with minimal set-up), Apple does not restrict users' ability to download and use alternative browser apps:
 - (a) on iOS devices, users in Australia can choose among a variety of other mobile browsers available on the App Store, including Firefox, Firefox Focus, DuckDuckGo, Google Chrome, Microsoft Edge, Brave, Aloha, Cake, Opera Touch, DuckDuckGo Privacy Browser, and Dolphin. Additionally, Bing Search, Yahoo Search, Ecosia, Quant, Start Page, and Google Search are all search-enabled apps that allow users to browse the web; and
 - (b) further, Apple devices enable users to quickly change their default browser to the browser of their choice, and some web browser apps, including the DuckDuckGo browser, prompt users to switch their default browser when a user opens the app. Since the introduction of the App Store, Australian users have downloaded alternative browser apps or search-enabled apps millions of times on Apple mobile devices.
24. More fundamentally, if Apple were engaged in "self-preferencing" behaviour of the kind described in the DPSI Report, and if Apple had the market power alleged, one would observe over time a strengthening effect in the market position of Apple's apps that compete with third party apps. This is simply not happening, with competing apps from well-established players such as Microsoft, Hulu, Spotify, PayPal, Amazon, Skype, Google, and Meta often having a much greater share of the market in those downstream app categories than equivalent Apple apps.
25. It cannot be seriously argued that Apple must grant the same level of access to third-parties as it does to its own integrated apps, and at the same time. Apple must be careful when providing access to software technologies to ensure that the security, safety, quality, device performance, and integrity of the user experience is not compromised. This takes time to develop, refine, and test. It takes time to develop public APIs before being released because, once released, third party developers rely on the underlying functionality of the APIs always being there to power their own apps. And there are some technologies that Apple does not make available to third-party developers if doing so would compromise the security, safety or privacy of Apple's users.
26. Apple seeks to ensure that apps are held to a high standard for privacy and security, because nothing is more important to Apple than maintaining the trust of its users. Consumers expect devices that work seamlessly right out-of-the-box. Apps must both work and be integrated with the Apple devices upon which they will be used.
27. To achieve this, Apple has reviewed apps since the opening of the App Store in 2008. Apple has expended significant effort to put in safeguards which allow the company to detect and



stop harmful third-party apps. The primary safeguard is that when developers submit their applications, Apple ensures that the app is not doing things it shouldn't be doing. There are going to be some apps - such as apps containing pornography, malware and apps that invade user privacy - to which Apple will reasonably say no.

28. To ensure apps available on Apple's devices meet these standards, the App Store, like all stores, has rules: namely, the App Store Review Guidelines (**Guidelines**). Apple publishes these Guidelines transparently for all to see.
- (a) The Guidelines provide transparency to developers and users, ensuring that apps do what they say they will do. This makes the App Store a safe and trusted place for consumers to discover and download apps.
 - (b) The Guidelines apply equally to everyone—including Apple's own apps that are on the App Store.
 - (c) Because Apple develops both the hardware and software for its devices, distribution through the App Store allows Apple to take full responsibility for the user experience.
 - (d) Apple's products, like the iPhone and iPad, could offer access to a trove of users' personal data—data which unscrupulous actors could seek to collect or exploit. Apple's rigorous App Review Process is designed to protect users of Apple's devices from malware and security threats.

C. Many of the proposed reforms place consumer welfare (including privacy and security) at substantial risk and will result in net public detriments¹²

29. Regulators and policymakers should review the contrasting choices made by large digital platforms that affect Australian user privacy, security and choice. On such a review, it is clear that the proposals set out in the DPSI Report are too blunt a tool. In particular, the ACCC proposes to equate size with harm, and then recommends a one-list-fits-all set of regulatory obligations without providing an opportunity for the platform to explain, and the regulator to assess, whether – on balance – there are broader benefits to consumers or businesses.
30. The ACCC's proposals should provide a mechanism for individual platforms to explain and objectively justify different business models and certain practices. They should also provide for decision makers to explicitly consider a set of holistic and consistent policy considerations – ones that assess the evidence of actual harm and the countervailing benefits of the practices a platform seeks to maintain.
31. Specifically, Apple's human-led App Review process is an integral part of Apple's multi-layered approach to security. App Review carries out a comprehensive check of every app and app update before it is made available for download, providing a critical layer of security through a mix of human review and automated processes. App Review applies the App Store Review Guidelines which helps to ensure that the apps on the App Store are safe, provide a good user experience, comply with Apple's privacy rules, secure devices from malware and threats, and use approved business models. When users download an app from the App Store, they can trust that the app will:
- (a) work properly;
 - (b) not compromise the functionality of their device; and

¹² See generally Consultation Paper Q4, Q7-Q8, Q13-Q16.



- (c) not engage in forms of program abuse that harm customers, such as tricking users in to purchasing subscriptions, engaging in bait-and-switch tactics to evade human review, or impersonating other apps.
32. To the extent that there are differences in access to Apple’s proprietary technologies between third-party apps and Apple services, such differences are objectively justified by the need to ensure the safety and performance of Apple devices and the privacy and security of users. Any requirement that, for example, Apple give "*comparable access to device hardware or operating system features as [its] first-party apps*" would undermine Apple’s rigorous privacy and security controls (including App Review) and result in net consumer welfare detriments.
33. The Android iOS provides a real-world illustration of the counterfactual. In 2021, the iPhone platform accounted for just 1.72% of malware infections globally. By contrast, Android accounted for 27% and Windows/PC accounted for 39%, according to the 2021 Nokia Threat Intelligence Report:
34. The regulatory interventions canvassed in the DPSI Report are ill-founded and premature, given the absence of any evidence demonstrating real competitive harm insofar as Apple is concerned. With respect to the App Store, this is particular concern given the draconian nature of the interventions proposed, including the possibility that Apple could be required to provide full access to iPhone hardware or iOS features to all third-party apps within the App Store – to the detriment of the secure ecosystem which Apple has developed to protect users’ privacy and personal information.
35. Apple has built a reputation for quality products that also protect user security and privacy both through the operation of the App Store – which is designed to ensure that apps meet Apple’s standards, add value to users, and safeguard users’ privacy and security – and through the creation of high-quality devices that contain built-in privacy features and software.
36. Apple’s commitment to data privacy and security has always been one of Apple’s core principles. Apple has a decade-long track record of designing privacy protections into its products. Data privacy and security are fundamental pillars of the App Store and are crucial elements of its success. Consumers trust that Apple will equip them with tools to control the data they share with apps, and that Apple continuously seeks to improve the App Store’s user privacy and security features to confront novel privacy and security risk.
37. Apple’s multi-layer approach to security is designed around its “walled garden”, of which a single App Store is a key element. Replacing Apple’s robust systems of App Review and quality control with a blanket obligation to provide access to hardware and iOS features to third-parties would in no way be sufficient to match the protection offered by Apple’s current approach. This is obvious from the fact that Android, which does rely on lesser protections, has a significantly poorer track record on preventing malware. Similarly, Apple’s built-in privacy protections, such as App Tracking Transparency, would be rendered ineffective by such remedies, as apps could access device or user data and collect or share this without the user’s permission.
38. On the other hand, the incentives of individual developers are *not* aligned with Apple’s (and ultimately consumers’) in the same way: a developer cares for its own app, not for the App Store, and not for the impact that the App Store experience has on the performance, functionality or sale of Apple devices. A developer can inflict negative externalities on the App Store (and the ecosystem) which it does not “internalise” (in practice, a “bad” experience with an app damages the App Store more broadly and potentially other apps too, if the consumer decides to “switch away”, but the developer of that particular app does not care about these externalities). Apple, on the other hand, has designed its business model to internalise the complementarities across its products and services, and directly takes into account that users



benefit from a vibrant app ecosystem and that a larger user base on iOS in turn is attractive for app developers.

39. The increased risk of malware attacks that would result from mandating unfettered access to hardware or software features would put all users at greater risk. The App Store is designed to detect and block today's attacks, but changing the threat model would bypass these protections from more sophisticated attacks. Scammers would then use their newly developed tools and expertise to target third party stores as well as the App Store, which would put all users at greater risk, even those who only download apps on the App Store. Further, malware would not just impact the entry point app. For example, it could seriously undermine the functioning of other apps because effects such as excessive battery use or invasive data collection interfere with apps already downloaded.
40. Potentially even more seriously, malware introduced into a device can be used as a stepping stone to getting access to other devices or systems to which that device connects. Individual mobile devices are recognised as a common entry point to deploy network-wide attacks in enterprise settings. Moreover, with access to personal information from a user's device, attackers are well positioned to launch attacks on a user's friends and family.
41. The DPSI Report's proposed regulatory interventions risk not only failing to meet their stated aim of increasing competition and consumer choice, but actively reducing the existing choice available to consumers and exposing consumers and their families to substantial greater privacy risk. In addition, it would be patently unreasonable to impose regulation which removes the existing necessary security and privacy protections available on the assumption that Apple could be expected to find alternative safeguards to replace them. Not only is it clear that the integral and embedded nature of the existing protections cannot be fully replicated, but such a requirement would force Apple to completely re-architect its systems and spend potentially vast amounts of resources developing security solutions that would, of necessity, be likely less effective than those it already offers users.

D. Existing competition in app marketplaces is sufficient to constrain any purported exercise of market power by Apple¹³

Apple faces strong competition on both sides of the app marketplace, and has strong incentives to maximise third-party apps on iOS

42. The ACCC considers that the "*market power of some large digital platforms is substantial and enduring*" (relevantly, in the case of Apple, "*in the supply of mobile [operating services] and likely significant market power in mobile app distribution*").¹⁴ This conclusion is based on the ACCC's assessment that "*app developers can only offer apps through the Apple App Store*", and that "*[a]ny competitive constraint provided by other app marketplaces (such as the Google Play Store) is limited once a user is within the Apple ecosystem*".¹⁵
43. These conclusions are unfounded. There is no evidence which suggests that Apple has market power in that it has an ability to act persistently in a manner materially different from the behaviour that would be observed for a firm in a "workably competitive" market. For example, Apple has no ability to restrict entry or significant expansion by rivals nor insulate itself from constraints from competition from rivals. On the contrary, Apple must engage in constant rapid innovation to remain a relevant choice for consumers or be left behind in hardware, software and services.

¹³ See generally Consultation Paper Q1, Q7.

¹⁴ DPSI Report, p 36.

¹⁵ ACCC, DPSI Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services (February 2022) p 20 (**February 2022 Discussion Paper**).



44. The first iPhone launched in the United States in 2007 had no App Store (that is, there was no third-party native software development for the first iPhone). Apple was very concerned that third-party development could undermine the security and integrity of the device. The immediate success of the iPhone, and the power of its computing platform, led to calls in the developer community for the ability to create third-party native applications. Apple ultimately made the decision to open the iPhone to third-party development, but it did so deliberately and carefully with the interests of users fully in mind.
45. The App Store (which has always been available on iPhones sold in Australia) revolutionised the distribution of software and led to the emergence of hundreds of thousands of new software developers. The App Store reduced barriers to entry for developers and provided developers with the potential for broader distribution and access to a worldwide audience.
46. Twelve years ago, before the App Store, only a handful of the very biggest developers could reach such an audience. Software development and distribution was once limited to a handful of large, well-resourced companies, with high barriers to entry. Around 50-70% of software sales revenues were retained by retailers under this distribution model.
47. Apple has continuously sought to make the iOS platform more attractive for users and developers alike by improving quality, innovation, security, privacy, user experience, as well as commission levels, all in active comparison to other platforms. The principle driving that innovation and improvement has been, and continues to be, competition to offer the best platform in competition with the alternatives available on iOS devices themselves (eg, web-based apps) and with the alternative platforms on the other devices they own and use every day.
48. Today, millions of developers, large and small, have the opportunity to reach a global audience and build a business with very little cost. An entire industry has been built around app design and development since 2008 - creating competition and economic opportunity. As explained further at paragraphs 59 and 61 below, over 84% of apps on the App Store do not share any of the revenue they make from the App Store with Apple.¹⁶
49. Apple's fully integrated devices face strong competition from multiple Android original equipment manufacturers, both in relation to price and device features. In recent years, new entrants to the premium smartphone market have increasingly challenged Apple. Besides Samsung and Huawei, other Android smartphone manufacturers including Motorola, Oppo, Vivo, Xiaomi, Google, LG and others have rapidly penetrated the Australian and global smartphone markets, including with high-end devices.
50. Customer switching between devices with different operating systems (both between iOS and Android and between either of iOS or Android and other device operating systems including Samsung Smartphone) is a constant threat for Apple should it cease to compete effectively for customers through innovation. There is a meaningful, consistent and upward-trending willingness of consumers to switch between devices and platforms, and an ongoing capacity for them to do so.
51. To compete successfully with Samsung, Google, Huawei and others, Apple differentiates itself on the basis of its continuing commitment to policies that protect the value that consumers clearly recognise and the benefit that developers clearly derive. This has, from the outset, been at the heart of Apple's vision and proposition to consumers and has significant benefits in relation to consumer protection, privacy, device and data security, and child safety. 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.

¹⁶ Apple, *App Store*, <https://www.apple.com/app-store/>.



52. In contrast to other digital platforms the subject of the DPSI Report and the recommendations made by the ACCC, Apple does **not** sell its consumers' personal information to advertisers or others. Apple generates the vast majority of its revenue from the sale of products like the iPhone and iPad. Indeed, approximately 20% of Apple's overall global revenues come from Apple Services, including the App Store.
53. Apple's overall business model informs its incentives with respect to the App Store - a key component of what makes Apple's products uniquely attractive to consumers. From the beginning, Apple has made clear that a central "*purpose in the App Store is to add value to the iPhone.*"¹⁷
54. Apple's business model therefore depends on the availability of high-quality third-party apps that customers can integrate with Apple's products. The App Store features numerous third-party apps that compete with Apple's own Calendar, Camera, Cloud Storage, Mail, Maps, Messaging, Music, Notes, Podcasts, TV, Video Chat, and Web Browsing apps. Many of the most popular apps compete against Apple's own services. Specifically:
- (a) Third-party apps enhance the functionality of Apple products and, by providing a superior user experience, increase their desirability for consumers. This in turn increases consumers' desire for Apple devices like iPhones and iPads.
 - (b) Third-party apps have enjoyed large-scale success in the App Store, compete with Apple's apps across every category, and, in many cases, have a greater market share than Apple's own apps. For example:
 - (i) Apple Music competes with Spotify, Amazon Music, Deezer, Google and others. Spotify has twice as many paid subscribers as Apple Music does worldwide.¹⁸
 - (ii) Apple Maps competes with Google Maps, Waze, Here WeGo and Citymappers. Google Maps has been downloaded by Apple users hundreds of millions of times globally over the past five years.¹⁹
 - (iii) Messages competes with WhatsApp, Telegram, Facebook Messenger, Snapchat and Discord. Snapchat and Facebook Messenger were among the most frequently downloaded free iPhone apps globally in 2022.²⁰
 - (iv) Mail competes with dozens of other mail apps on the App Store, many of which are free to download, including Gmail, Spark, Yahoo Mail, and Canary.
55. Apple is therefore incentivised to create a robust app ecosystem with as many quality apps as possible. The health and diversity of this ecosystem is critical to Apple's success because it,

¹⁷ See "'The Mobile Industry's Never Seen Anything Like This': An Interview With Steve Jobs at the App Store's Launch", *The Wall Street Journal* (25 July 2018), <https://www.wsj.com/articles/the-mobile-industrys-never-seen-anything-like-this-an-interview-withsteve-jobs-at-the-app-stores-launch-1532527201>.

¹⁸ See "How many users do Spotify, Apple Music and other big music streaming services have?", *MusicAlly* (19 February 2020), <https://musically.com/2020/02/19/spotify-apple-how-many-users-big-music-streaming-services/>.

¹⁹ Kyle Andeer, Responses to Questions for the Record from the Honorable David N. Cicilline, U.S. House of Representatives - Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary (16 July 2019), <https://docs.house.gov/meetings/JU/JU05/20190716/109793/HHRG-116-JU05-20190716-SD036.pdf> at p. 7..

²⁰ Brenda Stolyar, "Apple unveils the most popular iPhone apps of 2019", *Mashable* (2 December 2019), <https://mashable.com/article/apple-most-popular-iphone-apps-2019/>.



in turn, drives the sale of our hardware products, which is Apple's core business. Apple has a strong incentive to keep its ecosystem open and to deliver choice and quality to consumers.

56. Different business models and monetisation strategies are key aspects of competition. Apple's business model, which focuses on the sale of devices, means that Apple has no incentive to foreclose third party apps, like Spotify, Netflix and others, from the App Store. The availability of a wide variety of high-quality third-party apps in the App Store adds value to, and increases the desirability of, Apple devices. Apple has no reason to undermine apps which contribute to that dynamic, even in circumstances where those apps compete with Apple's own apps.
57. Apple also competes with other software distribution platforms to attract developers to the App Store. The DPSI Report misapprehends the importance and extent of competition on this side of the market. By way of example, at least 22 other digital distribution platforms launched between 2008 and 2011 with which the App Store competes, including Google's Android Market (now Google Play), Nokia and Samsung's Ovi Store, Galaxy Apps Store, Amazon's App Store, and Nintendo's eShop. Apple also competes against PC and console app platforms such as Microsoft's Xbox and Sony's PlayStation, and other tablet devices. Apple seeks to attract new developers and to encourage existing developers to invest additional resources to enhance their existing apps or develop new apps. It does so by introducing new or improved features and services, and by adjusting its commission downwards for various categories of developers.

Apple is not a "gatekeeper" - developers have, and make use of, alternatives to native app distribution on the App Store

58. The ACCC considers that "*Apple's market power in the supply of mobile OS provides it with market power in relation to the distribution of mobile apps through the Apple App Store*".²¹ In taking this approach, the DPSI Report fails to capture the distinction between "distribution of native apps" into the store and "distribution/monetisation of content" by developers.
59. The App Store is one of many distribution channels for apps to consumers; developers have multiple options for distributing their content to consumers. For example, Apple has supported web apps (as an alternative means for developers to distribute apps to iOS users, other than the App Store) since the earliest days of the iPhone. Apple embraced the concept of web apps in 2007 when it launched the iPhone. Apple believed that web apps provided a great opportunity to create for the iPhone. When it decided to open its proprietary technology platform to native apps, Apple continued to support web apps. And in recent years, Apple has continuously added new functionality to its WebKit application programming interface (**API**) to enable greater features and functionality for web apps.
60. Apple submits that the relevant market encompasses the distribution of both iOS and non-iOS apps, and so it is difficult to accept the ACCC's position that Apple has "*significant market power in mobile app distribution*".
61. Developers can also avoid paying any commission by offering apps to be downloaded for free and then monetising through alternative means (such as in-app advertising). In practice, most apps are free to download (both for users and developers) and native app distribution does not trigger a commission unless the developer chooses to charge for the app download itself, which is rarely the case. 84% of native apps on the App Store do not attract any commission payable to Apple (as at October 2020), and most developers that pay a commission to Apple are eligible to pay only 15%. In particular:

- (a) Apple receives **no commission** when developers:

²¹ February 2022 Discussion Paper p 20. See also, ACCC, DPSI Interim report No. 2 (March 2021) p 43; DPSI Report pp 36-38.



- (i) offer apps for free;
 - (ii) offer apps that generate revenue from in-app advertising;
 - (iii) sell physical goods and services in their app; or
 - (iv) offer "reader apps", where users purchase or subscribe to content outside of the app, but can access that content on their devices (eg, a subscription to Netflix or Spotify, book titles for use in Amazon's Kindle app, or newspapers or magazines).
- (b) Apple receives a 15% commission:
- (i) for digital subscriptions purchased through the App Store after the first subscription year; or
 - (ii) where developers earn less than US\$1 million in revenue in the previous calendar year for all their apps, as well as developers new to the App Store.
- (c) For other purchases of paid apps on the App Store (including in-app purchases of digital content and during the first year of digital subscriptions), Apple receives a 30% commission.
62. Apple has **never** increased its commission - which is substantially less than the 50% to 70% industry-standard revenue share charged on software application sales when Apple launched the App Store. Apple's commission offers Apple a fair return on its investment in the App Store, the value of Apple's tools, software and other intellectual property, and the App Store's value in connecting developers to users.
63. Any assessment of Apple's market power in relation to distribution of native apps on the App Store must therefore take into account the options available to app developers to adjust their monetisation approach and avoid paying the commission altogether.
64. The ACCC says that it is concerned that "*Apple ... market power in [its] dealings with app developers is highly likely to enable [it] to unilaterally set and enforce the rules that app developers must satisfy*", which "*have generally included requirements for certain app developers to use the in-app payment system provided by ...Apple*".²² The ACCC says that the "*[t]ying of app store services to in-app payment systems leads to a loss of consumer choice as consumers are unable to use any other payment option when making payments in apps ... [and that this] could negatively impact the quality and functionality of the apps and services the app developers wish to provide their users*".²³ Once again, these statements ignore the reality that developers can and do sell digital content for use in their iOS apps outside of Apple's In-App Purchase (**IAP**). On this, they pay no commission to Apple - and never have.
65. Many significant apps successfully use these strategies to "disintermediate" Apple and distribute their content outside of the App Store. Prominent examples are music streaming services (Spotify above all) and video streaming services (eg, Netflix). With apps available for free download on the App Store, Spotify and Netflix have in essence disintermediated the App Store, continuing to appear in the App Store but in reality acquiring the bulk of their subscriptions outside the App Store (and thus avoiding paying any commission). Spotify, for instance, **turned off entirely** the option for consumers to subscribe via Apple's IAP in 2016,

²² DPSI Report p 133.

²³ DPSI Report p 133.



and has relied instead since then on Apple's reader-rule to allow users to access content on Spotify's iOS app.

66. The ACCC's assessment of "the distribution of mobile apps" as an activity where Apple purportedly has market power ignores this reality. Apple, as the owner of the App Store platform, is concerned about quality, integrity, safety, and overall experience. It has strong incentives to ensure that apps can be distributed through the App Store only if they meet sufficiently high standards. However, developers choose how to monetise their apps. If they choose to charge for download, Apple will take a commission on that sale. Alternatively, developers can use the App Store for app discovery and distribution and have their app loaded for free, whilst monetising their service also on different platforms and allowing users to import and consume the content on the iOS app free of charge.
67. Apple's IAP is also hardly unique; Google's Play Store, the Amazon Appstore, the Microsoft Store, and many video game digital marketplaces, such as Xbox, PlayStation, Nintendo, and Steam, all have similar fees and requirements to use the marketplace's official in-app purchase functionality.
68. The Government has already announced consultation on payment systems reforms to address perceived gaps in current regulatory structures, including in relation to competition issues, in the context of in-app payment services and digital wallets. As the DPSI Report acknowledges,²⁴ Apple considers that consultation and regulatory development forum to be a more appropriate means of identifying and addressing any sector-specific reforms in payment systems regulation for digital wallets and in-app payment services.²⁵

E. Proposals to limit developers' and other platforms' use of consumer data are welcome, but have no relevance to Apple²⁶

69. Apple welcomes measures to limit or restrict the commercialisation of user data, particularly with respect to data which is collected without the user's knowledge and permission.
70. Privacy is embedded in the DNA of Apple's products and the App Review process. Apple believes privacy is a fundamental human right, and privacy has long been an integral part of Apple's brand.
71. Apple's business does not depend on the commercialisation of user data. Apple sells products and services, like the iPhone and iCloud, to consumers. It does not operate a data-driven business that relies on selling its customers' data to advertisers. That is not, and never has been, Apple's business model.
72. In fact, Apple **limits** the use of user data by third-parties by:
 - (a) not engaging in tracking consumers across third party apps in the provision of Apple-delivered advertising. Therefore, unlike third-party advertising service providers, Apple does not need to prompt users for permission to track because it does not engage in this practice. Apple simply does not track users in this way;
 - (b) giving users an additional privacy choice related to Apple's own limited data collection practices across a limited number of first party apps – a choice that third parties do not give users. As this is an additional consumer choice about the use of their data, Apple proactively presents users with a more prominent, unavoidable option to choose between Personalised Ads On or Off for Apple-delivered

²⁴ DPSI Report p 163.

²⁵ See further Consultation Paper Q3.

²⁶ See generally Consultation Paper Q8, Q17.



advertising. This choice screen is presented upon launch of the App Store or of Apple Stocks or Apple News in Australia and informs users as to the purpose of Personalised Ads and its privacy practices, so that the user can decide whether to turn on or off Personalised Ads; and

- (c) when users choose to have personalised advertising, relying exclusively on a limited amount of first-party data (ie, data that is collected by a company through the use of its own services, such as the information that a user provides directly to a developer from their use of a developer's app). By contrast, most major advertising platform companies — including Meta and Google — do not offer users a choice of disabling the use of first-party data for targeted advertising. And those that do offer such a choice bury it beneath a cumbersome process involving numerous settings screens. Apple is once again at the forefront, by expressly and unavoidably prompting users for permission to use first-party data to deliver Personalised Ads.

73. However, part of the ACCC's proposal includes Apple being required to ring-fence its data obtained as an app marketplace operator from other operations and business decisions to minimise the risk that the information provide an unfair competitive advantage over other app developers.

74. Such a remedy would be inordinately burdensome on Apple and the organisation of its business, and without any basis insofar as Apple is concerned. Apple's business is perhaps uniquely structured in a cross-functional way, with different functions all working together cohesively and operational units being shared with multiple business groups across Apple.²⁷ Remedies that mandate functional or structural separation could require significant systemic changes across that business. And obviously, such systemic changes would have a long-lasting impact on Apple.

75. The ACCC has provided insufficient evidence of harm to warrant such a burdensome remedy and conversely has not articulated with cogent evidence, in the case of the integrated Apple hardware, software and services, what the benefit to consumers would be or doing so.

F. Any new or increased regulatory burden – including any mandatory codes – should be subject to merits review and independent, expert determination

76. If the Treasury ultimately considers, contrary to the matters outlined in this submission, that there is a sufficient market failure justifying the implementation of the reforms canvassed in the DPSI Report, any such measures must be subject to appropriate regulatory oversight.

77. Specifically, if mandatory industry codes were adopted in the form discussed in the DPSI Report for 'designated' digital platforms, the process of 'designation' (which the ACCC suggests be assessed according to quantitative and/or qualitative (ie, subjective) criteria) should be as objective as possible, and directed towards addressing actual, identifiable harms to competition - rather than the mere possibility of market failure having regard to the size, revenue or number of active users (that is, *success*) of a platform service.

78. It is uncontroversial that the mere possession of market power is not, of itself, detrimental to competition, and is not impermissible under competition policy. Rather, the *misuse* of market power (or 'abuse of dominance') has the potential to cause anticompetitive harm under certain market conditions and competitive dynamics. The assessment of whether a platform service should be subject to 'designation' must therefore be undertaken on a case-by-case basis having regard to the facts and market dynamics in issue. An indiscriminate approach which

²⁷ See <https://hbr.org/2020/11/how-apple-is-organized-for-innovation>



punishes successful platforms risks chilling the efficient use of, and investment in, the digital economy.

79. This is consistent with the approach taken under the National Access Regime (**NAR**),²⁸ where a threshold for 'declaration' under the regime requires that "access (or increased access) to the service, on reasonable terms and conditions, as a result of a declaration of the service would promote a material increase in competition in at least one market (whether or not in Australia), other than the market for the service".²⁹ The size of the relevant infrastructure facility (or service provider) is merely one of a number of criteria for declaration under the NAR which must be weighted equally - and which must all be satisfied - before increased regulatory burden is placed on service providers.
80. In addition, Apple submits that designation and other decisions under any industry code should be subject to merits review, and subject to rigorous economic analysis conducted by an appropriately qualified, independent agency such as the role of the NCC in analysing whether the s44CA declaration criteria are satisfied and making recommendations to the Minister..
81. Merits review would at least enable a person affected by the administrative action of the designated Minister or the ACCC to have that action reviewed on its merits, or to challenge a finding of fact. In general, merits review is the process by which a person or body:³⁰
- (a) other than the primary decision maker;
 - (b) reconsiders the facts, law and policy aspects of the original decision; and
 - (c) determines what is the correct and preferable decision.
82. As a general principle, decisions that are made by an expert body, or that require specialist expertise, should be reviewable on the merits. That review should be of a quality comparable to that applicable to the decision. These principles are consistent with those developed by the Administrative Review Council in its publication *What decisions should be subject to merits review?*:³¹

The principal objective of merits review is to ensure that those administrative decisions in relation to which review is provided are correct and preferable:

- *correct - in the sense that they are made according to law; and*
- *preferable - in the sense that, if there is a range of decisions that are correct in law, the decision settled upon is the best that could have been made on the basis of the relevant facts.*

This objective is directed to ensuring fair treatment of all persons affected by a decision.

Merits review also has a broader, long-term objective of improving the quality and consistency of the decisions of primary decision makers. Further, merits review ensures that the openness and accountability of decisions made by government are enhanced.

²⁸ *Competition and Consumer Act 2010* (Cth) Pt IIIA.

²⁹ *Competition and Consumer Act 2010* (Cth) s 44CA(1)(a).

³⁰ Administrative Review Council, 'What decisions should be subject to merit review?' (1999) <<https://www.ag.gov.au/legal-system/administrative-law/administrative-review-council-publications/what-decisions-should-be-subject-merit-review-1999>> [1.1].

³¹ Administrative Review Council, 'What decisions should be subject to merit review?' (1999) <<https://www.ag.gov.au/legal-system/administrative-law/administrative-review-council-publications/what-decisions-should-be-subject-merit-review-1999>> [1.3].



83. Merits review provides the only means to correct decisions made by an administrative decision maker on the basis of incorrect facts. Judicial review rarely allows for factual errors (other than jurisdictional errors) in decisions to be revisited or corrected. The court's concern in judicial review proceedings is limited to whether the legal framework for decision-making was observed, and whether the law was properly interpreted.
84. The decision to 'designate' a digital platform would enliven substantial regulatory obligations on the provider of the platform service and would have a significant effect on the rights and obligations for both platforms and consumers alike. Designation decisions are not in the category of policy decisions of a high political content so as to fall within the exception from merits review for issues of the highest consequence to the Government.³²
85. In the absence of merits review, the decision whether to 'designate' a platform would be within the sole discretion of the decision maker (such as the ACCC, or the relevant Minister). The provision for independent merits review provides a necessary and important layer of oversight within the designation process, and promotes confidence in the independence of administrative decision making and any apprehended bias.
86. Further, the decision to 'designate' a platform – as well as any review of that decision – should be undertaken independently of the agency responsible for the enforcement of any code or other obligation on designated platforms: namely, the ACCC. It would be inappropriate for the ACCC to be given responsibility both for the first stage of the process, designation, and the second stage – investigating and determining whether a platform has complied with the obligations under a code or other regulation.
87. These are roles that require the ACCC to act with independence, both actual and perceived. The ACCC's independence in executing these roles would be jeopardised if it were responsible for determining the scope of any code, and the content of its obligations (as well as the ACCC's antecedent role throughout the DPSI and the views it has already expressed about digital platforms throughout that market inquiry). The circumstances are different, but the concern is the same, as that explained by the High Court in *R v Australian Broadcasting Tribunal; ex parte Hardiman* (1980) 144 CLR 13, 35-36: "*if a tribunal becomes a protagonist...there is a risk that by so doing it endangers the impartiality which it is expected to maintain in subsequent proceedings*".
88. Again, an analogy may be drawn with the process under the NAR, where each stage of the process is demarcated between the independent, specialist National Competition Council (**NCC**) which makes recommendations as to whether the 'declaration' criteria for an essential facility have been met, and the ACCC, which is responsible for the arbitration of access disputes for such facilities.
89. Importantly, under the NAR, both declaration decisions (made on the recommendation of the NCC) and arbitration determinations (made by the ACCC) are subject to merits review by the Australian Competition Tribunal (the **Tribunal**). The Tribunal is a specialist review body constituted with judicial and lay members having knowledge of or experience in industry, commerce, economics, law or public administration.
90. Whichever body is responsible for the threshold 'designation' decision, and the review on the merits of that decision, Apple believes that these roles should be performed independently of that envisaged for the ACCC under any regime, and by persons with the appropriate regulatory, industry, economic and competition law expertise.

³² Administrative Review Council, 'What decisions should be subject to merit review?' (1999) <<https://www.ag.gov.au/legal-system/administrative-law/administrative-review-council-publications/what-decisions-should-be-subject-merit-review-1999>> [4.2].