MOBILE ECOSYSTEMS MARKET STUDY
APPLE RESPONSE TO INTERIM REPORT

The launch of the iPhone in 2007 has been described as "*kickstarting a mobile revolution that has transformed the modern world*".[1] One of the keys to the iPhone's success is the seamless user-experience that makes it easy to set up and use the iPhone, with minimal hassle from interoperability issues and security threats. This user experience was not due to happenstance but stems from Apple's decision to develop an integrated solution, including the operating system (iOS) which was - and remains - about guaranteeing a high-quality, safe and trusted mobile experience for consumers through its devices.

Today, Apple is in direct and fierce competition with Samsung, Google, Huawei and many others on a global basis, competition which has and continues to yield remarkable advances in innovation. To compete successfully, Apple differentiates itself on the basis of its continuing commitment to tight integration across product areas and policies that protect the value that consumers clearly recognise and the benefit that developers clearly derive.

This integration has, from the outset, been at the heart of Apple's vision and proposition to consumers[2] 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.

The evidence before the CMA demonstrates the reasons why Apple has designed its products as it has, and the benefits that this has delivered to consumers and developers. Yet on the basis of partial analysis and hypothetical concerns – as detailed below – the Interim Report (IR) proposes interventions in an already highly competitive market that would fundamentally change the iPhone and have huge implications for consumers, including in terms of Apple's industry-leading privacy and security standards, and would reallocate the distribution of benefits of the app economy from the broadest set of developers to a small set of successful incumbents.

Apple respectfully submits that the second half of the market study must undertake a more balanced investigation of the issues under consideration. The findings of the market study are intended to feed into the actions that may be taken by the new Digital Markets Unit and could have an impact on other regulatory proceedings worldwide. With so much at stake, the final report of the market study must go beyond the acceptance at face value of often self-serving complaints from a limited number of the largest market participants. It must hear more from consumers about why they continue to choose Apple devices. The final report cannot rely on hypothetical considerations to the exclusion of positive evidence submitted by Apple, app developers and other interested parties. And it must contain a fuller examination of the implications of the interventions that it is proposing.

---

1 https://www.businessinsider.com/watch-steve-jobs-first-iphone-10-years-ago-legendary-keynote-macworld-sale-2017-6?r=US&IR=T#jobs-took-to-the-stage-in-his-trademark-black-turtleneck-sweater-for-the-now-legendary-presentation-in-january-1.

2 This involves reliance on a single, curated App Store, the requirement for browsers to use a single browser engine, charging a commission on the in-app sale of digital goods and use of IAP to collect that commission. These have been in place since the iPhone was originally developed and opened up to third-party app distribution. They are foundational to Apple's ecosystem and its business model and to the success of the iPhone over the last fifteen years. They are a reflection, not of market power, but of Apple's unique innovation in creating a holistic smartphone experience for users.

A. Introduction

1. The IR recognises the wide-ranging benefits that Apple's tightly-integrated ecosystem has brought to consumers and developers, including ease of use and performance, ongoing investment in innovation and privacy, and the establishment of trust in the platform that leads consumers to try new apps:

High consumer satisfaction with the iPhone: ease of use and performance

- The evidence demonstrates that overall users' satisfaction with iPhones is high, with over 9 in 10 satisfied with their device and [60-70]% reporting particularly high satisfaction.[3]
- The convenience associated with pre-installation and defaults can bring real benefits which are valued by the users of mobile devices, likely to most benefit those users who are less technologically savvy and would struggle to find and install apps which would allow them to achieve their mobile device's full potential.[4] This reflects Apple's aim, which is to provide the best possible overall iPhone experience to users.
- Apple's App Store payment system offers the convenience of being able to use a single set of payment details and deal with a single trusted point of contact for payments, which can be of significant value as users know that their interests will be protected by Apple, and also indirectly benefits developers through the greater confidence users have in placing transactions through the App Store.[5]

Significant and ongoing investments in innovation and privacy

- Apple has invested in innovation and has made many enhancements that have dramatically improved the processing speed, functionality and quality of its mobile devices and connected devices. Apple has innovated in chip design and performance, and haptics, and has introduced new materials like Ceramic Shield Glass to the iPhone. Apple has also introduced innovative privacy features, exploiting its hardware technologies, to empower users.[6]
- Apple has invested billions of dollars in making its ecosystem thrive, by providing tools, software, and technology to make it as easy as possible for developers to bring their ideas to life on the iPhone. Apple's R&D efforts are protected by copyrights, patents, and other intellectual property ("IP") protections. Apple licenses this incredibly valuable IP to developers, providing access to more than 150,000 APIs that allow developers to unlock the potential of Apple's proprietary technologies.[7] Each app made available through the App Store is built on the basis of these innovations from Apple.
- Users have benefitted as the quality of mobile devices has increased,[8] with survey evidence indicating that users consider Apple's devices to be of a higher quality than those of other manufacturers.[9]

---

3 See, IR paragraphs 9, 2.72 and 3.59.
4 See, IR paragraph 6.92.
5 See, IR paragraph 6.174.
6 See, IR paragraphs 9, 3.46 and 3.91.
7 See, IR paragraphs 9, 3.46 and 3.91.
8 See, IR paragraphs 9 and 3.47.
9 See, IR paragraph 3.42.

- Apple's privacy initiatives (which do not preference Apple over third-party apps), such as personalised ads prompts and ATT prompts, empower individuals and enhance user control over their data on Apple devices.[10]

The iPhone has established consumer trust to the benefit of small developers

- Developers consider that Apple's stewardship, in particular through app review processes and strong security features, has established consumer confidence and trust, which is vital for small start-ups and unknown brands.[11]
- By providing and maintaining the App Store with low costs of entry for developers, Apple enables new businesses to come forward that otherwise may not be viable.[12]
- Apple's stable, secure, and trusted platform has also helped create an environment that encourages developer investment in future innovation.[13]

2. Yet the IR sets these benefits aside, without reasoned basis, either ignoring them entirely or dismissing them on the basis of nothing more than speculation, for example dismissing Apple's established record of innovation by stating "*it is difficult to understand how high this level of innovation is and whether it could have been higher with greater competition*".[14]

3. In so doing, the IR reaches conclusions about technologies, product design, and competitive impact derived from the unsubstantiated allegations and hypothetical concerns raised primarily by self-serving complaints from a handful of multi-billion dollar developers such as Microsoft, Facebook, Match, Spotify, and Epic,[15] all seeking to make deep changes to the iPhone for their own commercial gain, without independent verification. Examples include:

   - Paragraph 6.36: "*[One developer] told us that, contrary to Apple's claims, NFC access could be provided to third-party mobile wallets without jeopardising security*". This appears to be the sole evidence for the finding at 6.49 that "*in some cases discussed above – such as access to the NFC chip … there could be less restrictive approaches to controlling access to APIs which would foster competition without compromising security or user experience*" [emphasis added].
   - Paragraph 6.134: "*Spotify stated that it cannot be excluded that Apple might be able to use IAP data to inform its own commercial decisions about Apple Music*" and "*Proton Mail said it*

---

10 See, IR paragraph 6.261.

11 See, IR paragraph 9.

12 See, IR paragraphs 9 and 2.67.

13 See, IR paragraphs 9 and 2.67.

14 IR paragraph 3.92.

15 Many of these developers have clear biases against Apple, including the Coalition for App Fairness (an organization created by Epic Games, funded by Spotify, Match and Tile, whose sole purpose was to generate "continuous media and campaign tactic pressure" on Apple and Google) and Hausfeld & Co LLP (which acts for the claimants against Apple in a UK class action), and which consequently have a potential financial interest in adverse findings against Apple. Other complainants include Microsoft and Tile (who have publicly criticised Apple) and Epic Games and Masimo (who have been involved in litigation against Apple). The potential for such biases to skew any findings is particularly high given the very limited evidence base underpinning the IR, notably with respect to evidence from app developers. From the face of the IR, it is clear that the submissions received from app developers can represent no more than around 1% of app developers with apps in the UK App Store.

was concerned that Apple 'could be using commercial data which it receives through IAP to gain a competitive advantage when it comes to its own product development' and that this 'could give Apple superior market intelligence over its competitors or any potential competitors'" [emphasis added].

4. As a result, the findings in the IR are, in effect, no more than hypotheses about how Apple's ecosystem "may" have the "potential" to harm competition, being as they are untested and based on one-sided evidence. Such hypotheses are insufficient to warrant, never mind support, a discussion of potentially radical remedies at this stage, whilst there remains significant investigative work needed to ground any theories of harm and consider the real impact on competition and on consumers.

5. A clear example of this is in relation to the proposed remedy to mandate alternative app stores or allow sideloading. Apple has provided objective third-party research that confirms its approach to security, including its ban on alternative app stores and sideloading, is many times more effective than Android's or any other consumer computing platform.[16] The IR places little to no weight on this evidence, or even on its own finding that potential remedies which are designed to "*allow more choice or competition within an ecosystem could in principle result in weaker protection for the security of users' mobile devices*" [emphasis added].[17] As a result, the IR significantly downplays the security risks associated with this proposed remedy. It also fails to account for the fact that users highly value that security, and that many choose Apple over Android on that basis. Remedies that jeopardise Apple's holistic approach to security would effectively remove the competitive differentiation between Apple and Android, taking this valued element of choice away from users.

6. Apple is deeply concerned that the IR is proposing solutions to hypothetical problems that will result in real-world market interventions that could force it to redesign the iPhone to benefit a handful of powerful developers. The IR appears to assume that its proposed changes would be relatively simple. Yet many would require a complete re-architecting of a product that has existed for 15 years, has been constantly improved by Apple's investment in IP and is valued and trusted by millions of consumers. It would force changes that could limit choice and significantly increase costs to both consumers and the broadest set of developers, and would disadvantage smaller and start-up developers as compared to the large incumbents who currently dominate digital services such as music, gaming, and video streaming. The CMA cannot dictate and control the direction and speed of future innovation on the basis of speculative concerns fuelled by large tech companies intent on using the regulatory process to undermine Apple's ecosystem.

7. Apple urges the CMA 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 impacted.

8. To this end, Apple's response below addresses the following topics:

   - Section B addresses competition between the Apple and Android ecosystems, providing a high-level overview of the Apple ecosystem, the drivers behind how the ecosystem operates and its impact on competitive differentiation and user experience.

---

16 For example, The Nokia Threat Intelligence Report 2020 results confirm that iOS devices suffer 15 to 47 times fewer malware infections than Android devices. Another third-party study found that 98 percent of mobile malware targets Android, rather than iOS devices.

17 IR paragraph 7.27.

- Section C addresses the IR's assessment of the App Store.
- Section D addresses the IR's assessment of mobile browsers and browser engines.
- Section E considers Apple's privacy initiatives.
- Section F considers Apple's approach to cloud gaming.
- Section G provides Apple's initial assessment of the proposed remedies.

B. The Competitive Interaction between Apple and Android ecosystems

9. The evidence shows that Apple's integrated business model offers consumers a clear alternative to the Android system, providing them with a real choice across key parameters of competition. For developers, Apple offers an integrated, curated alternative to Android's licensed OS. The evidence also shows that the level of competition between the Apple and Android ecosystems is high, and has been significantly underplayed in the IR.

(i) The IR significantly understates competition between Apple and Android devices

10. The IR draws the "initial conclusion that both Apple and Google have substantial and entrenched market power over the users of their mobile operating systems".[18] This conclusion is based on a preliminary assessment that competitive constraints for Apple and Google are "limited" because of limited user-driven competition, barriers to switching between iOS and Android, and barriers to entry and expansion for rival providers of mobile OS.

11. This view is unfounded, as Apple competes vigorously with Samsung, Google, Huawei and other Android device manufacturers. It strives to attract and retain consumers who might otherwise be tempted to purchase an Android device, and this is the cornerstone of its commercial strategy across all components of the ecosystem. The view in the IR that that there are two "silos" existing side by side, one speaking to the top end and the other to the bottom end of the market is wholly incorrect, and that flaw colours the competitive assessment throughout the IR.

12. 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 and Samsung. Besides Huawei, other Android smartphone manufacturers from China, such as Xiaomi and One Plus, have rapidly penetrated the European market, including with high-end devices. With almost all non-iOS smartphones running on Google's Android OS, this means that around 70% of smart mobile devices in Europe will have an Android-based OS installed, with just 30% of devices running iOS.[19]

13. The assertion in the IR that there is not enough competition between Apple and Android devices is impossible for Apple to reconcile with its daily experience of the UK market. It relies on a narrow and incomplete assessment, drawing far-reaching conclusions on the basis of a flawed interpretation of limited observations.

14. For example, the IR argues that "there is limited price competition between iOS devices and Android devices"[20] based on the observation that *iOS devices sell at higher average prices than Android devices on average*. This kind of comparison makes no sense. Apple is active predominantly in the premium segment, while Android phones are offered both at the "budget" end of the market and in the premium segment. While this necessarily implies that Apple devices are more expensive than Android devices on average, it is wrong to infer that this would imply limited competition.

- First, the IDC data on which the IR relies shows that various manufacturers of Android devices, including Samsung, OnePlus, and Huawei, are active in the high-end segment with products as expensive or more expensive than Apple's.

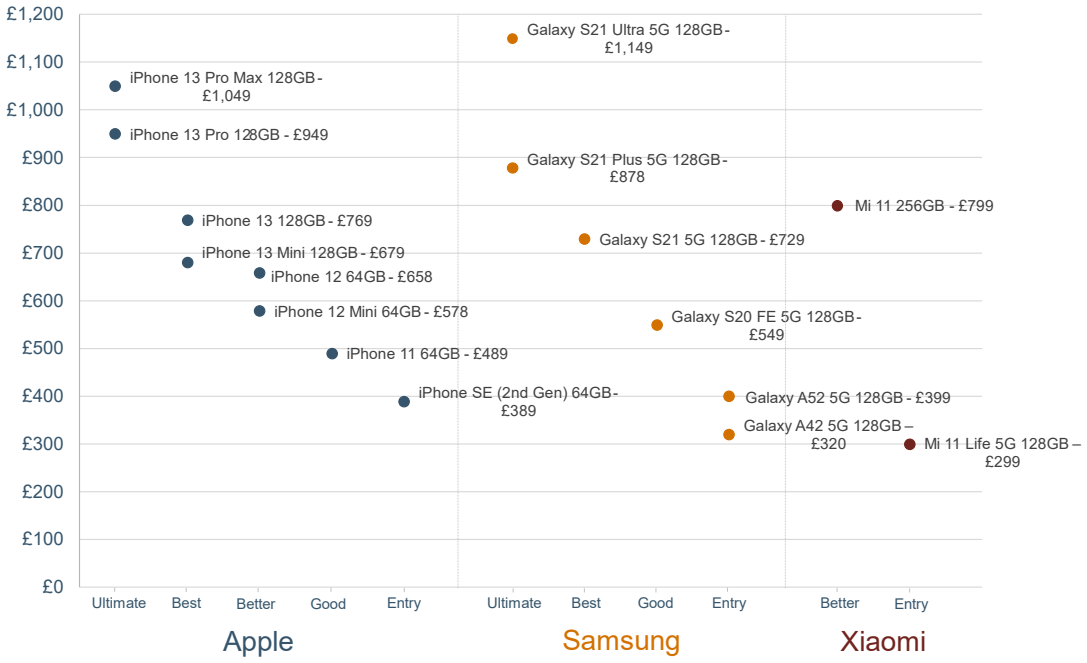
18 IR paragraph 3.191.

19 See Statcounter, https://gs.statcounter.com/os-market-share/mobile/europe.

20 IR paragraph 3.185.

- Second, there are competing devices at each price point at which Apple devices are sold, as illustrated in Figure 1 below.
- Third, Apple constantly monitors and benchmarks its performance in the UK against rivals, on a weekly basis; (i) focusing on how its devices compare across carriers (for contract sales), across channels and in terms of "total cost of ownership"; and (ii) responding with its own campaigns and initiatives to ensure that carriers promote attractive offers for Apple devices. This would not be the case in the absence of strong competition against other device manufacturers.

Figure 1: Price comparison UK, 2022



Source: Apple's weekly analysis of minimum retail prices across Amazon UK, Argos UK, DSG Retail UK, and JLP UK. The figure presents price comparisons with prices at Argos.

15. A reliance on "average price differences" also ignores the fundamental fact that this is a vertically differentiated market, where users trade off price and quality ("value for money") and competitive constraints bear across the price range: consumers will "trade down" if they no longer find a high-end device is worth the price premium. Accordingly, Apple is constrained in its premium segment also by competitors from lower segments (and vice versa). That there is a range of price points is not evidence of lack of competition when there is a range of quality and characteristics at different prices. This needs to be accounted for in the final report's competitive assessment.

16. The IR also relies on survey evidence apparently suggesting that consumers rarely switch mobile OS when replacing their devices, to conclude that "[t]his suggest there is a limited competitive constraint on Apple and Google from rival suppliers of mobile devices and operating systems (including each other)".[21] This is again conceptually wrong, and not borne out empirically. One cannot assume low switching to be the result of a "lack of competition" without at least exploring alternative explanations:

- First, as a matter of principle, while high levels of switching are typically indicative of competition, low levels of observed switching say nothing, *per se*, about competition.

21 IR paragraphs 3.81 and 3.82.

- Second, any interpretation of customer loyalty needs to take account of the extraordinarily high levels of user satisfaction for iPhones. Survey evidence available to Apple in the ordinary course not only confirms that users are highly satisfied on average with their iOS devices, but also shows that those who are not have a higher propensity to leave their respective ecosystem. This is what one would expect in a competitive market where differentiated products are offered, and consumer preferences are relatively stable over time.

17. The IR further claims that survey evidence the CMA has available shows that customers switch more often from Android to Apple than the other way around, and this is evidence that constraints on Apple are weaker.[22] But this overlooks a much more plausible explanation: Apple simply offers more popular products, so users have little reason to switch back to Android. It is well known that loyalty is driven by customer satisfaction. This view is also supported by survey evidence available to Apple in the ordinary course. First, survey evidence confirms *high levels of satisfaction by iOS device owners*, which needs to be taken into account when interpreting the observation that iOS users are less likely to switch OS relative to Android users (because this can reflect higher user satisfaction, rather than barriers to switching). Second, it shows that users switching from Android to iOS are significantly more satisfied with their new device than users switching the other way. Third, when looking at the share of users who switched mobile OS among those upgrading their device, the survey also shows that it is the iOS users who were not highly satisfied with their previous device who tend more to switch to an Android device. This confirms that users switch when they are less satisfied with their iOS device; and they are not held back by barriers to switching. Overall, the CMA cannot simply disregard satisfaction with the device as an obvious driver of consumer choice – and conclude that low switching must be evidence of artificial barriers.

18. Indeed, instead of recognising the impact of user satisfaction, the IR postulates that three main categories of barriers are responsible for a lack of switching: learning costs, transfer costs (for data, apps, and subscriptions), and the availability and characteristics of first-party apps, services, and connected devices.[23] The IR asserts that survey evidence documents the salience of these barriers. However, a closer look shows that only a negligible proportion of survey respondents expressed views that would be consistent with such barriers. What the evidence shows first and foremost is that these are, in fact, not an issue for most smartphone users. There will be, of necessity, some "costs" associated with learning to use a different product: to avoid such costs or ensure availability of the same first-party apps, services, and connected devices, the ecosystems would have to be identical. This cannot reasonably be the benchmark for assessing "barriers to switching". Transferring data etc. across ecosystems is not only possible but it is easy, both from Android to iOS and vice versa.[24] All major smartphone OEMs offer tools to seamlessly transfer content from Apple to Android devices and vice versa.[25] Well-rated apps from third-party providers are equally available.[26] The survey results referred to in the IR[27] are from 2017: they are

---

22 IR paragraph 3.26.

23 IR paragraph 3.102.

24 See, for example, https://www.computerworld.com/article/3218067/how-to-switch-from-iphone-to-android-ultimate-guide.html

25 Such tools include Samsung Smart Switch and TouchCopy. Since several apps seamlessly transfer content and apps from iOS to Android devices, the IR's allegation that "*there does not appear to be a main mechanism through which a third-party switching app can reliably obtain data on which apps a user has installed on their iOS device*"(§3.116) is misguided.

26 For example, Wondershare MobileTrans boasts to be the "Best Secure Phone to Phone Transfer Solution" and works with Android and iOS devices alike. See https://mobiletrans.wondershare.com/

27 IR paragraph, 3.119.

outdated and, in any event, suggest that a vast majority of users were in fact *not* concerned about losing data when switching the ecosystem.

19. The IR not only relies on weak data and analysis, but in places also on outright speculation. Whilst briefly acknowledging that competition takes place also on non-price dimensions, the IR contends that "*it is unclear how strong the competition on features, functionality and performance is*".[28] This is not an analysis, it is the *omission* of any analysis. In fact, as set out in section (ii) below, competition on such dimensions is strong. Statements such as "*the available content on a device does not play a material role in driving whether a user chooses an iOS device or an Android device. This is because (…) many of the same popular apps are available on both iOS and Android devices*"[29] are missing the point; the range of available content may be "similar" on the two ecosystems, but what drives consumers to choose an Apple device is the combination of content, integrated functionalities, ease of use and safety features. Moreover, this ignores the interplay between non-price competition and price competition - offering a high-quality, functionally better product warrants charging a higher price.

20. Overall, the IR cannot be said to present an evidence-based analysis of competition between Apple and Android devices. It relies on limited datapoints (price averages, limited switching) that are overinterpreted as being salient indicators of weak competition. Those few observations are wholly insufficient to support the proposition that there is limited competition between Apple devices and other smartphone devices.

(ii) <u>The iPhone's features meet consumer demand across a number of qualitative competitive parameters</u>

21. That Apple competes directly against other smartphone manufacturers using Android-based OSs is reflected in consumer perceptions. As the IR accepts, Apple devices are perceived as being of a higher quality than those of other manufacturers, with survey evidence showing that Apple's brand scored higher than Samsung's brand on statements such as 'has products with the latest innovation' (68% vs 62%) and 'has products with appealing design' (64% vs 56%).[30] In particular, Apple offers a valued experience for users with respect to the following areas:

<u>Performance</u>

22. Apple's integrated approach to hardware and software provides it with a significant advantage in terms of the performance of its devices. For over a decade, Apple's world-class silicon design team has been building and refining Apple proprietary Arm-based systems-on-a-chip (SoCs). These are tightly integrated with iOS and other software, such as WebKit. Independent tests show that this gives Apple devices significant performance and efficiency benefits compared to Android devices.[31]

23. Additionally, Apple provides greater ongoing software support for older devices than Android, allowing iOS users to retain their devices for longer periods. Indeed, Apple has continuously

---

28 IR paragraph 3.93.

29 IR paragraph 3.94.

30 IR paragraph 3.42.

31 See, for example, A15 v. QCOM S888: https://www.anandtech.com/show/16983/the-apple-a15-soc-performance-review-faster-more-efficient/2; A15 v. QCOM S8G1: https://www.anandtech.com/show/17102/snapdragon-8-gen-1-performance-preview-sizing-up-cortex-x2/2

supported its older iPhone models with frequent software updates even years after its release, whereas companies that develop Android phones are recognised as making their phones obsolete in just two to three years.[32] This difference in approach is an additional reason why users choose iPhones over others.[33]

Functionality and ease of use

24. Functionality and ease of use are key drivers of consumer choice. The IR recognises the importance of innovation in driving device and OS functionality and the efforts that Apple has made in this respect. Apple seeks to make Apple's devices more attractive to users over devices that use Android by offering a superior ease of use and multiple innovative functionalities.

25. A hallmark of the iPhone since its release in 2007 is its ease of use. A user can open the iPhone, set it up in a handful of easy to understand steps, and immediately have a device that works; there is no need to go through many set-up screens and choices. To enable this "out of the box" experience, the iPhone includes a number of pre-installed apps, like the Phone app, the browser or the camera. For example, Apple invested significant resources in building a web browser which, when pre-installed immediately launches the web page selected in Apple Maps or Messages, without the user having to open the browser app and input or paste the web link into the URL box.[34] This seamless and easy-to-use experience is a key driver of consumer choice, with survey evidence showing that 45% of users cite this as "one of the main criteria in their choice of mobile phone".[35] Apple supplements this immediate functionality with the ability to add to the user's personal smartphone experience by offering millions of apps through the App Store.

26. Accessibility is another area where Apple leads the way, with many built-in features such as VoiceOver, Reduce Motion, Spoken Content, shortcuts and workflows, Assistive Touch, Accessibility Keyboard and active listening features, all designed to make the iPhone easier to use.[36] These many functionalities rely on the hardware and software integration that Apple's ecosystem allows.

27. Similarly, with respect to the quantity and quality of content available in a mobile ecosystem, Apple's continued investment in the iPhone, not to mention significant investments in tools and services, have made the impossible, possible over the last fourteen years. Many of the apps available on the App Store today would not have been possible in 2008. Apple's investments in R&D and technology year after year has resulted in an incredibly rich assortment of high-quality apps. Recent examples include the development of health-tracking apps (using ECG and oxygen sensors in wearables), apps that use augmented reality technology to let users visualize in the world around them things that would be impossible or impractical to see, professional photography apps (using Camera developments, such as portrait mode), increased security on pay-by-phone parking and other apps (using Sign-in with Apple), and apps offering customized shared in-app experiences, such as watching or listening to media streaming simultaneously (through SharePlay APIs). In 2008, Apple released a software development kit with 10,000 Application Programming Interfaces ("APIs") which supported the development of 500 apps available through the App Store. Today there are more than 150,000 APIs available to developers. And there are more than 1.8 million apps available on the App Store.

---

[32] See, https://www.techtimes.com/articles/263017/20210717/android-vs-apple-why-phones-limited-support-compared.htm

[33] See, https://www.vice.com/en/article/dypxpx/google-is-forcing-me-to-dump-a-perfectly-good-phone

[34] Of course, users can change the default browser from Safari to another browser in Settings if they so wish.

[35] IR paragraph 3.10 and fn 81.

[36] See, https://www.apple.com/accessibility/.

Security and privacy

28. The IR grossly downplays the importance of security and privacy from a user-choice perspective, including them together with other aspects within the category of "features, functionality and performance". However, in Apple's view these features are essential drivers of choice and of Apple innovation, such that they warrant consideration separately.

29. Apple's emphasis on privacy is not new. It has long been a key differentiator for Apple. Back in 2010, Steve Jobs stated "*[w]e've always had a very different view of privacy than some of our colleagues in the Valley. We take privacy extremely seriously. … Privacy means people know what they're signing up for. In plain English, and repeatedly*".[37] The defining principle for Apple is that the user is empowered to choose how their data is treated and is given sufficient information and options to allow them to make an active choice.

30. Apple adopts an approach of "privacy by design", which reflects this stance. Apple's belief is that users should not be subjected to invasive data collection practices without their knowledge or consent. As a result, every Apple device combines hardware, software and services designed to work together for maximum security and privacy and a transparent user experience in service of the ultimate goal of keeping personal information safe.[38] For example:

- Apple is committed to on-device processing of user data to the fullest extent possible. Apple's focus on privacy means that it actively avoids gathering user data where possible. This holds across Apple's apps and features, such as Apple Maps, Apple's Photos app, Messages, Siri, and Apple Pay.[39] If data is needed to make a service work, as far as possible Apple associates the collection with random identifiers and not the user's identity.

- Apple has introduced significant innovations over the years, including Touch ID, Face ID, iCloud Keychain (which securely stores and autofills passwords across devices), private browsing, and fingerprinting defence to prevent advertisers and websites from combining multiple data points to "fingerprint" a given user; all of which are aimed at improving the security of devices and the information held on them.

- Apple has introduced specific privacy features over the years, including: (i) *Sign-in with Apple,* which hides a user's email addresses from developers to reduce tracking of activity in apps; (ii) *Intelligent Tracking Prevention (ITP),* which limits tracking across websites while still enabling websites to function normally. ITP is turned on by default, there is no need to change anything in Settings or Safari preferences to receive tracking protection;[40] *(iii) Privacy nutrition labels,* which provide users with information about how an app tracks, collects, and uses data; (iv) *App Tracking Transparency*, which further provides users with the ability to decide how their data is treated by requiring apps to show a prompt to users to choose whether to allow a developer to track their activity across other companies' apps and websites; and (v) *Personalized Ads Choice*, which provides a prompt requiring users to choose between allowing the use of first-party data for Personalized Ads On or Off. Apple holds its own apps to this same set of standards. In the case of Personalized Ads Choice, it is holding itself to a higher standard than third party developers. Section E below provides further detail on Apple's recent privacy initiatives.

---

37 https://www.digitalmusicnews.com/2018/03/25/steve-jobs-user-privacy-2010/.

38 For further detail, see https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf

39 For further detail, see Apple's comments on the market study statement of scope document.

40 https://www.apple.com/safari/docs/Safari_White_Paper_Nov_2019.pdf.

31. The importance of security and privacy as a competitive parameter and driver of consumer choice should not be underestimated. Survey data shows that for users, security and privacy is one of the top three reasons for purchasing an iPhone.[41] This is hardly surprising, given the "*dramatic evolution in the role and uses of mobile phones over the last two decades*" and the "*fundamental role [they play] in the lives of UK citizens*".[42] Mobile devices contain a wealth of private and sensitive data to an extent that far exceeds computers, including photos, contact details, location data, activity data, credit card information, usernames and passwords, health information and personal correspondence.

32. Apple takes a multi-layered approach to security to protect iOS users from malicious apps and other threats.[43] This approach is significantly more effective than Android. Indeed, Nokia's 2020 Threat Intelligence Report finds that devices that run on Android had 15 times more infections from malicious software than the iPhone, with a key reason being that Android apps "*can be downloaded from just about anywhere*" unlike the iPhone, which has a single App Store and does not allow sideloading. Similarly, the requirement to use WebKit as the rendering engine allows Apple to push out security patches and updates immediately across any app that shows a webpage, thus addressing malware attacks and reducing security vulnerabilities efficiently.

33. Apple leads the industry in consumer protection, in particular in protecting children by offering controls for parents that are intuitive and customizable.[44] These include: (i) Screen Time limits, (ii) Restrictions that can limit features such as FaceTime, Camera, and Safari, multiplayer gaming and certain social media apps, and also designate appropriate content, and (iii) Family Sharing's Ask to Buy feature, which allows parents to approve all app downloads, app purchases, and in-app purchases made by their children (using their own device to approve or reject the purchase or download), as well as controls for spending and receipt of funds using Apple Pay services like Apple Cash. Further, Apple's App Review process allows Apple to individually screen apps to prevent inappropriate content being aimed at children.[45]

(iii) <u>Apple's integrated approach brings multiple benefits to users and developers</u>

34. Apple's vision to develop products that offer the best possible smartphone experience has been rooted from the beginning in its integrated approach and its belief that the very best solutions require deep integration of hardware and software. The iPhone combines cutting edge design with a tightly integrated package of hardware components (including components designed by Apple, like its market-leading microprocessor technology and camera), and a proprietary operating system that is designed to the specific attributes of the iPhone. This ensures that each component of the system is trusted, which validates the system as a whole. From initial bootup to iOS software updates to third-party apps, each step is analysed and vetted to help ensure that the hardware and software are performing optimally together and using resources properly. It is this approach that gives Apple products their distinctive "look and feel" and that allows Apple to create an integrated ecosystem that is distinct from competitors' ecosystems. In this model, Apple's devices and its services are complementary, with the "whole" driving the consumer experience, allowing Apple to offer consumers a qualitatively different smartphone experience.

---

41 Kantar Comtech GB research CQ1 2021 See, also, https://www.nytimes.com/wirecutter/reviews/ios-vs-android/

42 See IR paragraphs 2.1 and 2.2.

43 A summary of this multi-layered approach can be found at: https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf

44 See https://www.apple.com/legal/privacy/en-ww/parent-disclosure/

45 See https://www.apple.com/uk/families/

35. Apple's choices are explicitly intended to further the interests of consumers – from opening its proprietary technology for use in third-party apps, while preserving quality standards; to pioneering privacy innovations that empower consumers to make informed choices about their data.

36. Apple also has a strong incentive to 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.[46]

37. Developers have benefitted enormously from Apple's approach. Apple has made it easy for them to create applications using Apple's proprietary technologies and intellectual property. And it has made it easy for them 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. As a result, developers earned over £1.6 billion in billings on the UK App Store in 2021 alone.

(iv) Implications for the second half of the market study

38. The importance of competitive differentiation between Apple and Android ecosystems and the way this benefits consumers and developers must be appropriately addressed in the second half of the market study. In particular, the CMA's consideration of potential remedies must recognise that users have a choice between iOS and Android, which are evaluated by users on significant parameters such as performance, security, and privacy. Apple strives to address the needs of those constituencies of users who particularly value such elements through its approach to integration.

39. This high-value offering to users is secured through Apple's specific approach to its ecosystem, including its reliance on integration and the inclusion of complementary services that make its overall offering more attractive in competition with others. The CMA must therefore be aware that if it undermines Apple's approach through potential remedies (for example, by mandating alternative app stores on iOS devices), the CMA would, in fact, be removing that qualitative choice from consumers, and positively mandating an increased privacy risk for such consumers.

[46] IR paragraph 2.39.

C. The IR's Consideration of the App Store

40. With respect to the App Store, the IR highlights a number of areas for follow-up in the second half of the market study, including: (i) the effects of pre-installation across app categories; (ii) the importance of app search navigational and categorical queries; and (iii) the use of data by Apple's app development teams. Apple looks forward to engaging further with the CMA on these topics. In this response, Apple addresses some fundamental misconceptions in the IR's preliminary assessment of the App Store.

41. The IR's consideration of the App Store suffers from a failure to recognise the importance and extent of competition between Apple and other software distribution platforms to attract developers. At least 22 other digital distribution platforms launched between 2008 and 2011, 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 for its 3DS device. 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. This competitive interaction has played out to the benefit of developers.

42. In terms of features and services, Apple offers developers access to hundreds of thousands of APIs that simplify and accelerate the development process. Through the global footprint of its Developer Relations Team, Apple is also committed to providing further support to app developers, and is constantly working to improve App Store functionality and associated search performance. The extent to which this is driven by competition is clear. For example, Apple introduced wireless charging in 2017, which was already available on Samsung devices, offered female health tracking on Apple watch in 2019 following the introduction of similar features by FitBit and in 2020, answered Google's Instant Apps with App Clips. On other occasions, Apple has led the way, as, for example, with app ratings, where Google introduced its new feature to weight app ratings following Apple's revision of its app ratings feature, and with editorial features, where again Google followed Apple in expanding these features.

43. With respect to pricing, Apple has introduced new rules that allow developers to avoid or reduce transactions that are subject to a commission. Apple's unfailing practice over the last fifteen years has been to consistently reduce commissions, either through rules such as the Reader Rule and the Multi-Platform Rule, or programmes like the Video Partner Program and others that involve reduced commissions. Again, the competitive interplay here is clear. When Apple announced in 2016 that it was reducing the App Store commission to 15% for subscriptions in their second year, Google responded by matching the policy. In 2020, Apple responded to Google's launch of promo codes with the introduction of subscription offer codes. More recently, following Apple's announcement of the Small Business Program, Google announced that it would lower commissions to 15% for the first $1 million of revenue earned by developers.

44. In positioning its competitive assessment of the App Store, the IR makes two fundamental conceptual errors. First, its focus on the role of Apple as a "distributor of native apps" into the App Store ignores the competitive constraints under which it operates. Second, the IR treats Apple's App Store as a standalone object separate from devices, which entirely fails to appreciate Apple's device-centric business model. The sub-sections below highlight key elements that must be borne in mind in order to properly frame an assessment of Apple's position and conduct.

(i) The IR's consideration of the App Store wrongly focuses on "distribution of native apps" instead of competitive constraints

45. The IR finds that "*the limited competitive constraints placed on them mean that Apple and Google each have substantial and entrenched market power in the distribution of native apps within their ecosystems*".[47] In taking this approach, the IR fails to capture the distinction between "distribution of native apps" into the store and "distribution/monetization of content" by developers. Whilst the App Store is a distribution channel for apps to consumers, developers have multiple options for distributing their content to consumers. The IR also fails to take into account the two-sided nature of the market and the fact that the availability of a broad selection of innovative and popular apps helps Apple sell iPhones.

Constraints on the distribution of native apps

46. The IR focuses on the distribution of native apps through the App Store. In its assessment, the IR ignores the two-sided nature of the market and fails to account for Apple's incentives to ensure that it can offer a broad selection of innovative and high-quality apps on the App Store. A rich library of high-quality third-party applications helps Apple sell iPhones and iPads. 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 monetization 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.

47. The IR also ignores the competitive constraint on Apple from alternative monetization approaches app developers can pursue on iOS, as well as the fact that those competitive constraints differ as between apps with different characteristics. Developers have multiple monetization options which they can pursue to avoid paying a commission to Apple. For example, a developer can avoid paying any commission by offering the apps to be downloaded "for free" and then monetizing through alternative means. 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 (94% of native apps on the App Store were free as of December 2021).[48] Apple's model has created a wealth of free content for users, with over 1 million free-to-download apps on the UK App Store in 2020, a growth of over 6,000% since 2008.

48. While developers who offer their apps for free in the App Store pay no commission for app distribution, they can and do, however, 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).[49] Other apps pay no commission because they rely on advertising or focus on physical sales, none of which triggers any commission.

49. 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 (e.g. Netflix). With apps available for free downloaded on

---

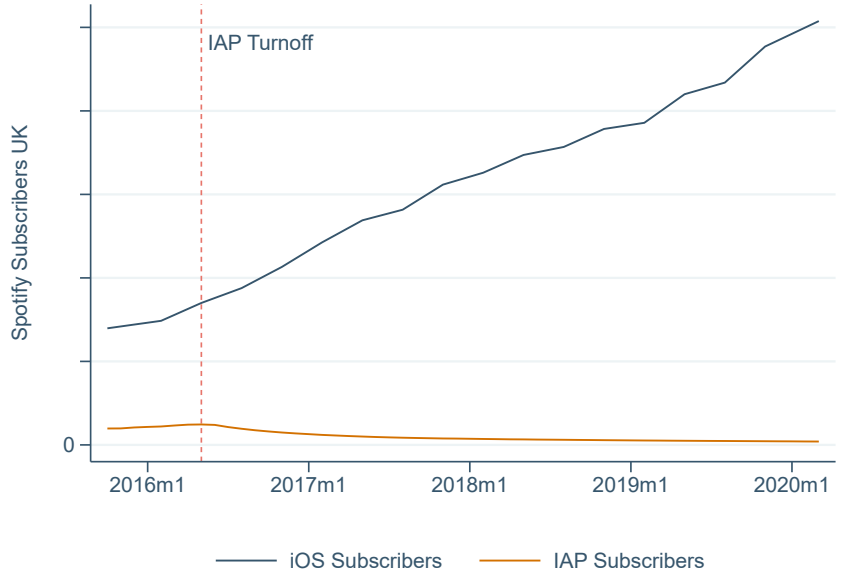
47 Chapter 4, p.124.

48 See https://www.statista.com/statistics/1020996/distribution-of-free-and-paid-ios-apps/ .

49 App developers can and do circumvent Apple's commission entirely by relying on the so-called reader or multi-platform rules.

the App Store, Spotify and Netflix have in essence disintermediated the App Store, continuing to appear in the Store but in reality acquiring the bulk of their subscriptions outside the App Store (and thus avoiding paying any commission).[50] Spotify, for instance, turned off entirely the option for consumers to subscribe via Apple's IAP in 2016, and has relied instead since then on Apple's reader-rule to allow users to access content on Spotify's iOS app.[51] Spotify has continued to thrive, attracting subscribers in the UK from other channels.

Figure 3: Spotify overall Premium subscribers on iOS, vs Premium subscribers acquired through IAP (UK)



Source: MIDiA for Spotify UK subscriber numbers, survey evidence for the share of Spotify UK subscribers with an iOS device, Apple data for the number of IAP subscribers.[52]

50. Video streaming services ("VSSs") similarly distribute their digital content, including subscriptions, mostly through the web. Netflix and Sky Go have stopped offering the option of purchasing digital content through IAP at all. Figure 4 shows the breakdown of overall revenue earned by third-party VSSs from iOS users in 2020: in 2020, the total net commission revenue to Apple was only about 2-3% of third party VSS providers' revenues earned from iOS users. Third-party VSSs paid no commission on the vast majority of VSS revenues earned from iOS users in the UK in 2020, although these users can freely stream videos on their iOS devices.

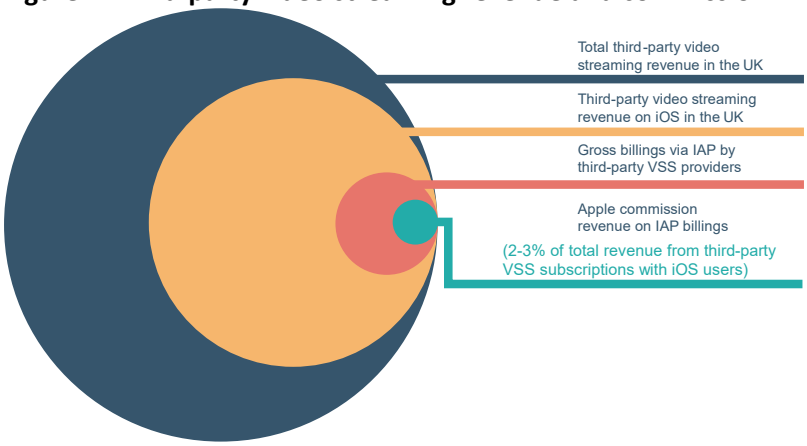
---

50 Spotify used IAP only for a short period of time and stopped offering it in 2016. Only few legacy customers are still on IAP, see https://www.cnet.com/tech/mobile/apple-fires-back-spotify-pays-fees-on-less-than-1-percent-of-members/. The reader rule allows app developers including Spotify to provide access to digital content like music, videos or e-books purchased outside the app to their users without incurring a commission by Apple. See e.g. https://developer.apple.com/app-store/review/guidelines/, 3.1.3 (a)

51 This holds also at a global level, see https://www.statista.com/statistics/813828/spotify-revenue-quarterly/ and https://www.statista.com/statistics/244995/number-of-paying-spotify-subscribers/ for statistics

52 The number of Spotify iOS subscribers is based on the share of Spotify subscribers in the UK whose primary device is an iPhone, elicited from a 2020 survey conducted by Apple in the context of EC proceedings. It is assumed, for the purposes of Figure 3, to be constant over time. The total number of Spotify UK subscribers is interpolated based on quarterly data from MIDiA.

Figure 4: Third-party video streaming revenue and commission in the UK (2020)



Source: Analysis of Statista and Apple data.[53]

51. Gaming apps multi-home on several platforms (smartphones, game consoles and PCs) and developers can exploit the fact that content purchased on another platform can be accessed by users of the app within iOS without incurring additional charges by Apple to the developer or user.[54] Dating service providers rely on a similar approach, as users of dating apps can use their dating subscription plan previously made via web app or the provider's website in their iOS device.

52. The IR's assessment of "the distribution of native apps" as an activity where "Apple 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 monetize 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 monetizing their service also on different platforms and allowing users to import and consume the content on the iOS app free of charge. Apple is constrained by these alternatives, and over time it has indeed *reduced* the commission it charges to app developers for in-app sales of digital subscriptions (a reduced commission of 15% as of the second year;[55] a reduction to 15% also for developers whose revenues were below 1m USD in the previous year;[56] a lower commission also for participation in the Video Partner Program for providers of premium video content[57]).

---

53 The bubble size is proportional to the number represented. Third-party VSS revenues for 2020 calculated by deducting Apple TV+ revenue from aggregate 2020 UK VSS revenue (from Statista). Third-party VSS revenues on iOS estimated by multiplying third-party VSS revenues by the share of iOS users among third-party VSS users in a survey conducted for Apple. IAP gross billings and commission include Netflix, YouTube, Disney+, Amazon Prime Video, Sky Sports and NOW TV All figures in GBP.

54 These apps can rely on the multi-platform rule and monetize their content by selling it in the app via Apple IAP and in parallel also outside the app on other platforms. See https://developer.apple.com/app-store/review/guidelines/, 3.1.3 (b).

55 See e.g. https://developer.apple.com/support/downloads/terms/schedules/Schedule-2-and-3-20211213-English.pdf, 3.4

56 See e.g. https://www.apple.com/newsroom/2020/11/apple-announces-app-store-small-business-program/

57 Apple, "Auto-renewable Subscriptions," available at https://developer.apple.com/app-store/subscriptions/, accessed on January 7, 2022 ("The net revenue structure for auto-renewable subscriptions differs from other business models on the App Store. During a subscriber's first year of service, you receive 70% of the subscription price at each billing cycle, minus applicable taxes. After a subscriber

The App Store cannot be viewed on a "standalone" basis

53. The IR frames the App Store as a "standalone" object. This is fundamentally wrong. The App Store was created as a complement to the iPhone. Apple's conduct on the App Store cannot be assessed in isolation; competition with Samsung, Google, Huawei and other device OEMs drives Apple's choices on the App Store as well.

54. There is no independent demand for "App Stores" that Apple is seeking to develop *separately from devices.* Apple's incentives are to add value to the App Store (with curated content, high privacy standards, high consumer experience) because that helps sell devices, while at the same time continuing to introduce new features into its devices because that also creates more activity on the App Store.[58] Apple's incentives are aligned in creating a mutually reinforcing customer proposition that works, not because consumers have no choice, but because consumers recognise the value they are being offered.

55. The IR recognises there is what it calls a "waterbed effect" of this kind in operation, accepting that "*Apple has some incentive to lower the price of its devices in order to capture more add distribution revenue*"[59] but argues that "*the relevant question is not whether there is a waterbed effect at all, but whether it is sufficient to offset Apple's market power in native app distribution*"[60]. It dismisses this possibility on grounds that (i) the App Store generates high gross margins, and at the same time the iPhone has the highest margins of Apple's devices, and, (ii) iOS device prices have "increased" relative to Android device prices. This is incorrect for a number of reasons:

- First, the observation that Apple's iOS business is profitable overall in no way casts doubt on the existence or strength of the waterbed effect. The waterbed effect means the margins of the device business and the App Store are interlinked, not that they are necessarily low.[61]
- Second, the argument that iPhone prices have increased relative to average Android prices is irrelevant, as comparisons of average prices of all Android devices with iOS devices do not

---

accumulates one year of paid service, your net revenue increases to 85% of the subscription price, minus applicable taxes."); Apple, "Apple Video Partner Program," available at https://developer.apple.com/programs/video-partner/, accessed on January 7, 2022 ("This program is designed for apps that deliver premium subscription video entertainment services. Participating apps are required to integrate with a number of Apple technologies, such as Universal Search, Siri, AirPlay, and single sign-on or zero sign-on, to ensure a seamless experience for customers. … As a program member, you earn 85% of sales from customers who sign up using Apple's in-app purchase system.").

58 The fact that Apple's device centric business model generates these types of incentives, and that Apple's choices are aligned with the interest of consumers, has been formalised in terms of economic analysis by Etro (2020, 2021). Etro illustrates in a formal setting what is Apple's business reality: that a device-funded business model creates better incentives for quality and curation of the app store (relative to an advertising-funded model); and that revenues from App Store activities contribute to Apple's ability to offer more competitive devices. See: Etro, Frederico (2021): Device-funded vs. ad-funded platforms. International Journal of Industrial Organization. 75 (2021). https://doi.org/10.1016/j.ijindorg.2021.102711

59 IR paragraph 4.190.

60 IR paragraph 4.191.

61 More generally, the Interim Report remains silent on what it means by "*offsetting Apple's behaviour in native app distribution*". As discussed at length in the previous subsection, native app distribution is mostly free of charge. Also, "offsetting" device prices and IAP commissions suggests a separate evaluation of both. However, this is wrong both from a customer point of view as well as from Apple's point of view. Customers purchase both devices and services, and Apple accounts for this in its pricing. In particular, Etro (2021) shows under a broad set of assumptions that customers are typically better off when Apple is free to set prices as to optimise its profits rather than being exogenously constrained in one product dimension.

provide any relevant basis on which to assess device level competition, for the reasons described in Section B above.

- Third, App Store terms and in particular the headline commission rates are substantially the same across the world and these reflect the constraint Apple faces from device competition at a global level. It is therefore wrong to claim that the intensity of local UK device competition would be insufficient to constrain Apple's conduct on the App Store.

(ii) Apple's API restrictions are not a form of "self-preferencing" or "third-party preferencing"

56. The IR echoes the arguments from Spotify and a handful of like-minded developers that Apple engages in so-called "self-preferencing" behaviour by failing to immediately make all of its proprietary technologies available to millions of third-party developers. As a preliminary matter, Apple notes that it works hard to make technologies available to third-party developers 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 has invested significant engineering time and resources to make more 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.

57. More fundamentally, if Apple were engaged in "self-preferencing" behaviour, one could expect some strengthening effect in the market position of Apple's apps that compete with third party apps. This is simply not happening, and the IR does not suggest otherwise. Indeed, it would be hard to do so given the competing apps from well-established players such as Microsoft, Hulu, Spotify, PayPal, Amazon, Skype, Google, and Meta, who often have a much greater share of the market in those downstream app categories (with Spotify, for example, holding over 60% of the music streaming market in the UK;[62] Amazon accounting for almost 90% of UK e-book sales;[63] and Microsoft with 89% of office productivity software[64]).

58. It cannot be seriously argued that Apple must grant the same level of access in the same timeframes to third parties as it does to its own integrated apps. 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.

59. The IR simply repeats the criticisms from a handful of developers in relation to Apple's approach to providing third-party access to hardware and software. It then concludes that "*in some cases …. total restrictions on third-party access are likely to significantly distort competition and that there could be less restrictive approaches to controlling access to APIs which would foster competition*".[65] The question is not whether, in theory and absent any context, there are less

---

62 See: https://www.kantarworldpanel.com/global/News/Spotify-is-shaking-off-the-competition-in-the-UK-audio-

63 See: https://publishdrive.com/amazon-ebook-market-share.html

64 See https://www.computerworld.com/article/3637079/as-google-moves-to-reshape-workspace-barriers-to-business-adoption-remain.html

65 IR paragraph 6.49.

restrictive approaches, but rather whether any restrictions that Apple does place on third-party access are objective and whether they, in fact, constrain competition. It is clear from the IR, that the evidence relating to the APIs under review does not come close to supporting such a conclusion:

- The IR relies on a single unnamed developer's assertion to conclude that NFC access could be given to third-party mobile wallets without jeopardising security. Apple has provided detailed evidence as to why this is not the case and why any unlocking of NFC card emulation mode by Apple for use by third-party contactless payment applications would expose Apple device users to new attacks against their digital footprint and would create a new high-value attack surface in the Apple user ecosystem. Potential alternatives, such as the HCE solution, developed by tech providers and banks, have a security stance that is acknowledged widely as having fewer protections, with inconsistent deployments of those protections it does offer, contained in apps that are subject to the choices and capabilities of each developer (whose own data protection and security programs may be insufficient).
- With respect to the Ultra-wideband (UWB) chip, as the IR recognises, Apple has already begun to provide access to third parties to the chip. It released specifications for chipset manufacturers last spring and began certification of products last fall.[66] Third parties have already announced products that will take advantage of UWB in iPhone.[67]
- Apple's decision to test split-view multi-tasking with a limited group of third parties before opening up access more widely is a sensible and valid approach to security, and does not even begin to support a conclusion that this "*potentially distort[ed] competition*", as suggested in paragraph 6.45. Indeed, such a suggestion runs counter to the IR's earlier finding that "*In some instances, [Apple] may also give a competitive advantage to certain privileged third-party apps, but we have not heard concerns about restrictions on API access distorting competition in this way*".[68]
- With respect to third-party voice assistants, enabling access to certain device functionality implicated in the IR would entail considerable privacy risks. For example, allowing third-party apps to have always-on access to the microphone of iOS devices or to read user texts in the Messages app would immediately nullify Apple's data privacy policies because it could no longer guarantee that user utterances and data exposed to the device microphone or in the Messages app (including sensitive health or financial information) would be collected, processed, and protected according to Apple's stringent privacy standards. Indeed, data-harvesting companies like Google and Amazon operate with entirely different business models regarding user data.

60. To the extent 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.

(iii) <u>App Review must be assessed in the wider context of its role in protecting users and developers</u>

61. The IR suggests that App Review functions as a gatekeeper and this "*could result in Apple … giving preferential treatment to [its] own apps [and be] liable to hinder innovation by app developers more broadly*"[69]. The assumption underlying this concern (that Apple would want to disadvantage

66 https://developer.apple.com/nearby-interaction/

67 See https://www.engadget.com/tile-pro-ultra-wideband-tracker-new-devices-100025451.html

68 IR paragraph 6.27.

69 IR paragraph 6.74.

third-party apps) is flawed. There is no objective evidence that Apple has used App Review to hinder its competitors. On the contrary, Apple's incentive is to ensure that a wide array of high-quality apps is available on the App Store.

62. The IR's concerns are based on anecdotal complaints from a handful of multi-billion dollar developers who want unfettered access to Apple's technologies and consumer data. The concerns ignore entirely the contrary evidence of app developers that "*Apple's stewardship of its ecosystem, in particular through app review processes…, helps to create consumer confidence and trust, which is vital for small start-ups and unknown brands.*"[70]

63. App Review 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: (i) work properly; (ii) not compromise the functionality of their device; and (iii) 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.

64. For developers, App Review not only provides a ready user-base who are willing to trust in the apps available on App Store and thus to download new apps, but also provides considerable protection against fraud and IP infringements. App Review identifies thousands of copycat apps (more than 5,000 in 2021 alone), which are removed from the App Store, thus protecting the original app developer. App Review also provides indirect benefits for developers through its role in preventing malware that could infect individual apps or features of the iPhone on which the apps rely. App clean-up also helps developers to showcase their best work to consumers.

65. The limited number of complaints with respect to delays or rejections that have been raised with the CMA must be viewed in this overall context. Apple reviews approximately 100,000 new and updated apps each week, of which the majority are reviewed in less than 24 hours, and almost all within 48 hours. Similarly, Apple's current Service Level Agreement (SLA) commitment for appeals is 48 hours. Further, most app rejections are for issues that will negatively impact the consumer experience, and, in some cases, the issues are so dangerous - like human trafficking, illegal content, spyware/malware, identity theft - that the app needs to be re-reviewed and, if verified, taken down immediately.

66. Apple works constantly to improve the App Review experience for developers and to take account of developer feedback. For example, in August 2020, Apple implemented a new procedure for developers to suggest changes to the App Review Guidelines. Before making new updates to the App Review Guidelines, Apple reviews and considers changes suggested by developers. If a suggestion promotes the guiding principles of the App Store—to provide a safe experience for users to get the best apps and a great opportunity for all developers to be successful—Apple makes the change and informs the developer who submitted the suggestion. In October 2021, Apple launched a new App Store submission process that provides for correspondence on App Store Connect (the portal through which developers interact with Apple and the App Store) to remain available for a longer period. Some of the complaints relied on in the IR, such as those by Basecamp, predate this development and should be assessed in that light.

[70] See, IR paragraph 9.

(iv) The benefits of In-App Purchase have not been fully appreciated or assessed

67. The IR's assessment of Apple's IAP requirement fails to fully appreciate the nature of IAP. It is not payment processing. IAP is the commerce engine that enables Apple to collect its commission – by cataloguing transactions so that Apple may receive payment for running the App Store and providing the tools, technology, distribution, and other services to developers. IAP provides developers with a means of monetizing their apps and allows Apple to collect a commission for the plethora of functions that it has put in place (including technology, customer connection, and customer trust) to lead to an in-app purchase in the first place. Comparing the benefits of IAP to those offered by payment processing firms is therefore an inapt and inadequate assessment.

68. IAP also enables a number of features that are fundamental to the premium consumer experience on the App Store This is clear from the comprehensive benefits that IAP provides, which are substantively different to those provided by a payment processor. As set out at paragraph 6.173, the benefits of IAP include:

- "Family Sharing" and "Ask to Buy", which allow parents to approve all app downloads, app purchases, and IAP purchases made by their children, with obvious financial and safety benefits.
- Clear and Conspicuous Pricing, which does not allow a purchase to complete until sufficient pricing information is shown to the user.
- Biometric Authentication, via the consumer's fingerprint on Touch ID-enabled devices, or the consumers face on Face ID-enabled devices.
- Email Receipts and Purchase History, which provides customers with insight into and control over their spending.
- Report a Problem and Refunds, which provide users with the significant benefit of dealing with a single point of contact and with a company of Apple's reputation, rather than having to track down individual developers.
- Restore Purchase, which enables the completion or restoration of purchases, whether in situations where either a user hit the "buy" button for an IAP purchase and the developer did not deliver the content for some technical reason, or where the user wants to transfer an app and in-app-purchased content onto a new Apple device.
- Subscription management, which makes it easy for users to cancel subscriptions across multiple apps in a single, convenient place with a single tap on their devices.
- Fraud prevention, through the identification of trends and overarching developments, allowing Apple to root out scams and unscrupulous developers.

69. These benefits go beyond just the user experience and provide vital consumer protection functions, ensuring that bad actors cannot take advantage of consumers on the App Store and that users can make purchases through the App Store with confidence. For example, the Ask to Buy capability empowers parents to control the purchases of digital goods and content by their children. Importantly, if a developer tries to circumvent these controls by using a third payment service provider, Apple can immediately address the issue.[71] Similarly, Apple's subscription

[71] Such controls are vital, given the possibility for children, particularly those playing gaming apps, to unintentionally spend significant sums of money. See for example, https://www.businessinsider.com/fortnite-addictive-epic-games-parliament-prince-harry-2019-6?r=US&IR=T#fortnite-sells-digital-currency-in-packs-for-between-10-and-100-parents-can-restrict-

management provides real protection for users that might be tricked or trapped into signing up for online subscriptions, by requiring clear and conspicuous disclosures and customer consent for subscriptions and by making it very easy for users to cancel subscriptions.

70. The CMA recognises the importance of this role that IAP plays, noting that, for users, being able to use a single set of payment details and deal with a single trusted point of contact for payments is an important benefit, which may provide "significant value" to users and that developers are "likely to indirectly benefit from users having greater confidence in placing transactions" through the App Store.[72]

71. The IR appears to recognise that these benefits are available because IAP is part of an integrated commerce system and IAP transactions are catalogued and verified through that commerce engine.[73] However, the IR then goes on to say that "*alternative payment systems offer users several benefits that [IAP] currently [does] not, such as greater flexibility in the pricing structures and payment methods offered to consumers and the ability to manage refunds directly*".[74] Even from the face of the IR, it is clear that two individual payment-processing benefits cannot outweigh the many other benefits set out above that users receive from the use of IAP, nor does the IR even attempt to assess how they could.

72. The IR's assessment in any event fails to fully take account of the pricing flexibility that IAP does offer. Apple's pricing system allows developers to set a price for an app or digital content in their local currency and then have the same price automatically equalized in local currency across the App Store's 175 storefronts around the world.[75] This is particularly important for those developers who may not be able to offer global services, where they may know little about local market practices regarding pricing, subscriptions, and promotions, among other things.

73. Apple continually introduces more flexibility when its systems can support doing so in a safe and effective manner. Apple has continued to release different types of subscription offers over time based on developer feedback, starting with introductory offers (for new users), then promotional offers (for lapsed/existing users), and, most recently, subscription offer codes (for out-of-app distribution).

74. In the absence of a proper recognition and examination of the Apple IAP benefits in comparison to the arguments raised by a limited number of developers, the IR is not in a position to properly find that IAP raises competition concerns and/or potentially harms consumers.

(v) <u>The CMA's concerns with the Anti-Steering rules are significantly overstated</u>

75. At paragraph 6.217, the IR states that *"[a]lmost all the app developers we contacted who use Apple's IAP and have apps available on multiple platforms have confirmed that the anti-steering rules prevent them from advertising to customers within a native app that cheaper purchase options are available outside the iOS app, such as via the developers' website*", leading the CMA

---

purchases-for-kids-but-it-requires-changing-account-control-settings-outside-of-the-game-4, covering Parliament's inquiry into Epic Games' "Fortnite", including whether it has proper restrictions in place to keep players, and more specifically children, from spending too much time or money on the game.

72 *Ibid*.

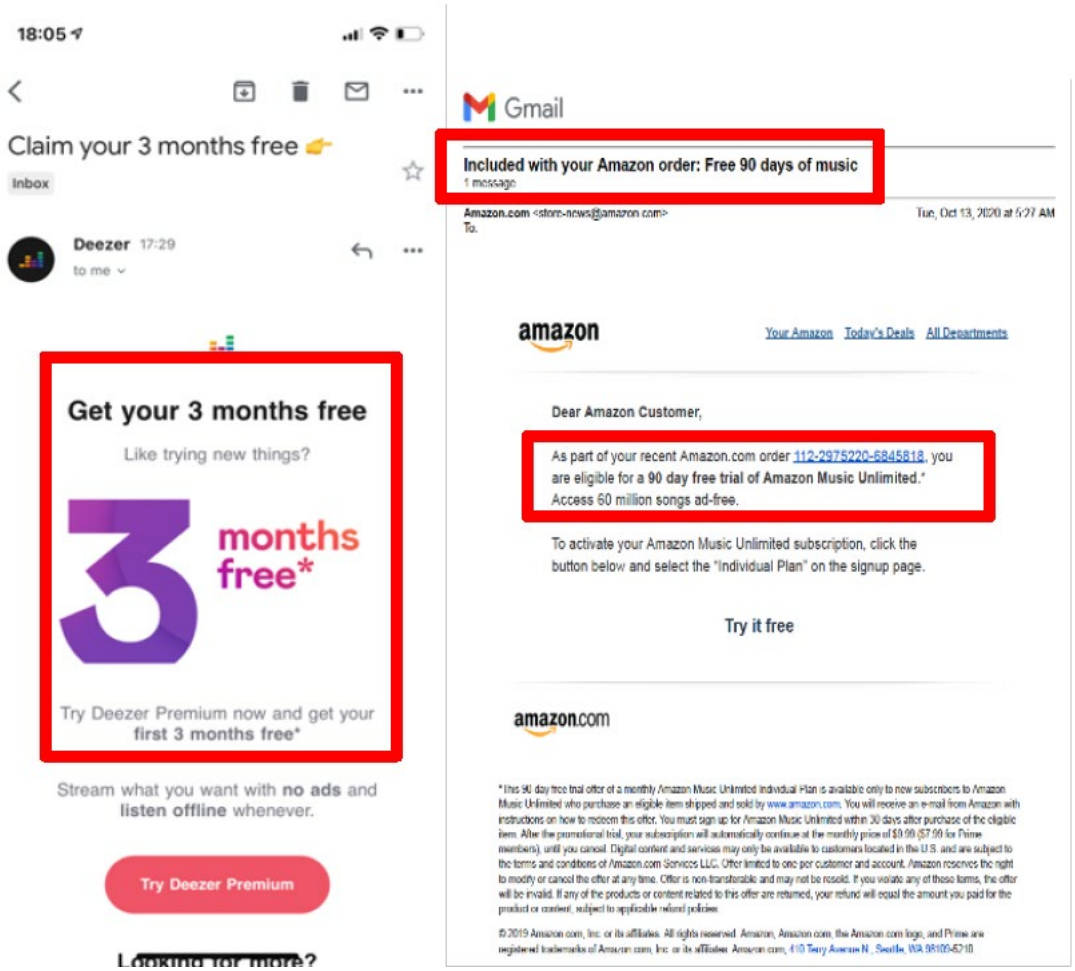
73 IR paragraph 6.174.

74 IR paragraph 6.175.

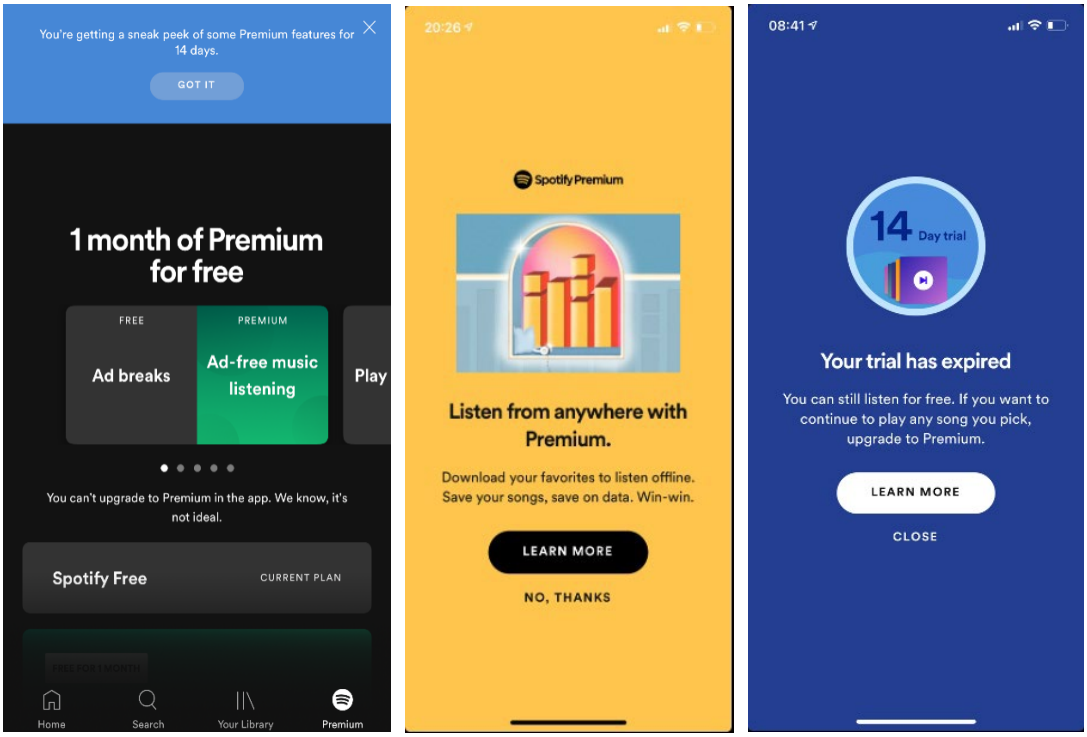
75 This pricing flexibility comes on top of the marketing and editorial support to developers as well as billing and tax services Apple offers to developers.

to find a potential concern that "*the anti-steering rules may mean that users are unaware of alternative, possibly lower cost options for purchasing outside of an app*".

76. Apple imposes no restriction on any developer's ability to engage in general marketing activities or even to communicate with individual users about payment methods outside of their iOS app in a targeted fashion. This means developers can market their non-IAP subscriptions to individual iOS users with emails generated by calls to action within the app, highlighting Apple's commitment to broaden marketing opportunities available to app developers. Examples of emails making such offers are:



77. Importantly, a quick review of Spotify notifications to consumers through its iPhone app shows that there are ample means for developers to communicate to users even within the iOS app itself:



78. As a result, it is clear that there is no reason for the IR to assume that consumers would be "unaware of alternative, possibly lower cost options for purchasing outside of an app". Rather than preventing competition or inhibiting consumer awareness, the anti-steering rules simply prevent app developers from circumventing the requirement to use IAP and to pay Apple its lawful commission.

79. The CMA's concern with respect to Anti-Steering, namely that Apple "may" be preventing developers and consumers from accessing lower-cost options for purchases, also reflects a failure to appreciate the extent to which developers can choose to monetize their apps in ways that avoid the use of IAP at all. The most significant of these are through the use of rules such as the Reader Rule and Multiplatform Rule that Apple has developed over time to allow developers to sell digital content to iOS consumers without using IAP or paying a commission to Apple:

- The Reader Rule makes IAP optional for developers selling digital music, eBooks, video, audio, newspapers, and magazines (including webtoons). Apple recently announced changes to enable a link out of a Reader app to manage subscriptions and purchases in early 2022. It is currently working on guidelines to enable linking out of Reader apps in a way that is consistent with Apple's longstanding commitments to safety, security and privacy.
- The Multiplatform Rule provides developers that implement IAP with additional flexibility, by allowing them to sell digital goods and content outside of the app (through their website, on a gaming platform like Microsoft Xbox, or some other channel of distribution) and then have users access that content within the iOS app. The developer pays Apple no commission on those transactions that take place on other platforms but are nonetheless consumed within iOS.

80. These and other changes have enabled payment choices for every developer. Most developers, including 85% of the developers on the App Store, choose not to use IAP at all. And rules like the Multiplatform Rule and the Reader Rule mean that for those developers that implement IAP in their apps, it is only one option for developers to sell digital content and goods to users.

(vi) The CMA's views on potential remedies are insufficiently considered

81. The IR's consideration of potential interventions is ill-founded and premature, given the lack of evidence demonstrating real competitive harm. With respect to the App Store, in particular, this is of key concern, given the draconian nature of the interventions proposed, including the possibility that Apple could be required to allow alternative app stores on iOS devices and alternative payment methods within the App Store.

82. The IR recognises that "*there are potential security and privacy risks associated with permitting third-party app stores and sideloading.*" However, it appears to consider that these may be relatively easily addressed by "appropriate safeguards."[76] Such a blithe assumption is unwarranted. Apple's multi-layer approach to security is designed around its "walled garden", of which a single App Store is a key element. Replacing this with certification or verification arrangements 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.[77] Similarly, Apple's built-in privacy protections, such as ATT, 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.

83. If Apple were to be forced to allow alternative app stores or sideloading, the increased risk of malware attacks 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. 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.[78] 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.

84. With respect to IAP, the IR recognises that, if Apple were to be required to allow an alternative to IAP, it would have to develop alternative ways to collect its commission. As the IR notes, one of the risks of this intervention is therefore that the alternative would be "*less efficient or result in harmful unintended consequences*".[79] Indeed, given the integrated nature of IAP into Apple's commerce engine it is undoubted that any alternative would necessarily be less efficient.[80]

---

76 IR paragraph 7.58.

77 For example, the Nokia Threat Intelligence Report 2020 finds that devices that run on Android had 15 times more infections from malicious software than iPhone, with a key reason being that Android apps "can be downloaded from just about anywhere" unlike the iPhone, which has a single App Store and does not allow sideloading. See also https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf

78 See: https://www.perle.com/articles/why-byod-culture-poses-a-major-risk-to-enterprises-40188803.shtml

79 IR paragraph 7.101.

80 For example, following the recent decision of the Dutch Competition Authority, Apple will allow dating app developers in the Netherlands App Store to use a third-party payment system within the app. To do so, a developer will need to request one of two new entitlements and submit a separate app binary for review.

85. It is clear therefore that the IR's proposed remedies 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 require a remedy that 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 less effective than those it already offers users.

D. The IR's consideration of mobile browsers and browser engines

86. With respect to mobile browsers and browser engines, the IR also highlight areas for further engagement in the second half of the market study, including: (i) in-app browser functionality; (ii) web browser apps; and (iii) Apple's ITP. Apple looks forward to engaging further with the CMA on these topics. In this response, Apple addresses some fundamental misconceptions in the IR's preliminary assessment of the role of WebKit with respect to security, privacy, and performance.

(i) Webkit is an integral part of Apple's overall security, privacy and performance efforts

87. The IR states that "*[w]e have not seen compelling evidence that suggests Apple's ban on alternative browser engines is justified on security grounds*"[81]. This fundamentally misunderstands WebKit's role in ensuring the security of devices. It also ignores the very real benefits that WebKit brings with respect to privacy and performance.

88. Apple designed the iPhone to ensure that code executed by apps on the device comes from a known and vetted source. Through the Developer Program and the App Store, Apple ensures that apps come from known developers who have agreed to follow its guidelines, and to subject their apps to App Review. While the web is vital to the user's experience on iOS, it also exposes the device to unknown and unvetted sources. This creates an inherent conflict; users must have the ability to surf the web, but the web is also a critical vector for unknown, malicious actors to perpetrate attacks on iOS devices. To protect iOS devices, Apple has tightly integrated WebKit into iOS to provide a number of key security features and benefits:

- WebKit on iOS supports a customized sandbox profile that represents a decade's worth of security improvements and is substantially different from other iOS processes and even from WebKit on macOS. WebKit's sandbox profile on iOS is orders of magnitude more stringent than the sandbox for native iOS apps. This dramatically restricts the attack surface from which malicious actors can attack iOS processes. Via close collaboration between WebKit and iOS security engineers, the WebKit sandbox is regularly updated, and new sandbox technology developed to tighten it in response to evolving and emerging threats.

- Today, roughly 1 million apps render web content on iOS, and all of them use a common WebKit install. This allows Apple to distribute important security updates to all of these apps in a single update. Apple has historically shipped security updates for WebKit with regular releases approximately 7 times a year, as well as on an *ad hoc* expedited basis in response to significant security threats. Other platforms take a fragmented approach to browser engine security, permitting apps to embed different browser engines, which are, in effect, different versions of the browser engine. For example, on Android, the Chrome, Edge, and Samsung browsers each embed a different version of the Blink browser engine, and these are not necessarily updated consistently when Google ships a security update to Android. As a result, Android cannot control when Blink-embedded apps patch serious vulnerabilities, meaning that updates are never applied consistently at scale. As a result, apps may be allowed to continue using outdated embedded browser engine versions many months, or more, after fixes have been released by the browser engine vendor. Even a "dedicated" browser app, like the Samsung browser, which the IR notes has more than 15% share of usage on Android in the UK, hasn't updated its embedded browser engine in more than 5 months.[82] The Epic

[81] IR Chapter 5 key findings table.

[82] Samsung Browser Chromium Release 92.0.4515.166 (last verified 7 February 2022).

Privacy Browser's Android app hasn't updated its embedded browser engine in nearly three years; whereas its iOS app's browser engine was last updated on January 26, 2022.[83]

- WebKit is the only iOS process capable of accessing the just-in-time compiler or "JIT". The JIT allows apps browsing the web to quickly and efficiently render JavaScript content, which is valuable for users but also exposes a vulnerability that malicious actors can exploit. To mitigate the risks posed by the JIT, WebKit leverages tight integration with iOS hardware. Apple employs a highly effective hardware security extension (APRR) to prevent attackers gaining access to the JIT. Apple also implements Pointer Authentication Codes (PAC) to prevent attackers from gaining code execution outside of the JIT. PACs provide cryptographic signatures and authentication to function pointers and return addresses to protect against the exploitation of memory corruption bugs.

89. The IR pays little attention to privacy and performance, but these are vital reasons behind the WebKit requirement. By integrating WebKit into iOS, Apple is able to guarantee robust user privacy protections for every browsing experience on iOS devices. WebKit employs a suite of technologies and strategies to defend user privacy, including third-party cookie blocking by default, storage and service worker partitioning, private browsing, requiring a user permission for websites to access the device orientation or motion APIs, and preventing fingerprinting of device microphones or cameras via the WebRTC API. As WebKit implements new web features, it looks for fingerprinting or other privacy vulnerabilities to ensure that all users browsing on iOS devices remain safe from privacy-invasive attacks and continue to differentiate iOS devices from their competitors.[84]

90. WebKit has also been carefully designed and optimized for use on iOS devices. This allows iOS devices to outperform competitors on web-based browsing benchmarks,[85] while also achieving industry leading power efficiency and battery performance.[86]

(ii) Apple cannot guarantee a private, high-performance, and secure browsing experience on all iOS devices if third-party browser engines were required to be allowed

91. Mandating Apple to allow apps to use third-party rendering engines on iOS, as proposed by the IR, would break the integrated security model of iOS devices, reduce their privacy and performance, and ultimately harm competition between iOS and Android devices. Today, users trust that their iOS devices offer world-class security and privacy, as well as all-day battery life, out-of-the-box. These qualities substantially enhance iOS device appeal compared to Android devices, which abdicate security management and privacy protections to individual app developers and offer less optimization or lower efficiency. The IR's proposed remedies, if implemented, would eliminate this differentiation and diminish competition between iOS and Android devices.

---

83 Epic Privacy Browser Chromium Release 72.0.3626.121 (last verified 7 February 2022).

84 See Karami *et al* "*Awakening the Web's Sleeper Agents: Misusing Service Workers for Privacy Leakage*", Network and Distributed Systems Security (NDSS) Symposium 2021.

85 https://www.pcmag.com/news/iphone-13-benchmarks-apples-a15-chip-crushes-qualcomm ("On Basemark Web, a web browsing benchmark, Safari on the iPhone 13 Pro gets nearly double the score Chrome on the Galaxy S21 Ultra does"); https://www.anandtech.com/show/16192/the-iphone-12-review/3

86 https://www.anandtech.com/show/17004/apples-iphone-13-series-screen-power-battery-life-report-long-lasting-devices; https://www.anandtech.com/show/16983/the-apple-a15-soc-performance-review-faster-more-efficient/2

92. As an initial matter, third-party vendors' browser engines would lack important features and security protections that WebKit gains from its tight integration with Apple Silicon and iOS. For example, no third-party engine would offer PACs. More critically, no third-party engine would offer an equivalent to the hardened sandbox profile resulting from WebKit's integration with iOS to protect against malicious web-based attacks. Developers implementing browser functionality in their apps would be left with the generic "container" sandbox built for native iOS apps, which was designed to be significantly more permissive in order to support the full extent of the iOS SDK. Allowing a third-party browser engine to run inside a container sandbox for which it was not designed would undo a decade's worth of browser security improvements and would result in a browser so insecure as to nullify the privacy and security promises that Apple makes to its users and that underpin the appeal of iOS devices. The lack of process separation would allow attackers to enjoy ready access to highly sensitive user data, including data stored on the iCloud Keychain. Attackers could likewise target data that the user shares with family and colleagues, thereby multiplying the threat throughout the user's social network.

93. Compounding the problem, the IR's proposed remedies would help malicious actors circumvent App Review. Via App Review, native app developers must expose the compiled binary of their apps to scrutiny. Critical to this protection is the fact that the behavior of the native app is observable. Web content is not. Browser engines compile and execute code originating from websites in real time, much of which is not static and may be unseen and unknown to users. Today, iOS guarantees that the only dynamic code on the platform is vetted by WebKit in a dedicated process, helping Apple to ensure that dynamic code cannot be abused to circumvent App Review and attack the user's device or invade the user's privacy. With third-party engines on iOS, attackers would have more avenues to infiltrate a device undetected by system security protections and more opportunities to degrade user privacy.

94. The IR's proposed remedies underscore that changes to WebKit would have ramifications across the iOS platform. As the IR observes elsewhere "*where security is optimized across the ecosystem … changes in one part of the ecosystem could therefore have an adverse effect on the integrity of the system more generally.*"[87] The second half of the market study must take account of the tight integration of WebKit into iOS and that iOS as a whole is incontrovertibly more secure than Android. The Nokia Threat Intelligence Report 2020 confirms that iOS devices suffer 15 to 47 times fewer malware infections than Android devices. Another study found that 98 percent of mobile malware targets Android, rather than iOS devices.[88] iOS's superior security is a key driver of purchasing decisions for iOS devices,[89] and efforts to convert iOS into an Android-alike platform threaten to diminish iOS's system-level competitive security advantage and thwart demonstrated user preferences.

95. To fully assess and even attempt to mitigate the risks implicated by the IR's proposed remedies, Apple would need to completely rethink the iOS security, privacy, and performance model and it (and third parties) would incur massive costs in the process. To take one example: architecting a novel sandbox for third-party browser engines would require ground-up analyses of third-party engines with which Apple is not familiar. Third-party vendors would very likely need to substantially re-design their engines to meet iOS security and privacy requirements.

96. Even then, significant risks would remain. Apple and third-party vendors would need to engage in ongoing collaboration to ensure compliance with and improve upon security and privacy protocols and maintain engine functionality. Apple would no longer control the cadence of updates to the

87 IR paragraph 7.27.

88 PurpleSec, "2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends," 2021.

89 See Section B.

browser engines supporting browser apps iOS, which would fragment security updates on iOS, even if limited to "dedicated" browser apps. Guidelines directing developers to implement browser engine updates would not be sufficient to address the issue: even if Apple sanctioned non-compliant developers by removing their apps from the App Store, this would provide no protection for users who have already downloaded and are using the vulnerable apps. iOS also operates under extremely stringent battery performance standards, and browsers using third-party engines can be problematically inefficient.[90] To avoid substantial impacts on battery performance, Apple and third-party vendors would need to undertake comprehensive evaluations of third-party engine performance, which may force substantial changes to the third-party engines. The increased security, privacy, and performance risks and the substantial costs of mitigation measures would constrain Apple from investing in new features and functionalities, diminish the appeal of iOS devices, and increase costs on consumers and developers.

97. The IR's assessment of proposed remedies also ignores its own findings, and the ramifications on user privacy on the web. Worldwide, Blink and the Chrome browser are the dominant market players, far ahead of WebKit and Safari.[91] The IR finds that all surveyed content providers ensure compatibility with Blink-based Chrome,[92] and the CMA has previously found that Chrome is the "UK's most-used web browser."[93] The IR acknowledges that Blink faces limited constraints from smaller browser engines and that, for smaller browser engines "web compatibility is a key barrier to competition" with Blink.[94] Despite these findings, the IR makes no real attempt to address Blink's dominance, nor does it assess the impact on user privacy from failing to take any steps to curb the "Chrome-only" web compatibility advantage,[95] or the Blink advantage more generally. But the implications are clear: not addressing known web compatibility issues would empower web developers worldwide to refuse to make their sites compatible with competing engines and force UK users preferring the privacy features of WebKit or Gecko to choose between diminished privacy protections or being denied access to sites across the web. Far from enhancing competition and diversity of choice, the IR's selective approach would help to secure a privacy-invasive, Chrome and Blink monoculture for the web.

(iii) Apple has the incentive to increase the availability of browsers and web apps on iOS devices

98. The IR is concerned that Apple's requirements in relation to browser engines and its approach to functionality and support for browsers and web apps are aimed at self-preferencing Apple's Safari browser or "protecting" Apple's position in relation to the App Store.[96] These concerns ignore both the incentives that Apple has and Apple's actual conduct.

99. 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. As is clear from the evidence, a greater choice of features and functionality that users desire is key to ensuring the attractiveness of Apple's devices. This includes the availability of alternative browsers and of different methods

90 https://www.laptopmag.com/articles/chrome-tabs-mac-battery-life
91 See: https://gs.statcounter.com/browser-market-share
92 IR paragraph 5.80.
93 Digital Platform Market Study, Appendix E, 4.
94 IR paragraph 5.148.
95 https://www.theverge.com/2018/1/4/16805216/google-chrome-only-sites-internet-explorer-6-web-standards; https://arstechnica.com/gadgets/2019/03/microsofts-new-skype-for-web-client-an-early-taste-of-the-browser-monoculture/; https://arstechnica.com/gadgets/2018/12/the-web-now-belongs-to-google-and-that-should-worry-us-all/
96 See IR paragraphs 5.138 and 5.139.

of engaging with content, including web apps. Apple's approach is, as with all things, bounded by the need to protect security, privacy, and performance. Subject to those overriding requirements, Apple's approach fosters competition in relation to browsers and web apps on iOS in a number of ways.

Apple promotes competition in relation to browser engines and browsers

100. First, WebKit and Safari have pioneered innovation, enhanced user choice, and prompted responses from competitors. For example, in 2005, Safari was the first browser to offer a private browsing mode, which is now ubiquitous. When WebKit introduced ITP In 2017, it was the first engine to block third-party cookies by default and combat privacy-invasive cross-site tracking, and was followed by Mozilla's Enhanced Tracking Prevention (ETP), first announced in 2018 and implemented by default in 2019.[97] In 2021, WebKit followed ITP with Private Click Measurement to meet demand for a privacy-friendly way to measure ad clicks across websites and from iOS apps to websites while still protecting users from being tracked across websites. Despite acknowledging that Gecko likewise implements tracking prevention,[98] the IR fails to recognise that these and other features are borne of robust competition. The second half of the market study must take a more balanced approach to evaluating the existing competition in this area.

101. Second, whilst Safari is pre-installed on iOS devices in order to provide a seamless out-of-the-box experience of 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. On iOS devices, users in the UK 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.

102. In addition, 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 2015, UK users have downloaded alternative browser apps or search-enabled apps from the App Store more than 35 million times on Apple devices, including more than 32 million times on Apple mobile devices. Since the beginning of 2020, UK users have downloaded alternative browser apps or search-enabled apps from the App Store more than 11 million times on Apple devices, including more than 10 million times on Apple mobile devices.

103. Third, Apple allows other browsers to differentiate themselves from Safari and thus offer a real choice for users. WebKit permits for substantial differentiation between browsers, allowing developers to build features and interfaces on top of WebKit, while upholding Apple's stringent privacy and security protections. Other developers control third-party browsers (Google controls Chrome, Mozilla controls Firefox, etc.) and are free to build features into their browsers that are not available in Safari within the constraints of the iOS ecosystem.

104. Indeed, third-party browsers have implemented web platform features on top of the WebKit browser engine to differentiate themselves from Safari. WebKit is an open-source project, which means that any contributor can contribute code. Moreover, developers can enable features on top of WebKit. For example, third-party browser Brave shipped Web Authentication support that

---

97 https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-by-default/; https://blog.mozilla.org/futurereleases/2018/08/30/changing-our-approach-to-anti-tracking/

98 See IR paragraph 5.219.

they built on top of WebKit before it was made broadly available via WebKit. Web Authentication enables the creation and use of strong cryptographic credentials by web applications, for the purpose of strongly authenticating users on specific websites. Similarly, Brave implemented Global Privacy Control (GPC) in 2020, including in its iOS browser, a feature which is not yet available in WebKit. GPC is a web standard that web browsers and websites can use for making and handling online privacy requests. Google's Chrome iOS app also supports Google's Scroll to Text Fragment feature (which allows a link to a specific portion of a web page), even though that feature is not supported by Safari or WebKit at this time.

105. Additionally, browser vendors design application UI features such as tab interfaces, bookmarks, history, downloads, and autofill of saved user information. For example, third-party browser Google Chrome shipped Voice Search and Translation on iOS, which they built on top of WebKit.

106. Finally, Apple has already implemented or is in the process of implementing many of the features and functionality that have been raised as concerns with the CMA, such as Screen orientation functionality, TouchEvents, WebGL 2.0, Media Capture and Stream APIs, File and Directory Entries API, service workers and getUserMedia(). In this respect, Apple cautions that browser quality cannot be measured purely by the length of the browser's list of features or the speed with which new features, many of which are not subject to standardization efforts, are introduced. This is especially true of browser feature development that prioritizes expedience over quality or that involves substantial compromises on performance, privacy, or security. Apple does not therefore consider that the introduction of a feature later in time indicates that the feature was "delayed" or that this results from any intent to reduce or frustrate competition.

107. Rather, Apple implements new features in a way that allows the security, privacy and performance of devices to be preserved; an objectively reasonable approach given the recognition by experts of "*the severe risks of browsers deploying new features without an in-depth evaluation of their security and privacy implications*".[99] The IR uncritically embraces certain "features" as pro-consumer and simply assumes that there are anticompetitive effects from WebKit's decision to refrain from implementing such features until it finds a privacy- and security-preserving method of doing so, rather than acknowledging the legitimate concerns associated with such features. For example, the IR suggests that Web Bluetooth is a "key feature" that WebKit does not support,[100] failing to acknowledge that Gecko does not support Web Bluetooth, that Mozilla has labelled it as "harmful",[101] and that there are legitimate privacy risks associated with such a feature.[102] Apple urges the CMA to take a more balanced approach to assessing competition in the second half of the market study.

Apple promotes competition in relation to web apps

108. Apple has supported web apps 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, it continued to support web apps. In recent years, Apple has added new functionality to WebKit to enable greater features and functionality for web apps. For example:

---

99 See Karami *et al* "*Awakening the Web's Sleeper Agents: Misusing Service Workers for Privacy Leakage*", Network and Distributed Systems Security (NDSS) Symposium 2021.

100 See IR paragraph 5.131.

101 https://mozilla.github.io/standards-positions/#web-bluetooth

102 https://github.com/mozilla/standards-positions/issues/95

- With the introduction of iOS 11 Apple introduced support for Service Workers, a programmable network proxy which has become a critical component for the development of progressive web apps. This is a script a browser can run in the background and does not depend on any particular page in an app being open, which means the web app runs independently of user action, and, most importantly, independently of network connectivity. Service Workers can intercept network requests from the application, control the downloading and caching of content, background synchronization, and perform a variety of other tasks that are not possible with standard web pages.

- Apple has released the Web Authentication API, which allows web apps to access Touch ID and Face ID and use of external security keys for secure user authentication.

- WebRTC allows peer-to-peer communications, including video communications, so that web apps, like web-based video conferencing and streaming game services, do not have to be dependent on a central server and can rely on the peer-to-peer connection.

109. WebKit continues to innovate and respond to demand for features and functionality that improve web apps. For example, WebKit is currently developing the following features:

- Support for small, large, dynamic, and logical new viewport units. WebKit is pioneering this feature to improve web apps' ability to accurately measure the dimensions in which their app can be displayed.
- Support for the HTML dialog element. This tool helps web app developers create overlays, such as prompts, to enhance the display of content and information to the user. Before releasing this feature, WebKit has worked to ensure that it accommodates prevailing accessibility standards.
- Support for Web App Manifest icons and improvements to manifest file fetching. These features support web app interface theme and icon capabilities.

(iv) Implications for the second half of the market study

110. Apple looks forward to engaging further with the CMA with respect to WebKit and to competition in respect of browsers and browser engines. In particular, the second half of the market study will need to test properly the concerns that have been made with respect to security and functionality, and to take proper account of the potential implications of mandating changes to Apple's approach in this respect.

E. Apple's Privacy Initiatives

111. The IR expresses concerns with respect to Apple's privacy initiatives, in particular the distinction between Apple's Personalised Ads prompt and the App Tracking Transparency (ATT) prompt and the impact of the latter on certain developers.[103] It is disappointing that many of these concerns appear to be based on self-serving allegations from data aggregators and social media companies interested in compiling large amounts of personal data from various sources and selling personal data. Apple looks forward to engaging further with the CMA on Apple's efforts to empower users by giving them greater control over how their data is used, in the same manner in which it engages extensively and constructively with the Information Commissioner's Office ("ICO") on our privacy practices and initiatives. In this response, Apple addresses some fundamental misconceptions underpinning, and concerns with respect to, the IR's initial analysis.

(i) There is a clear distinction between Apple's first-party data use and "tracking"

112. Apple's approach to privacy is longstanding and consistent, taking the view that "*Privacy is a fundamental human right".*[104] To protect this right to privacy, Apple has consistently led the industry in educating users with respect to how their data is used and in seeking to empower users to control that use. As Apple sets out in its privacy commitment to users "*Your devices are important to so many parts of your life. What you share from those experiences, and who you share it with, should be up to you. We design Apple products to protect your privacy and give you control over your information.*"[105]

113. A key concern for Apple is the extent to which consumers' data is collected, combined, and mined. Consumers simply do not know and cannot be expected to know about the maze of hidden practices some companies use to collect vast volumes of personal data. Apple continues to try to educate consumers about these data collection practices. For example, it recently published a report titled "A Day in the Life of Your Data," which describes how companies build and harvest extensive data profiles of users through tracking.[106] Apple has also introduced specific measures to empower consumers and provide them with the ability to control the use of their personal data:

- In 2010, some consumers complained about unauthorized exposure of individual, persistent identifiers. To alleviate these concerns, Apple introduced the IDFA, a random device identifier assigned by Apple to a user's device, in 2012. Advertisers use this to track data so they can deliver customized advertising. Following an opt-out mechanism in Settings, by clicking on the "Limit Ad Tracking" button, consumers could indicate to developers that they did not want to be tracked through use of the IDFA.
- In 2013, Apple created a "Reset Advertising Identifier" button to make it easier for users to reset their IDFA.
- In 2016, the Limit Ad Tracking button was enhanced such that when a user enabled it, the value of the IDFA was set to all zeros.
- In 2017, Apple also introduced ITP, which uses on-device machine learning to determine the methods that advertisers use to track users across websites without their knowledge, and then to isolate and purge those tracking cookies that third-party advertisers attempt to store on a user's device without permission. Examples of hidden tracking methods that websites

---

103 See IR paragraphs 6.254, 6.255, and 6.268 to 6.276.

104 https://www.apple.com/privacy/

105 *Ibid*

106 Available at: https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf

can use include social widgets such as Like buttons, Share buttons, and comment fields, which can track users even if they don't click them or use them. With ITP, Safari blocks this tracking by default, provides transparency and control, and asks users if they'd like to allow social widgets to access their identity, giving the user control.

- Apple continued to refine ITP to prevent third-party advertisers from engaging in permission-less, cross-site user tracking and, In 2020, announced ATT user prompts requiring developers to obtain explicit consent from users for cross-developer and cross-app tracking. The ATT prompt requires each developer to ask for user permission to track the user for purposes of targeted advertising or advertising measurement purposes, or sharing with a data broker or to access their devices' Identifier for Advertising (IDFA).

114. Apple has made a conscious decision to place itself at a competitive disadvantage for the sake of consumers' privacy. Apple does ***not*** engage 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.

115. Apple also gives 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 advertising. This choice screen is presented upon launch of the App Store or of Apple Stocks or Apple News in the UK 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.

116. In personalising advertising delivery (when users so choose), Apple relies exclusively on a limited amount of first-party data (i.e., 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).[107] 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.

117. The interests that want less transparency and power in the hands of consumers have sought to compare the Personalised Ads prompt and the ATT prompt. They argue that the differences in the prompt may make it more likely that users will choose to allow Personalised Ads than to allow tracking, thus preferencing Apple. These concerns are unfounded – given the fundamentally different nature of the two, there is no reason to conclude that the choice architecture and prompt wording should be identical.

118. First, as set out above, ATT concerns "tracking" user data across developers (in other words, using third-party data for purposes of advertising), whereas Personalised Ads concerns only the use by Apple of first-party data collected through its own services. There is a real and substantive

[107] As acknowledged at fn 529 of the IR, "*ads on the App Store do not access consumer data from other Apple services like Apple Pay, Maps, Siri, iMessage, and iCloud or data from devices through services and functions such as the Health app, HomeKit, email, contacts, or call history*." Moreover, Apple groups users into anonymised segments of at least 5000 people before ads can be shown to them, to further protect user privacy (IR, para 6.232).

difference between the two, widely recognised in the industry, with the former being considerably more intrusive than the latter.[108]

- As the U.S. Federal Trade Commission noted in a recent report on recommendations for consumer privacy: "*As to the first type of data collection, for the reasons discussed above, if the first party does not share information with third parties or track consumers across third-party websites, the practice would be consistent with the context of the consumer's interaction with the company. Therefore, the framework would not call for a consumer choice mechanism. In contrast, because the second type of data collection involves the transfer of data from one business to another and does not directly involve the consumer (and therefore is typically unknown to the consumer), it is unlikely to be consistent with a transaction or relationship between the consumer and the first party*."[109]
- The Center for Digital Democracy also focused on the distinction between first and third-party tracking, given users have less knowledge about this sort of data gathering and the privacy policy of third-parties: "*Not only is it hard for users to know which data brokers have their information or how they obtained the data, but users also do not have access to the privacy policies of such third parties brokers. Lack of knowledge of third-party privacy policies impedes the individual's ability to meaningfully and knowingly opt-in to this tracking process*."[110]

119. The ATT prompt is designed to increase the user's awareness of when their data will be shared with other companies and allow them to choose whether this is something they want. Indeed, this seeks to address the very concern that the CMA expressed in its digital advertising market study report: "*it is likely that most typical users are unaware of the full extent to which they may be tracked, and are not in a position to make informed decisions or to take actions (including technical measures) that limit tracking. In some cases, users face a choice to either accept tracking or to stop using many services and technologies altogether*."[111] [emphasis added]

120. The ICO opinion to which the IR refers acknowledges this distinction by discussing the distinct legal obligations for first-party data versus when that data is shared with another organization.[112] This is consistent with data protection laws, including the Data Protection Act of 2018, which requires organizations like Apple to be to be at all times responsible for determining the means and purposes of any personal data that it processes. There are separate, additional obligations applicable when a company shares that data with another organization.

121. Second, with respect to ATT, Apple and third parties are subject to the same rules. The only reason Apple does not surface the ATT prompt, which would be the appropriate prompt to compare to third-party ATT prompts, is because Apple does not engage in tracking. Third parties also do not have to surface the ATT prompt when they are relying solely on their own first party data. But Apple goes even further than simply not tracking users, and with respect to Personalised Ads, Apple actually imposes upon itself an obligation to give users even greater choice as to how

---

108 See, for example, https://clearcode.cc/blog/difference-between-first-party-third-partycookies

109 See: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, pg. 44. *See also* https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17., pgs 6-9; pdf; https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf, pgs. 46-49.

110 See: Comment to the FTC from the Center for Digital Democracy (Nov. 16, 2015)

111 https://assets.publishing.service.gov.uk/media/5fe49554e90e0711ffe07d05/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential_WEB.pdf (emphasis added).

112 See: ICO (2021), Data protection and privacy expectations for online advertising proposals, pg. 35.

their data may be used, going beyond that applicable to third parties. In this way, rather than benefitting itself in comparison to others, as the IR assumes, Apple is purposefully placing its ability to use user data at a considerable disadvantage to third parties.

122. If the CMA is keen to ensure "equality" between Apple and third parties in this respect, the logical outcome would be to require that third parties also display a prominent, unavoidable Personalised Ads choice prompt when they seek to use their first-party data for their own advertising services. The alternative reading of the IR's concerns is that Apple would be better placed to engage in tracking activities and then place the ATT screen on front of its users thereby ensuring a race to the bottom in relation to the use of user data. Apple cannot agree with this view and does not consider it likely that this is, in fact, what was contemplated by the IR.

123. Finally, the IR assumes, without evidence, that the stylistic differences between the ATT and Personalized Ads prompts will necessarily account for an unfair divergence in user choice rates. First, this conclusion rests on the tenuous presumption that users must equate cross-company tracking with first-party data use, and therefore any difference in choice must be attributed to presentation style and not substance. Second, and more generally, while it is too early to gauge the full impact of ATT, the evidence does not suggest that the implementation of ATT has materially boosted the performance of Apple's own advertising services.

124. The concerns of the IR are therefore considerably overstated, as a matter of principle, taking issue with important user privacy measures that Apple has introduced to empower users, and they do not support a finding that Apple is engaged in self-preferencing through its privacy measures.

(ii) <u>The harms against which ATT protects users need to be properly taken into account</u>

125. Apple considers it highly relevant that the majority of the concerns identified in the IR appear to be driven in large part by data-harvesting companies like Meta. This is clear from the IR's consideration of the "impact of ATT on developers" at paragraphs 6.268 to 6.273, not the impact on users. Apple recognises that ATT may have a negative impact on data-harvesting activities. However, it is this kind of hidden data collection and tracking activity that causes harm, as recognized by the ICO, and is intended to be addressed by ATT.[113] As Apple has pointed out to the CMA, consumer protection associations and privacy advocates have widely welcomed ATT, and the ICO has given Apple only positive feedback on the introduction of ATT. For example:

- Amnesty International, Human Rights Watch, the Electronic Frontier Foundation and others openly supported and advocated for these changes. The Center for Democracy and Technology applauded the feature, noting that it "*will help rebalance the ecosystem so that data collection and sharing is more transparent and tracking is no longer the default. Systemic change of this breadth is a huge leap forward for consumers*."[114]
- The Mozilla foundation launched an online petition to support the introduction of the ATT prompt: "*Apple's planned implementation of anti-tracking features is a huge victory for consumers, many of whom may not be aware that tracking can be done through their phone's*

[113] A recent Washington Post-Schar poll found that 79% of respondents though tech companies did not provide them with enough control over how their information is tracked and used. This same poll found that only 20% of respondents trusted Facebook to responsibly handle their personal information and data on their internet activity. See, https://www.washingtonpost.com/context/nov-4-22-2021-washington-post-schar-school-tech-poll/1f827037-688f-4030-a3e4-67464014a846/?itid=lk_inline_manual_6.

[114] See, https://www.apple.com/newsroom/2021/01/data-privacy-day-at-apple-improving-transparency-and-empowering-users/

applications. Indeed, a 2019 Mozilla-Ipsos survey found that half of iPhone owners were not even aware of the existence of IDFA and data collection through applications. In addition, those who were aware of their existence did not know how to reset them. Now, with the ability to opt out of tracking directly at the point of use, consumers will no longer have to search through their phone settings to protect their privacy. But first, Apple must implement this change. We need to ensure that the company does not move away from this measure".[115]

126. Developers have also been supportive of ATT, acknowledging its benefit to consumers. For example, Snap has applauded ATT, saying that "*we admire Apple, and we believe they are trying to do the right thing for their customers*" and "*we generally view [ATT] as a good thing overall for consumers, even if it's a little disruptive for advertisers in the near term*."[116]

127. Given the harms specifically being addressed by ATT, the CMA's assessment of its impact on developers cannot simply consider the financial impact and negative effects on their advertising activities and end there. Instead, the CMA must also take due account of the important countervailing benefits that ATT brings to consumers. For example, ATT provides users with the ability to choose to allow tracking on a developer-by-developer basis, encouraging developers to compete on privacy to attract users and gain users' trust. Users have exercised that choice, choosing to allow tracking for some developers at higher rates than others.[117] In the IR, in the few places where the CMA focuses on the effect of Apple's efforts on consumers, it acknowledges the benefit to users, noting in paragraph 6.301 that "*Apple's stated intention with ATT is largely consistent with preserving individuals' privacy and place individuals in control of their personal data.*" Apple would encourage a further analysis of these users' benefits, rather than just a superficial acknowledgment of them, and welcomes a proper assessment of how ATT counters the harm raised by hidden tracking and data-harvesting.

(iii) Implications for the second half of the market study

128. Apple looks forward to engaging further with the CMA with respect to its privacy measures. In particular, the second half of the market study should take due account of the fundamental principles underpinning those measures and the actual potential for such measures to positively impact consumers, bearing in mind, not only the actual impact on developers (and on Apple itself) but also the harms to consumers that Apple is attempting to address.

---

115 https://foundation.mozilla.org/fr/campaigns/apples-anti-tracking-plansiphone/?subscribed=1&utm_source=email&utm_medium=email&utm_campaign=2020advocacyfr&utm_content=appleidfathanks&utm_term=5383151 .

116 https://www.cnbc.com/2021/02/05/snap-ceo-spiegel-says-apples-iphone-privacy-change-is-good-for-consumers.html

117 See, e.g., https://www.cnbc.com/2021/07/22/snap-snap-earnings-q2-2021.html (Snap observed "higher opt-in rates than we are seeing reported generally across the industry due in part to the trust our community has in our products and our business.")

F. Cloud Gaming

129. The IR provisionally finds that "*Apple has used its control over app distribution on iOS to block the emergence of cloud gaming apps on its App Store*", apparently with the intention of increasing barriers to switching away from iOS devices and/or protecting App Store revenues.[118] None of the CMA's findings or concerns are borne out by the evidence.

(i) Apple's approach to cloud gaming is not aimed at blocking the emergence of cloud gaming

130. The App Store was created for native apps (i.e. apps licensed to use Apple's technology and built specifically for iOS, using its code library and able to access iPhone hardware features (camera, GPS, etc)). The App Store has always differentiated between native apps and "apps" that are in effect simply a means of pulling content from the web. This fundamental, technological distinction is central to Apple's curation of the App Store.

131. Apple does not prevent cloud gaming apps from appearing on the App Store, nor is it trying to block the emergence of cloud gaming apps. The App Store has constantly evolved, with new types of apps being created as technology develops. The App Review Guidelines constantly adapt to new technologies and business models, finding ways to allow new apps to appear in the App Store. This is an ongoing process and Apple has worked hard with developers to specifically address the challenges that cloud gaming presents and to allow them to offer game streaming services to users on iOS devices.

132. There are two ways for developers to offer streaming games content to iPhone users:

- The first is through web apps, such as those offered by Facebook, Amazon, Microsoft and, most recently Nvidia.[119] These web apps operate through a web browser and allow users to directly access games via the cloud.
- The second way in which developers can offer streaming games is through a native app on the App Store. Apple has worked with developers to reach a suitable compromise that allows the offering of cloud gaming apps while maintaining adequate protection of consumers. Developers can offer a single catalogue app that links to the App Store product page of each game included in the service. This allows developers to offer their entire gaming catalogue via their streaming app, with users able to select individual games to download directly from that catalogue via a single click.

133. Apple has sought to find ways to bring cloud gaming to its devices in a way that is consistent with its principles that ensure consumers are protected. Apple's device-centric business model is dependent on having each element work together for the performance of the system as a whole. This includes the content available on the App Store.

(ii) Apple's App Store precautions are a valid and objective means of securing its objectives as a platform operator to provide a safe and trusted experience for users

---

118 See IR paragraphs 6.305, 6.336 and 6.337

119 See, for example, https://www.theverge.com/2020/11/19/21573311/nvidia-geforce-now-ios-launch-beta-release-safari-mobile-web-app, noting that "Nvidia is joining its fellow cloud gaming providers in choosing to bypass Apple's App Store and launching a mobile web app version of its GeForce Now service. Nvidia's version is available today in beta form, meaning any of the service's more than 5 million registered users can fire up GeForce Now in mobile Safari on an iPhone or iPad and get playing."

134. Apple's role in relation to cloud gaming apps (or indeed any other type of app) is as the operator of the platform through which they can be accessed. Apple's App Store has a well-deserved and assiduously maintained reputation with consumers as a high-qualify, safe and trusted platform. Maintaining this reputation means that Apple cannot simply disregard the protections built into the ecosystem and allow new types of apps unfettered access to the Apple ecosystem. Apple must analyse how those apps may impact how the App Store functions for consumers and develop a solution that achieves the dual goals of allowing product innovation in the eco-system without undermining the fundamental values and protections valued by consumers.

135. Given the nature of native apps and the way they interact with the features of devices, ensuring the safety and performance of the device and guarding the privacy of users, requires that apps are subject to App Review. From its inception, this requires that, for native apps made available on the App Store, the app functionality is included in the file downloaded to the user's device (i.e. the app "binary") so that the content and functionality can be reviewed. Content and functionality that occurs outside of the app's binary by making calls to remote servers can bypass App Review and change at any time. Therefore, apps that do not really run natively but are simply pulling content or functionality from the web are rejected under App Review, regardless of their nature.[120]

136. The concern with cloud gaming is simple: games are software. Unlike movies or songs, which can be understood as "file types" that are simply executed to access the content, games software can evolve constantly based on user input, how the game is played (multi-player versus single player) and any changes made on the server side. Games may be modified to include objectionable content very rapidly. Without the ability to review an individual game when it is initially offered and when it updates, Apple's curated App Store model would be nullified. Other protections, such as those relating to user-generated content, and consumer protection measures such as Ask to Buy, loot box requirements and compliance with regulatory requirements relating to money gaming, must be performed with respect to each individual game; it is simply not possible to apply them to a "game store" through which multiple games are accessed.

137. Despite the attempts of complainants, such as Microsoft, to frame the cloud gaming issue as a "competition" concern, what it in effect amounts to is a request to allow them to be given unrestricted access to the App Store platform in a way that would bypass the protections and benefits afforded by App Review and is allowed for no other type of app. In so doing, they would increase the risk that users will be exposed to unapproved content and functionality that violates the Guidelines, thereby placing their privacy and security at risk. Furthermore, the controls built into Apple's software that protect user privacy (i.e. permission prompts for sharing personal information with developers) and allow parents to authorize their children's downloads and purchases would not work if apps are executing functionality off-device in the cloud.

---

120 See, for example, Rule 2.5.2 of the App Review Guidelines, which provides "*Apps should be self-contained in their bundles, and may not read or write data outside the designated container area, nor may they download, install, or execute code which introduces or changes features or functionality of the app, including other apps. Educational apps designed to teach, develop, or allow students to test executable code may, in limited circumstances, download code provided that such code is not used for other purposes. Such apps must make the source code provided by the app completely viewable and editable by the user*" and Rule 4.2, which provides "*Your app should include features, content, and UI that elevate it beyond a repackaged website. If your app is not particularly useful, unique, or "app-like," it doesn't belong on the App Store. If your App doesn't provide some sort of lasting entertainment value or adequate utility, it may not be accepted".* Rule 4.2 goes to include specific requirements with respect to app functionality, including that apps should not "*primarily be … web clippings, content aggregators, or a collection of links*".

138. Apple's rules strike a balance between preserving the App Store's essential curation model, and giving developers a clear path to offer app functionality that is not included in the app. Under these, developers can offer their streaming games in individual app binaries. This allows App Review to review the games, including new functionality that must be submitted to App Review for approval. Developers can also offer a single catalogue app that links to the App Store product page of each game included in the service. This model ensures that games offered in a streaming game services are compliant with the Guidelines, and it preserves the experience that App Store users expect in terms of security, parental control (which is particularly important in the context of gaming) and privacy.

139. Further, each game in the catalogue will have its own Store product page (which includes the game's age rating, user reviews, and privacy label), can be located in App Store search, and will be eligible for the App Store's charts and editorial sections (including the Today tab and flowcases).

140. In Apple's view, this approach allows cloud gaming apps to be distributed and discovered through the App Store whilst ensuring that the App Store remains the safe and trusted platform that users have come to expect from Apple and on which all developers (not just those few large developers focused on cloud gaming) can rely.

(iii) <u>The evidence does not support the IR's stated concerns with respect to Apple's approach to cloud gaming</u>

141. The notion proposed in the IR that Apple is seeking to hinder the development of cloud gaming in order to protect its device revenues does not survive scrutiny. Cloud gaming services may be a recent phenomenon but they are rapidly growing and are backed by large and powerful players such as Microsoft, Amazon, Google, Nvidia and others. Recent developments, such as Microsoft's acquisition of Activision Blizzard and Sony's acquisition of Bungie show that these large players are investing millions in developing cloud gaming services. Importantly, they have opted make cloud gaming available as web apps on iOS, taking advantage of functionality in WebKit that Apple has created for developers. Nvidia GeForce, for example, has launched as a web app "*joining its fellow cloud gaming providers in choosing to bypass Apple's App Store*" and has even recently launched a beta test to bring Fortnite back to iOS via a web app.[121] These developments show clearly that cloud gaming apps have not been "blocked" from iOS at all, but are in fact a growing force.

142. Further, the suggestion that Apple may have a policy of "hindering" their development is nonsensical. Even if Apple were to try to "block" native game streaming apps from the App Store, which the IR seems to suggest, this would not hinder their ability to reach consumers. Streaming game services can reach iOS users via gaming web apps. And those users that would prefer to access games via a native app would (as the IR foresees) more likely to switch away from the iPhone to another device. Given Apple's overall position in relation to mobile devices, not to mention the extent of competition from gaming consoles and other devices, it is not feasible that Apple would somehow be able to "hinder their development more broadly" such that this would have an impact on its device revenues. This supposition is entirely unfounded.

[121] See, https://www.theverge.com/2020/11/19/21573311/nvidia-geforce-now-ios-launch-beta-release-safari-mobile-web-app; and https://screenrant.com/fortnite-play-ios-nvidia-geforce-now-guide/#:~:text=In%20order%20to%20play%20Fortnite,a%20paid%20membership%20to%20participate: "*Fortnite has once again found its way back to iOS devices, but this time it's not through the App Store; players can use Nvidia GeForce Now instead*"

143. In fact, far from wanting to "block" such apps, Apple welcomes subscription apps with multiple games on the App Store. It simply requires that they are offered in a manner that provides the requisite protections to users and does not nullify the curation model of the App Store or circumvent the need to pay Apple's lawful commission. Apple has invested billions of dollars in developing the iPhone and the App Store, providing a safe and trusted means for developers to distribute content to users. However, Apple's success in doing so does not render the App Store a charitable endeavour for third parties to exploit however they please on whatever terms they please, no matter how much a small number of self-serving developers might wish this to be the case.

G. Remedies

144. The IR discusses a wide range of potential remedies, from behavioural commitments (such as providing notice of changes to Apple's search algorithm) through to measures that would fundamentally breach Apple's curated ecosystem (such as mandating alternative app stores and browser engines) and separation remedies. As set out in the IR, the intention of the CMA is not to make "*recommendations or advocate[e] any specific interventions at this time*", but instead to set out "*a high-level overview of the potential merits, risks and challenges associated with the potential interventions*".[122] Notwithstanding that caveat, the CMA must still ensure that its conclusions are not based on material errors of fact or irrelevant considerations.

(i) The IR's remedies discussion is premature and ill-founded

145. Apple's key concern with respect to the IR's discussion of potential remedies is, as set out above, that the consideration of these remedies is premature and ill-founded. The IR's assessment is predicated on the need to address concerns that are, in many instances on their face, hypothetical or are based on a one-sided view of the evidence, heavily reliant on untested and self-interested individual developer complaints.

146. To take one example, the IR's consideration of various separation remedies (most likely data or operational separation, but potentially even going so far as structural separation) to address the concern that Apple is "*in many cases … both the rule maker and the referee for app markets in which [it itself competes] and [has] the ability and incentive to provide an unfair advantage to [its] own apps*".[123] Underpinning the consideration of these draconian remedies is the conclusion that Apple's app review process "*creates uncertainty, costs and delays for app developers. This in turn is liable to hinder innovation and may be used to the advantage of Apple's own apps*".[124] As Apple has already demonstrated, and sets out further in this response, Apple's incentives are to increase the number and range of high-quality apps available on the App Store and it has it has never been Apple's policy to disadvantage third-party developers, through delays to approval or any other means.

147. Even aside from this, it is clear from the IR that the evidence base cannot under any reasonable interpretation be considered sufficient to warrant such potentially intrusive measures:

- First, the conclusion ignores entirely the contrary evidence of app developers cited above that "*Apple's stewardship of its ecosystem, in particular through app review processes … helps to create consumer confidence and trust, which is vital for small start-ups and unknown brands*", as indeed does the discussion of the potential separation remedies.
- Second, the concerns on which the above conclusion are based come from "*the majority of developers that we requested information from"*;[125] in other words, potentially no more than about 50 developers out of the 500,000 or so app developers in the UK. Whilst Apple does not suggest that universal agreement would be needed before the CMA could identify a potential harm to be remedied, it cannot seriously be argued that complaints from a handful out of hundreds of thousands of app developers amounts to a reasonable evidence base.
- Third, even those limited concerns have not been investigated to the extent that would be necessary to ground remedies of this nature. Even if the app review process does result in

122 IR paragraph 7.3.
123 IR paragraph 7.107.
124 IR paragraph 6.77.
125 IR paragraph 6.60.

costs and delays for some app developers, this is most likely to be with respect to developers that attempt to circumvent the rules, or that have apps with problems that need to be addressed before they can be safely offered to users. Further, the CMA has not examined or tested the seriousness of any costs or delays or the extent to which they actually could hinder innovation. In the absence of any demonstration of harm, it is hard to see how any remedies, let alone separation remedies, could be justified.

148. By engaging in such a one-sided approach, the CMA risks putting in place (or at least paving the way for) interventions that are manifestly unnecessary and disproportionate in practice and that risk harming competition, privacy and consumers in ways which the CMA has failed to investigate.

149. This risk has already been highlighted to the CMA in the comments on the statement of scope document submitted by ACT The App Association, which noted that the CMA's categories for intervention "*indicate that the CMA is proposing 'solutions' before identifying the problem. In a system as complex as the app ecosystem, such an approach is very risky and suggests a possible unbalance in the results of the study*"[126] and Developers Alliance which expressed that it was "*disappointed to see that the investigative phase of the study … anticipates harm*" and that "*the focus on market power versus the anti-competitive exercise of market power risks intervention where there is no evidence of harm*"[127]. Apple highlights, in this respect, two key risks with potential interventions discussed in the IR, namely the risk of interventions that inadvertently reduce consumer choice and competition and the risk of disproportionate interventions.

(ii) Risk of potential remedies causing greater harm to consumer choice and competition

150. The sections above also set out the importance for the second half of the market study to take due account of the tight integration between elements of Apple's ecosystem. This is particularly important with respect to remedies that could require significant changes to those elements, such as remedies mandating alternative app stores (or in the alternative, sideloading), alternative payment processing methods, and/or alternative browser engines to be allowed on iOS.

151. Section B explains how Apple's products are differentiated in terms of quality, performance (including features and functionality), security and privacy. These are key drivers of consumer choice and are well recognised as reasons why many users choose Apple devices over Android. Sections D to F highlight the key roles that elements of the ecosystem, such as the curated app store, IAP functionality and WebKit, are central to Apple's overall efforts to ensure that its devices offer the highest levels of performance, security and privacy protection. They also refer to third-party studies demonstrating that Apple devices perform markedly better than Android devices in terms of protection from malware.

152. The IR's discussion of remedies, however, takes a piecemeal approach to issues, asking whether individual remedies could be imposed with "adequate safeguards" in order to foster competition within specific areas of the Apple ecosystem (such as browser engines or app stores). This piecemeal approach runs counter to the IR's own recognition that remedies which are designed to "*allow more choice or competition within an ecosystem could in principle result in weaker protection for the security of users' mobile devices. This may be a particular concern where security*

[126] Available at: https://assets.publishing.service.gov.uk/media/617aa2198fa8f529834949d7/ACT_The_App_Association.pdf

[127] Available at: https://assets.publishing.service.gov.uk/media/617aa2d0e90e07198018fa28/Developers_Alliance.pdf

is optimised across the ecosystem, and where changes in one part of the ecosystem could therefore have an adverse effect on the integrity of the system more generally" [emphasis added].[128]

153. Indeed, Apple stresses that, in recognising this fact, the IR has put its finger on the most significant problem with these proposed remedies. Measures that reduce the security or privacy protections in a single area have repercussions across the whole ecosystem. For instance, a security breach brought about through an app downloaded from a store with inadequate review could impact, not only on that app but on other apps, on the performance of the device as a whole, and even on other devices that connect with the infected device. The same goes for malware introduced to a device through a third-party browser engine. In this way, measures that negatively impact security or privacy protections in a single area would result in the level of performance and protection offered by Apple being reduced to that offered by the least secure alternative introduced into the system.

154. Effectively, what this would mean is that Apple would be in the same position from a device performance, security and privacy stance as Android. The competitive differentiation between the two ecosystems would be essentially removed. Thus, whilst the remedy would, on the one hand, seek to increase choice within the Apple ecosystem for a given area, it would, on the other hand, destroy the competition currently existing between the Apple ecosystem and the Android ecosystem. Wider consumer choice would be reduced, as would the important competition that exists between ecosystems. The harm from this is obvious, not least as consumers that want to have a choice within an ecosystem are already catered for (and would remain so), whereas those that prefer to choose on the basis of the overall performance and quality of the ecosystem would lose that choice.

(iii) Risk of disproportionate interventions

155. Apple considers that there is a significant risk that remedies could be disproportionate to the actual competitive and consumer impact of Apple's conduct. This is particularly the case when the CMA relies on a very limited evidence base of negative and self-serving developer comments (particularly those of recognised Apple detractors) to the exclusion of positive evidence in order to ground concerns. Clearly, the more intrusive the remedy being considered and the wider the impact that the remedy could have, the stronger the evidence base underpinning the need for the remedy must be. However, as set out above, in respect of concerns such as those relating to app review, the evidence base set out in the IR is weak.

156. In contrast, the potential remedies include separation measures to keep app review isolated from app development. Such remedies would have an inordinately burdensome impact on Apple and the organisation of its business. As Apple has previously explained, its 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.[129] 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. It is clear from the IR that there is insufficient evidence of harm to warrant such extraordinarily burdensome remedies.

157. Further, it goes without saying that the global nature of Apple's business is an important factor to be taken into account. Apple's ecosystem operates on a centrally-run, worldwide basis. Remedies imposed by the CMA will not just affect the UK, but will be felt globally. Again, the potential for

[128] IR paragraph 7.27

[129] See https://hbr.org/2020/11/how-apple-is-organized-for-innovation

remedies to have such a wide-ranging impact indicates that a particularly strong evidence base would be required in order to avoid a disproportionate impact.

****