22 July 2022

MOBILE ECOSYSTEMS MARKET STUDY
APPLE RESPONSE TO CMA CONSULTATION ON MARKET INVESTIGATION REFERENCE PROPOSAL FOR MOBILE BROWSERS AND CLOUD GAMING

Apple's approach to mobile browsers and cloud gaming is no different than its approach with respect to all other elements of the iOS experience; that is to offer as wide as feasible a choice of features and functionality that users desire, thus ensuring the attractiveness of Apple's devices. As a result, whilst bounded by the need to protect security, privacy, and performance, Apple's approach is to foster competition in relation to browsers, web apps and gaming apps on iOS.

The evidence shows that, with respect to mobile browsers, WebKit and Safari have pioneered innovation, enhanced user choice, and prompted responses from competitors. Further, Apple does not restrict users' ability to download and use alternative browser apps, nor does it prevent other browsers from differentiating themselves from Safari. Apple implements new features for WebKit on iOS 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*".[1]

With respect to cloud gaming, 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. On the contrary, Apple has worked with developers specifically to allow them to offer cloud gaming apps, whilst maintaining adequate protection for consumers. Developers can, in fact, 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. Apple's approach strikes 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.

Despite this, the CMA has identified in its final report a number of "features" of the market that it proposes are sufficient to warrant the opening of a market investigation. Apple considers that the findings underpinning this proposal are based on a partial and erroneous analysis of the evidence submitted to the CMA during the market study. It further considers that the CMA's analysis of competition in the relevant markets is inappropriately narrow and excludes important aspects. In particular, in Apple's view the CMA has failed to consider privacy as a parameter of competition at the ecosystem level as well as the value consumers place on WebKit's unique privacy features. More generally, the CMA has failed to engage properly with the substantial body of objective technical evidence which Apple has submitted, including following publication of the CMA's interim report and Apple's comments thereon.

Apple considers that a balanced review of the evidence would lead to the conclusion that competition with respect to both mobile browsers and cloud gaming is robust and that, in particular, Apple's approach provides users with a valuable choice, centred on security, privacy and performance, between ecosystems. The potential remedies under contemplation by the CMA risk removing this choice and thus actively restricting competition at an ecosystem level. Any action that would result in such a loss of consumer choice and competition should be avoided.

In light of the above, and for the reasons explained in further detail below, Apple is strongly of the view that opening a market investigation would be neither necessary nor appropriate in relation to either mobile browsers or cloud gaming. Apple's response addresses the questions posed by the CMA in its consultation document, dealing separately with each of mobile browsers and cloud gaming.

---

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

A. Mobile Browsers

Question 1 - Do you consider that our analysis is correct with respect to the suspected features of concern in the supply of mobile browsers in the UK?

1. The CMA has identified a number of "features" which it considers give reasonable grounds for suspecting an adverse effect on competition in relation to mobile browsers. The paragraphs below address the features identified by the CMA, and show that, in reaching its findings, the CMA has misinterpreted and/or ignored objective evidence submitted by Apple.

The WebKit requirement does not inhibit competition between mobile browsers on iOS but rather drives competition through its opensource model

2. Apple considers that the CMA has either ignored or failed to take properly into account the considerable body of evidence it has submitted which together shows that WebKit and the wider iOS ecosystem fosters competition between alternative mobile browsers, as well as from web apps.

3. First, Apple has submitted evidence demonstrating that it has a clear track record of fostering and promoting the usage of web apps in response to developer demand, since the launch of the iPhone in 2007. In the last decade, Apple has made substantial investments in WebKit to enable powerful new functionality for web apps, with much of this investment spurred by contributions from developers and other stakeholders. Apple has drawn on input from a diverse array of engineering functions and has also made relevant investments in infrastructure, and supporting hardware and software. This includes support for Service Workers, the release of Web Authentication API and the introduction of WebRTC, which allows peer-to-peer communications.[2] Apple is continually developing new features for WebKit, demonstrating that it is sensitive to developer demands, including increased support for viewpoint units, the HTML dialog element, and Web App Manifest Icons. A further example of such innovation is Apple's recent announcement at WWDC that Web Push will launch on macOS Ventura and as part of iOS 16 in 2023. Apple's clear aim through the actions outlined above is to ensure that developers have the tools to provide iOS users with high quality experiences on web apps and that such experiences are on par with those available through native apps, in line with iOS users' expectations. Apple continues to think of ways to add greater functionality to web apps in a way that will encourage web app development as a credible option for developers.

4. Second, WebKit empowers developers to build features on top of WebKit to differentiate their browsers. This has engendered competition as developers have implemented numerous new features to differentiate their offering from Safari, such as Brave, which pioneered the use of WebAuthentication and Global Privacy Control. Another means by which vendors can and do differentiate their offerings is through design application UI features. An example of this is Google Chrome, which is shipped with Voice Search and Translation on iOS.

---

[2] Furthermore, Apple has provided detail on the large number of the web platform features pioneered in WebKit, including Private Click Measurement, SVG Fonts; HEVC/H.265 video format; HTTP Life Streaming (HLS); JPEG 2000 image format; AudioTrackList and VideoTrack List APIs for examination of media tracks; CSS filter() function; CSS color() function; CSS hanging-punctuation; Advanced :nth-child and :nth-last-child syntax from CSS Selectors Level 4; ui-serif, ui-sans-serif, ui-mnospace, and ui-rounded values for font-family from CSS Fonts Module Level 4; full support for CSS Multi-column Layout Module Level 1; and full support for Clipboard API.

(Cont'd on next page)

5. Apple has also presented clear evidence showing that users can choose among a range of attractive browsers on iOS. 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.[3] As such, Apple considers that objective evidence about the wealth of browser options available to iPhone users demonstrates that the barriers to entry faced by developers of new browsers are not significant.

6. In addition, Apple's position has always been to maintain WebKit as an open-source project and invite contributions to the project. WebKit began as a volunteer-supported community project, benefitting from input from thousands of contributors from a range of organisations, and it has been adopted by a range of vendors to render web content. Apple has also expended considerable effort to expand and support the project. Apple does not unilaterally dictate the features supported by the project, nor does it dictate which features ship on third-party ports of WebKit or WebKit-based browsers.

The CMA fails to take due account of the substantial body of relevant evidence which demonstrates Apple's ecosystem has 'best in class' privacy and security features

7. The CMA effectively ignores Apple's focus on the privacy-enhancing features of the iOS browsing experience, the pro-competitive differentiation of privacy-enhanced browsing on iOS, and the best-in-class privacy features available via WebKit. As Apple has noted previously, WebKit has been the leader in privacy features for browsers, since the introduction of Private Browsing mode in 2005, and through Intelligent Tracking Prevention and Private Click Measurement in 2017 and 2021, respectively. These pioneering innovations are borne of robust competition at the ecosystem level, which have benefited users and prompted an increased focus on similar features from competitors.

8. WebKit employs a suite of other technologies and strategies to defend user privacy, including storage and Service Worker partitioning, 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.

9. The CMA also fails to consider properly the evidence submitted by Apple explaining that for objective technical reasons the unique security benefits of WebKit's integration within the iOS ecosystem cannot be replicated by third parties. Apple has previously explained that WebKit's integration within iOS is a means to address the inherent security vulnerability which arises from the need for users to have the ability to surf the web on its devices. As outlined in Apple's previous responses, this integrated approach allows WebKit to utilize a number of effective security processes, including (1) a more robust sandbox functionality built on a decade's worth of security improvements and knowledge; (2) the ability to ship security updates for WebKit in a single, uniform approach that minimizes security vulnerabilities and prevents a long tail of unpatched apps; and (3) protections against vulnerabilities posed by the Just-in-Time compiler. Apple notes that WebKit's integration is a key pillar underlying its competitive differentiation on security and privacy, which is a key driver of consumer choice. As Apple has stated previously, this is a core

[3] Additionally, Bing Search, Yahoo Search, Ecosia, Quant, Start Page, and Google Search are all search-enabled apps that allow users to browse the web.

feature which consumers value: survey data shows that for users, security and privacy is one of the top three reasons for purchasing an iPhone.

10. Apple has also already explained at length that certain security functionalities would be extremely difficult to enable outside of the WebKit browser engine, including for example, how iOS implements PACs to secure system services like WebKit. Because Apple only conducts updates for PAC (which are frequent because this is still developing technology) for first-party services, this would mean that any time it deploys a PAC enhancement, it would render all third-party apps using PAC inoperable until they updated, which would be an unacceptable experience for users. As for sandboxing, it is unfeasible as a technical matter for Apple to tailor and continuously update a custom sandbox for third-party browser engines with which it is completely unfamiliar. Apple does not have a basis to understand the sets of system components that third-party developers would need, which would require Apple and third-party developers to expend significant resources and commit to an ongoing collaboration in order for this to be feasible.

11. Moreover, the use of different browser-rendering engines on iOS would make a rapid, efficient response to a privacy or security vulnerability in one browser impossible. Whilst WebKit allows Apple to distribute important security updates to all apps in a single update, other platforms permit apps to embed different versions of their browser engines. As a result, apps may be allowed to continue using outdated embedded browser engine versions many months, or more, after security patches and fixes have been released by the browser engine vendor. This kind of fragmented approach to browser security and privacy would leave iPhone users at the mercy of the browser's developers, who may fail to adequately address a system vulnerability, or decide to stop maintenance altogether. Guidelines establishing the principle that developers should implement browser engine updates in a timely way would not be sufficient to address vulnerabilities: 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 vulnerable apps.

12. Apple provides all browser developers with access to WebKit so that they can leverage Apple's industry-leading privacy and security safeguards and innovations in their offerings, helping to ensure that users are protected no matter what browser they choose to use on their iOS device.

13. The CMA has also failed to engage properly with Apple's technical submissions explaining that it would be very difficult for it to assess on an *ex ante* basis whether other browser engines meet Apple's privacy standard and performance standards. This is because browser engines are exponentially more complicated than native apps as they are not bounded to narrowly defined applications, and as a result it is not possible to review for every potential security and privacy threat posed by millions of web pages that are not controlled by the developer of the browser engine. Further, browser developers may expose latent vulnerabilities in a browser engine's code by failing to timely or competently ship updates, or worse, by intentionally creating "back doors" that evade review and facilitate remote code execution attacks by malicious web sites.

14. In short, WebKit is the most effective means for Apple to help ensure the security of iOS devices, which has proven effective for over a decade. Apple expends significant efforts and resources to make WebKit the safest experience possible and protect consumers despite not knowing what websites they may then access. Introducing different browser engines would introduce additional unknown risks and challenges and thus increase the overall vulnerability of the ecosystem.

15. Apple also has specific concerns about the relevance and robustness of a number of pieces of evidence which the CMA has relied on in reaching its conclusions in this context:

- First, the CMA relies on defective quantitative evidence in order to compare the security of the Android and Apple systems. The CMA recognises that such evidence, which is presented in Appendix F, may reflect no more than attacker preference (as more attacks will by necessity lead to more efforts to fix issues and provide updates) rather than the actual quality of the security safeguards put in place upfront. Notwithstanding this fundamental limitation, which effectively renders such evidence of no probative value, the CMA still relies on this evidence as a basis to say that Apple's browser engine is "*not demonstrably more secure*". The CMA's apparent position to justify this approach is simply that there is "*no way to effectively measure*" how many vulnerabilities affect software. Given that Apple has presented multiple third-party sources showing that Android's ecosystem suffers issues at an order of magnitude higher than those which affect iOS, Apple strenuously disagrees.

- Second, the CMA has been unwilling to provide Apple any of the analysis underlying the various security expert opinions which it cites in support of its findings in the final report. In Apple's view, as a procedural matter it should have been provided with an opportunity to test and scrutinise that analysis as part of the information gathering stage of the CMA's investigation. The CMA's failure to provide such an opportunity undermines Apple's ability to engage meaningfully with CMA findings and conclusions which rely in part on that evidence. Moreover, Apple is concerned as a matter of substance that the CMA has placed reliance on expert opinions which may be based on an inappropriate methodology or inaccurate, irrelevant and/or partial information.

- Third, the CMA has reached its findings in relation to WebKit at least in part by relying on irrelevant and misleading comparisons between iOS and macOS, which are two separate OSs with completely different functionalities. Apple has explained in detail that iOS must be considerably more secure and reliable than macOS, given the significantly increased security and privacy risks which arise from the fact that smartphone devices contain more highly sensitive personal information (including financial, health, and location information) and are more likely to be misplaced or stolen. This specific context dictated Apple's design choices, including its decision to develop iOS on the basis of certain security principles such as centralized App Distribution, App Review, Sandboxing, and Entitlements. Apple considers that it is entirely inappropriate for the CMA to assess aspects of iOS which are specifically intended to address security challenges (such as the presence of the WebKit requirement) by reference to its approach to macOS, where the same challenges do not arise.

The CMA's finding that Apple uses defaults and choice architecture to 'self-preference' its own apps is contradicted by Apple's incentives as a device manufacturer

16. Apple is concerned that the CMA is assessing Apple's legitimate and pro-competitive approach to defaults and choice architecture by reference to a vague and potentially inappropriate approach to defining 'self-preferencing' behaviour. Apple has submitted previously that, as a manufacturer of high-end devices, it has always been focussed on delivering a premium consumer experience out of the box in line with users' expectations for such devices. Indeed, given the primacy of device sales to Apple's business model, it is economically rational for Apple to offer a high-quality and varied app ecosystem – including both integrated Apple apps and third-party apps – in order to maintain and increase the demand for Apple devices.

17. Apple has also explained that users are empowered to delete or change certain default settings and pre-installed apps, with users further enabled by various tools that aid switching. Since the release of iOS 10, users have had the ability to delete the limited number of Apple pre-installed

apps[4] and since iOS 14 they have also been empowered to change defaults for browser and mail client. Apple has submitted that it and third parties provide seamless tools to enable switching of default mail and browser apps, with this supported by objective data demonstrating that a very significant number of users do in fact download and use alternative browser and mail apps.[5]

18. Against this backdrop, the CMA has not provided any objective framework for identifying and assessing 'self-preferencing' conduct. Instead, the CMA's current approach, which finds Apple's conduct 'may' or 'could' lead to such harm based on a vague and superficial analysis of the behavioural economics literature, represents a material departure from the CMA's normal empirical approach. Such an approach effectively allows the CMA to identify any Apple conduct as potentially harmful and gives rise to a significant risk of false-positives, particularly in light of the clear and strong pro-competitive rationale for Apple's approach, as set out above.

Question 2 - Do you consider that our analysis is correct with respect to the reference test being met in relation to the supply of mobile browsers in the UK?

19. For the reasons set out in Apple's response to Question 1 above, the CMA's analysis with respect to the 'features' of the mobile browsers market is not well founded. This means the legal test for a market investigation reference with respect to mobile browsers is not met.

20. In reality, the mobile browsers market in the UK is characterised by positive outcomes for developers and users, driven by intense competition at the mobile ecosystem level, as explained further below.

Apple has invested heavily in innovation to maintain its key areas of differentiation, leading to high levels of user satisfaction and a constant stream of new technologies

21. Since launching the iPhone in 2007, Apple has invested significantly in innovation and has made many enhancements that have dramatically improved the processing speed, functionality and quality of its iOS ecosystem. 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.

22. 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 protections. Apple must constantly innovate or risk losing customers to its highly motivated competitors. Indeed, in the markets where Apple competes it is typically one of the smaller players. This is one of primary reasons that Apple has expended between $15-20 billion over the last 3 years on R&D.

23. Apple investments have specifically promoted competition in relation to browser engines and browsers. 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. In 2017, WebKit introduced Intelligent Tracking

[4] Over two thirds (26 of the 40) of Apple pre-installed native apps can be deleted by users.

[5] 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.

Prevention to limit cross-site tracking, a feature that was subsequently adopted by Mozilla's Gecko engine. Apple has also pioneered a number of privacy initiatives (which do not preference Apple over third-party apps), such as Personalised Ads and App Tracking Transparency (ATT) prompts, empowering individuals and enhancing user control over their data on Apple devices. Every year, Apple offers new features, innovations and performance enhancements to ensure Safari remains an attractive browser choice for its iOS users. Examples of significant innovations Apple has made to the Safari browser include Start Page, Translation, Automatic Strong Passwords, AutoFill, Reader mode, and Private Browsing.

24. That Apple's competitive strategy has delivered consistently positive outcomes is apparent from objective evidence showing extremely high levels of user satisfaction and the huge array of new technologies which it has pioneered, many of which it has made publicly available. Users have benefitted as the quality of mobile devices has increased, with survey evidence indicating that users consider Apple's devices to be of a higher quality than those of other manufacturers and that iOS users are generally more satisfied with their devices than users of other brands. For example, a survey by Engine reported that Apple was the only phone brand making it into the list of the top 10 best brands in the UK for customer service experience in 2018. A key example of the important technology which Apple has developed and made available publicly is the huge catalogue of more than 150,000 APIs that allow developers to unlock the potential of Apple's proprietary technologies. This means that each app made available through the App Store is built on the basis of innovations originating from Apple.

Apple's privacy and security-focussed vertically integrated iOS model competes vigorously against Android's more open and diverse advertising-led model, providing users with a choice of what OS they prefer for mobile devices

25. Apple is in direct and fierce competition with Samsung, Google, Huawei and many others on a global basis. 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.

26. As a result of its efforts, 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%).[6]

27. Apple's approach to security and privacy — a key component being the WebKit requirement — is a vital competitive parameter and driver of consumer choice in this respect. Apple has explained that the high value consumers place on security and privacy reflects the fact that 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. The CMA recognises this during the Market Study, noting 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*".[7] In this context, it is clear that users who purchase iPhones will rely on its industry-leading security and privacy efforts. Indeed, the threat to users of malware and other cyber-attacks is very real and, as noted above, experts have concluded that if Apple were to loosen its current safeguards for mobile browsers this would lead to "severe risks" to users, with Apple experts also testifying in court to

6 Final report, paragraph 3.52.

7 See final report, paragraphs 2.1 and 2.2.

the same effect. Apple further considers that users' active engagement with its privacy initiatives such as ATT indicate that privacy is a driver of user decisions not only within the ecosystem but also more generally when choosing a device. Consistent with the above, survey data shows that for users, security and privacy is one of the top three reasons for purchasing an iPhone.[8] Further, Apple considers that it is reasonable to expect that the value consumers place on privacy will increase in future as a result of increasingly common privacy initiatives across the industry, which aim to educate and empower users in order to counter invasive practices, many of which currently occur without user knowledge or consent.

The CMA's approach risks turning Apple into a replica of Android, thereby reducing choice for users and dampening competition between the Apple and Google mobile ecosystems

28. The evidence shows that Apple's approach to security and privacy offers consumers a clear alternative to the Android system, providing them with a real choice across these 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.

29. Apple has previously articulated in detail that measures which 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 exploits 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.

30. By taking issue with the WebKit requirement, which is central to Apple's approach to security and privacy, the CMA risks placing Apple 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 and wider consumer choice would be reduced. 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.

31. In addition, a decrease in security and privacy at the ecosystem level would have significant adverse ramifications for the app economy. Users who are worried about their security and privacy are more likely to download fewer apps or to delete apps. A less secure ecosystem, in which users do not feel safe downloading apps, could mean users are less likely to try out innovative new apps or take a chance on apps coming from new or lesser-known developers. This could blunt the growth of the app economy, further harming developers and further depriving users of choice.

Question 3 - Do you agree with our proposal to exercise the CMA's discretion to make a reference in relation to the supply of mobile browsers in the UK?

32. Apple considers that it is apparent from the evidence before the CMA that the necessary basis for making a reference is not present in relation to mobile browsers. The factors to be taken into

[8] See final report, paragraph 3.51 and footnote 104.

account by the CMA when considering whether to exercise its discretion to make a reference are therefore not triggered.

33. In any event, it is clear that, since there is already effective competition within the mobile browser market, there are no adverse effects on competition, let alone at a scale to warrant a reference. Specifically with respect to the mobile browser market, users who choose iOS as an operating system find an innovative browser landscape on iOS with all leading mobile browsers delivering browsers that are compatible with the App Store Guidelines, and new web browsers and new features for web browsers appearing over time.

34. Further, if the CMA continues to consider that Apple's conduct and, in particular, the requirement to use WebKit as the sole browser engine for iOS devices prevents, restricts or distorts competition, then it would be more appropriate for the CMA to open a Chapter 2 antitrust investigation under CA98. Apple has already engaged in an in-depth market study investigation, submitting detailed evidence to the CMA regarding WebKit and Safari. As set out above, Apple considers that the CMA's assessment of this evidence is significantly flawed. Given the potentially significant remedies that could be imposed, it is vital that any final findings are supported by a high degree of precision and expertise. Apple considers that, in this context, it is necessary for it to have the maximum opportunity to review and scrutinise the evidence within the CMA's file and to be presented with the possibility of an effective appeal at the end of the process; opportunities and rights which would be best protected in the context of a formal antitrust investigation.

Question 4 - Do you consider that the proposed scope of the reference, as set out in the draft terms of the reference published alongside this document, would be sufficient to enable any adverse effect on competition (or any resulting or likely detrimental effects on customers) caused by the features referred to above to be effectively and comprehensively remedied?

35. For the reasons set out above in response to Questions 1 and 2, Apple considers that the CMA's findings with respect to the suspected 'features' of the market for mobile browsers which the CMA has identified are not well-founded and as such it is neither necessary nor appropriate for the CMA to intervene in that market.

Question 5 - Do you have any views on our current thinking on the types of remedies that a MIR could consider (see above and Chapter 8 of the market study final report)? Are there other measures we should consider?

36. For the reasons already set out above in response to Question 3, Apple's view is that the CMA's potential interventions for mobile browsers would be unnecessary, disproportionate, and would give rise to the significant unintended consequence of undermining the current effective state of competition between iOS and Android at the ecosystem level, thereby harming users and developers.

37. The CMA also fails to take into account the potential harm to consumers arising from the increased risk of security and privacy breaches that would likely result from the CMA's proposed interventions. Apple considers that this harm must be assessed against any gains which the CMA considers could be derived from its proposed remedies.

38. Further, in light of the clear security, privacy and performance benefits of the WebKit requirement, any potential positive effects from alternative browser engines running on iOS would necessarily be marginal at best and would be significantly outweighed by the increased risks of security breaches and the costs that would likely need to be borne by Apple (and developers) of implementing additional measures to address those risks.

Question 6 - Do you have any views on areas where we should undertake further analysis or gather further evidence as part of an MIR in relation to the supply of mobile browsers?

39. For the reasons set out above, Apple considers that the reference test is not met with respect to mobile browsers and that it is not appropriate to make a reference.

40. For completeness and, without prejudice to the above, if the CMA were to make a reference in relation to mobile browsers, then it would be critical for the CMA to conduct further analysis to properly understand:

- The significant level of browser differentiation enabled by WebKit.
- The ease of transferring mobile browsers from other mobile browser engines (e.g. Blink, Gecko) to WebKit.
- The lack of material barriers to new mobile browser entry.
- Safari's performance compared to other browsers on aspects other than speed.
- The unique effectiveness of WebKit's integrated security features to help make iOS the most secure platform against malware infections and other risks.

B. Cloud Gaming

Question 1 - Do you consider that our analysis is correct with respect to the suspected features of concern in the supply of cloud gaming in the UK?

41. The CMA has identified one sole "feature" of cloud gaming, namely Apple's security-based requirements, which it considers give reasonable grounds for suspecting an adverse effect on competition in relation to cloud gaming. The paragraphs below address the CMA's analysis, and show that, in reaching its conclusion, the CMA has misinterpreted and/or ignored objective evidence submitted by Apple.

Objective evidence shows that, rather than "blocking" or "hindering" cloud gaming, Apple has taken active steps to encourage cloud gaming apps

42. 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. As Apple has previously explained, it has worked hard with developers to specifically address the challenges that cloud gaming presents and, in fact, does allow them to offer game streaming services to users on iOS devices.

43. Apple currently provides developers with two options for offering cloud gaming to iPhone users: (i) web apps, which enable developers to take advantage of functionality in WebKit that Apple has created, as discussed above; and (ii) through native apps on the App Store. As noted above, developers can offer a single catalogue app that links to the App Store product page of each game included in the service.

44. With respect to web apps, Apple places no additional or special restrictions on cloud gaming web apps, as security or privacy issues are adequately addressed through the safeguards embedded within WebKit. Apple stresses that Facebook, Amazon, Microsoft and Nvidia would not have opted to offer cloud gaming via web apps unless they considered that the underlying technology and the access to this technology provided by Apple was sufficient to enable them to provide a competitive user experience.

45. With respect to native cloud gaming apps, Apple applies the App Store Guidelines to ensure that such apps are discoverable in the most effective way, being: (i) through the main search channels in the App Store; and (ii) in a way that makes available the key information relevant to the user decision. Specifically, this approach ensures that each game will have its own App 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 showcases).

46. In each case, Apple's approach is consistent with its principles that ensure consumers are protected and its desire to maintain its reputation with consumers as a high-qualify, safe and trusted platform.

47. Given that cloud gaming services can reach iOS users via several channels on iOS devices, it is implausible that Apple is trying to (let alone succeeding in a strategy to) "block" cloud gaming. Further, 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 harm the development of cloud gaming more generally.

48. The CMA relies on isolated internal documents in an attempt to support its findings that Apple identified cloud gaming apps as a threat, despite the fact that the wider evidence base contradicts this — primarily that cloud gaming apps are permitted on the App Store. In presenting these documents, the CMA makes no attempt to provide relevant contextual information for such documents (including that they simply represent the views of individual staff, rather than Apple corporate policy). They are thus of little to no probative value and at the very least it is clear that they are outweighed by the significant body of evidence which Apple has provided showing that it has taken active steps to facilitate cloud gaming on its devices.

49. The CMA also fails to consider its own findings showing that web apps are suitable to support cloud gaming, given their enhanced functionality and efficiency. The CMA cites evidence showing that cloud gaming service providers consider that the ability to offer cloud gaming via web apps lowers barriers to entry and expansion. In particular, it states that web apps could lead to lower development and maintenance costs for developers and grant them the ability to offer a consistent user experience across different platforms, which the CMA notes "*could enable content providers to make their content available to a potentially much larger user base*." The material positive impacts on competition derived from these features of web apps do not appear to have been given proper weight by the CMA in its findings.

The CMA fails to engage with the objective evidence Apple has provided explaining why cloud gaming apps must be subject to the full scrutiny of the standard app review process

50. The CMA's assessment of Apple's security and privacy focussed approach to providing access to cloud gaming is subject to a number of significant limitations.

51. First, Apple has explained at length that games must be subject to individual App Review because this is the only way to ensure that the App Store protections that Apple provides to customers in relation to software applications can apply to those games. Apple's iOS prevents apps from accessing device user and sensor data, including location, contacts, and photos, without asking for and obtaining the user's explicit permission. Apple's Screen Time features allows parents to manage the apps on their children's devices, including by limiting the age ratings of apps that can be accessed on the device, and setting time limits for device usage. Apple also offers Ask to Buy through its Family Sharing feature, which gives parents the ability to approve all purchases and downloads that occur on a kid's device, including in-app purchases. These features are essential for parents to ensure that they can properly supervise their children's devices and experiences with game apps. If Apple were to allow individual software apps like streaming games to be distributed within a streaming game service app, none of these protections would be able to be applied to the individual games and customers would lose these significant benefits. The CMA's analysis simply fails to address this key issue.

52. Second, Apple has provided extensive technical submissions explaining, in an objective manner, the significant difference between the more dynamic nature of cloud games compared to other forms of traditional media such as movies, songs, or other forms of user-created content. This specifically includes a detailed comparison of the risks associated with cloud gaming as against those associated with online game creation services, along with a detailed breakdown of why those risks are not adequately mitigated by safeguards within the App Review process, Apple protection controls or App Store product pages. As Apple has explained at length, 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. Further, 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. Apple has also

made clear what would happen if it did not have the ability to review an individual game when it is initially offered and when it updates, which is that Apple's curated App Store model would be nullified, creating a critical consumer vulnerability that would undermine its vertically-integrated model.

53. Again, the CMA ignores Apple's evidence, choosing instead to accept the biased views of certain cloud gaming providers acting to support their own interest. Apple has cautioned the CMA to scrutinise the motives behind complainants such as Microsoft, which seek to frame the cloud gaming issue as a "competition" concern, when in reality this is an attempt to gain 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. Apple is deeply concerned that the CMA has lost sight of the fact that these issues are driven by the commercial interests of a few large developers focused on cloud gaming and risk the App Store losing its reputation as a safe and trusted platform, which is something that benefits all developers, particularly smaller developers.

54. The CMA's finding that cloud gaming service providers apply equivalent protections is incorrect and simplistic. In its limited assessment of the safeguards provided by cloud gaming service providers, the CMA does little more than describe those protections and does not attempt to engage in any serious or robust analysis of the quality or the effectiveness of those safeguards on a standalone basis, let alone in comparison to those currently offered through Apple's vertically integrated model. It is immediately apparent that, unlike Apple, whose incentives are to ensure the safety and performance of the wider ecosystem, individual cloud gaming developers have no real incentive to address threats that could impact on the security or functionality of the device. The assertion that cloud gaming providers could (and in part do) apply equivalent protections can neither be expected nor is it borne out by the available evidence. The failure of the CMA to address this obvious imbalance is symptomatic of the lack of analysis undertaken in the final report.

55. As a result, the CMA does not have the required robust empirical basis on which to reach findings that could have severe impacts on Apple's business and could give rise to significant consumer harm due to the clear potential to increase security issues on its ecosystem. The CMA's inadequate approach to its assessment of cloud gaming is further shown by its finding that Google has allowed cloud gaming apps to be distributed "*without any indication that this has compromised user safety*", which is directly contradicted by objective evidence showing that Android suffers significantly more vulnerabilities than iOS (as discussed above in relation to mobile browser engines).

56. Finally, the CMA highlights evidence indicating users expect to have access to multiple games within the same app, without considering that, for many users at least, this benefit may be significantly outweighed by privacy and security concerns. Apple has provided extensive evidence, including from an array of different survey results, showing that consumers value its security and privacy-focussed approach and that these features of its vertically integrated offering are a key competitive differentiator for its ecosystem. Apple has further explained that introducing security vulnerabilities into one aspect of its ecosystem has severe knock-on effects for the security integrity of all other features. The CMA fails to engage with that backdrop and engage in any analysis of whether users would in fact demand unrestricted access to cloud gaming in native apps if the clear trade-off for this would be to have an ecosystem with a lower level of security in line with that currently offered by Android.

Question 2 - Do you agree the reference test is met for cloud gaming?

57. For the reasons set out in response to Question 1 above, the CMA's analysis with respect to the one sole 'feature' of the cloud gaming market is not well founded. This means that the legal test for a reference with respect to cloud gaming is not met.

58. Further, as set out above with respect to mobile browsers, there is effective competition at the ecosystem level between Apple and Google which drives positive outcomes for users and developers in the cloud gaming market.

59. There is also robust competition across gaming platforms. This includes online cloud gaming platforms on the PC such as Steam (as the first mover, Steam pioneered digital distribution on PC and was a dominant player in the space by 2018 with 70 to 85 percent market share) as well as those which run off dedicated gaming consoles, such as Xbox Cloud Gaming for Xbox Series X, the cloud-based service launched by Nintendo for its 3DS device and Sony's PSP Go, as well as other PC and console app platforms.

60. As explained in more detail above, in response to consumer demand and competition at the ecosystem level, Apple has innovated by adapting its products and services in order to accommodate the technologies which underly cloud-gaming. Apple has expended considerable effort to work with cloud gaming service providers in order to develop multiple methods which permit the distribution of cloud gaming apps on iOS without compromising the iOS ecosystem's core privacy and security standards. Cloud games can feasibly be provided on iOS either via web apps (for those developers who choose not to meet the security standards for native apps) or via native apps, subject to Apple's guidelines, thus precluding significant adverse effects on competition.

61. Apple has further concerns that the CMA has not followed its own guidance that customer benefits must be weighed against the risk of potential adverse effects.[9] Apple's approach has strong positive effects in terms of precluding security threats and providing a consistent user experience. Apple's approach therefore contributes to offering differentiated products that cater to consumers' demand for high quality and secure products. These benefits have not been properly considered by the CMA, if at all, nor has it made any attempt to weigh them against any potential adverse effects arising from Apple's approach.

Question 3 - Do you agree with our proposal to exercise the CMA's discretion to make a reference in relation to the supply of mobile browsers and cloud gaming in the UK?

62. Apple considers that it is apparent from the evidence before the CMA that the necessary basis for making a reference is not present in relation to cloud gaming. The factors to be taken into account by the CMA when considering whether to exercise its discretion to make a reference are therefore not triggered.

63. In any event, it is clear that, since there is already effective competition within respect to cloud gaming, there are no adverse effects on competition, let alone at a scale to warrant a reference.

[9] Market Investigation References guidance, OFT511, paragraph 2.30.

64. Apple further reiterates the points made above at paragraph 34 with respect to the appropriateness of making a market investigation reference rather than opening a formal antitrust investigation.

Question 4 - Do you consider that the proposed scope of the reference, as set out in the draft terms of the reference published alongside this document, would be sufficient to enable any adverse effect on competition (or any resulting or likely detrimental effects on customers) caused by the features referred to above to be effectively and comprehensively remedied?

65. For the reasons set out in response to Questions 1 and 2, Apple considers that the CMA's findings with respect to the sole 'feature' of the market for cloud gaming which the CMA has identified are not well-founded and as such it is neither necessary nor appropriate for the CMA to intervene in that market.

Question 5 - Do you have any views on our current thinking on the types of remedies that a MIR could consider (see above and Chapter 8 of the market study final report)? Are there other measures we should consider?

66. For the reasons already set out above, Apple's view is that the CMA's potential interventions for cloud gaming would be unnecessary, disproportionate, and would give rise to the significant unintended consequence of undermining the current effective state of competition between iOS and Android at the ecosystem level, thereby harming users and developers.

67. The CMA also fails to take into account the potential harm to consumers arising from the increased risk of security and privacy breaches that would likely result from the CMA's proposed interventions. Apple considers that this harm must be assessed against any gains which the CMA considers could be derived from its proposed remedies.

Question 6 - Do you have any views on areas where we should undertake further analysis or gather further evidence as part of an MIR in relation to the supply of mobile browsers and cloud gaming?

68. For the reasons set out above, Apple considers that the reference test is not met with respect to cloud gaming and that it is not appropriate to make a reference.

69. For completeness and, without prejudice to the above, if the CMA were to make a reference in relation to cloud gaming then it would be critical for the CMA to conduct further analysis to be carried out to properly understand:

- The steps Apple has taken to encourage cloud gaming apps with the context of its App store rules.
- The additional security risks which arise from the dynamic nature of cloud gaming apps.
- The limitations of third-party cloud gaming providers' security safeguards.

****