APPLE'S RESPONSE TO CMA WORKING PAPER 7

POTENTIAL REMEDIES

30 August 2024

30 August 2024

APPLE'S RESPONSE TO WORKING PAPER 7
POTENTIAL REMEDIES

Apple responds below to the CMA's emerging thinking on potential remedies as set out in Working Paper 7.

A. Introduction

1. The CMA is empowered to impose remedies only where it has found that there is an Adverse Effect on Competition (AEC) stemming from feature(s) of a market that prevent, restrict or distort competition.[1] The CMA cannot simply speculate that market features "may" have such an effect,[2] nor is it sufficient for the CMA to hypothesize that certain conduct could theoretically be optimized to allow for more competition. The evidence base before the CMA in this case plainly does not support the finding of an AEC with respect to mobile browsing or cloud gaming, and fails to outweigh the multitude of harms that the CMA's proposed remedies would likely cause.[3]

2. To conclude that there is an AEC, the CMA must demonstrate the conduct in question results in the purported harm to consumers. The CMA, in this respect, has given undue weight to unsupported and outdated complaints, and little to no weight to the interests of consumers in having a user-friendly, stable and secure platform.[4] In fact, the CMA's proposed remedies threaten to degrade the robust iOS security and privacy protections and performance enhancements that Apple has created.

3. The evidence does not support the imposition of the drastic remedies being considered. To the contrary, the evidence base shows that:

   - Competition in mobile browsers on iOS is strong, with a large and diverse set of browsers characterized by a high level of differentiation;
   - Third-party browsers enjoy effective parity with Safari in their ability to deploy features and functionality;
   - Developers are satisfied with the variety of in-app browsing implementations that Apple offers;
   - Users report high satisfaction with Apple devices, awareness of the variety of mobile browser available, and ability to make effective switching decisions; and
   - Cloud gaming is fully supported and available on iOS.

[1] This is set out in section 134 of the Enterprise Act 2002 (EA02) as occurring where "*any feature, or combination of features, of each relevant market prevents, restricts or distorts competition in connection with the supply or acquisition of goods or services in the United Kingdom or a part of the United Kingdom*".

[2] The "balance of probabilities" standard applied by the CMA does not serve to lower this threshold. That standard simply means that the *evidence* "on balance" and "in the round" must show that the feature restricts, distorts or prevents competition.

[3] Crucially, the CMA has not shown why Apple has any incentive to limit browser competition on iOS. Without an incentive to harm competition, the CMA cannot simply adopt untested concerns raised by third parties and conclude that Apple's conduct leads to an AEC. Apple has provided the CMA with extensive evidence that its users' interests are paramount, and that Apple's approach is driven by the objective of providing users with a secure and trustworthy mobile platform, not by any incentive to limit competition. An objective assessment of the evidence does not support an AEC finding.

[4] This is evident throughout the assessments of competition in the CMA's working papers, where security and privacy concerns are treated almost as afterthoughts, and which draw conclusions that are dismissive of these key concerns.

4. In addition to demonstrating Apple's conduct results in an AEC, the CMA must establish that the remedies it proposes to address the AEC are effective, reasonable and proportionate. The CMA must demonstrate from the evidence that, on the balance of probabilities, Apple's conduct harms competition in mobile browsing and/or cloud gaming to a degree that justifies the proposed remedies.

5. As set out in Apple's responses to Working Papers 1 to 6, the CMA's substantive analysis fails to demonstrate any causal link between Apple's conduct and consumer harm or between any putative AEC and the intrusive and wide-ranging remedies under consideration.[5] Imposing remedies on Apple would be unwarranted and disproportionate in such circumstances.

6. Further, some of the proposed remedies are simply unworkable, others would impose significant burdens on Apple without corresponding benefits to developers or users, and some would actively harm the very users the CMA seeks to protect, by reducing privacy, impacting security, and degrading the user experience.

7. Apple addresses below the remedy options proposed by the CMA and specific questions set out in Working Paper 7. However, Apple notes that many of these proposals lack the specificity required for detailed engagement at this stage.

B. Comments on preliminary issues discussed in Working Paper 7

8. Before addressing the remedy options, Apple provides brief comments on certain issues identified by the CMA at the outset of Working Paper 7 as being applicable across all proposed remedies. These issues clearly raise a range of significant concerns, including proportionality, effectiveness, and comity; hence the CMA must exercise significant caution in its remedies assessment.

1. Measures taken in other jurisdictions – in particular, the Digital Markets Act 2022 (the DMA) entering into force in the European Union

9. The CMA states that it has taken Apple's compliance measures with respect to the DMA into account where relevant.[6] In considering remedies in the context of the UK, the CMA must give due weight to the fact that the DMA is an entirely different regulatory framework, with different obligations and operational parameters. The European Commission has not assessed whether there is an AEC in relation to mobile browsing, never mind whether one may be relevant to the UK, and it has imposed requirements on Apple that are not designed to address any harms that may arise from such a finding.

10. Apple further notes that the DMA has not long been in force and that the measures Apple is taking to comply with the DMA are new and continue to evolve. Apple also notes that there are significant harms and disadvantages to measures required under the DMA. In particular, the DMA requirement to allow third-party browser engines on iOS devices will significantly increase the security and privacy risks that Apple has long mitigated through the tight

[5] See, in this respect, *Tesco plc* v *Competition Commission* [2009] CAT 6 at [139]: "*In this regard it may well be sensible for the Commission to apply a "double proportionality approach": for example, the more important a particular factor seems likely to be in the overall proportionality assessment, or the more intrusive, uncertain in its effect, or wide-reaching a proposed remedy is likely to prove, the more detailed or deeper the investigation of the factor in question may need to be.*" Cited approvingly in *Barclays Bank PLC* v Competition Commission [2009] CAT 27 at [20]-[21].

[6] Working Paper 7, paragraph 3.6.

integration of WebKit and iOS.[7] It will also reduce the performance benefits that the WebKit requirement brings to mobile browsing.

11. The CMA cannot simply assume the appropriateness of DMA measures for purposes of its remedy assessment. To do so would result in replicating these harms for UK consumers.

2. The geographic scope of potential remedies

12. The CMA notes that it needs to consider the appropriate geographic scope of any remedies to ensure that they are both effective and proportionate.

13. Even if remedies were warranted, there is no basis for remedies to extend beyond the UK for them to be effective. First, the CMA's own analysis currently finds that the relevant geographic market for mobile browsing is the UK: "*while mobile browsers and browser engines are typically made available on a global basis, companies consider the specific country where their product is being used when designing it and making it available to users*".[8] This is consistent with Apple's experience that apps and services are frequently tailored to different geographic regulatory requirements.[9] There is no reason why mobile browsing apps should warrant remedial action beyond the UK.[10]

14. Second, even if the CMA identifies harms to UK consumers, based on information provided by UK users and developers, those harms should be addressed on a UK basis only.[11] The fact that some developers may wish to implement the same remedies elsewhere, for their own commercial benefit, does not provide a legal basis for the CMA to exercise its powers on an extra-territorial basis. Such an approach would also be inconsistent with well-established principles of comity.

15. Further, it would be wholly disproportionate to require fundamental changes to the iOS architecture on a worldwide basis to address UK-specific concerns. This would impose significant and unreasonable costs on Apple and actively harm users outside the UK who benefit from the current iOS architecture and Apple's carefully considered policies. Further, it would impose the CMA's views on markets outside the UK where other regulators may take

[7] See: https://www.apple.com/legal/dma/dma-ncs.pdf. Browser engines are constantly exposed to untrusted and potentially malicious content and can facilitate access to sensitive user data. As a result, browser engines are one of the most common attack vectors for malicious actors.

[8] Working Paper 1, paragraph 3.67.

[9] The CMA also notes at paragraph 2.37 of Working Paper 1 that browser versions are sometimes released which target particular territories, citing Firefox Lite (an Android browser) which was designed and marketed towards Asia and other regions in which a low-bandwidth browser would be appealing.

[10] Apple notes that in the Google Play Store case, the CMA indicated that remedies limited to app distribution in the UK would be sufficient to address concerns relating to an infringement of UK competition laws. Similarly, the European Commission has a long-standing practice across antitrust and merger cases of accepting remedies in the digital sector that were limited geographically to the EEA. These include the 2004 Microsoft infringement decision (COMP/C-3/37.792; specifically the remedy to address the Windows Media Player tying infringement), the 2014 Motorola infringement and Samsung commitments decisions (AT.39985 and AT.39939, respectively, where the Commission specifically limited its remedies to conduct occurring in the EEA, and only to SEPs granted in the EEA); and the 2023 Microsoft/Activision Blizzard behavioral remedy (Case M.10646, where the behavioral access remedy was limited to EEA-based users).

[11] In this regard, Apple notes that the CMA has previously submitted to the OECD that "*[i]n practice, remedies limited to parties' UK businesses are typically the least onerous effective remedy, and therefore the CMA has not often been required to consider the design of extraterritorial remedies*." Roundtable on the Extraterritorial Reach of Competition Remedies - Note by the United Kingdom, 5 December 2017, available at: https://one.oecd.org/document/DAF/COMP/WP3/WD(2017)40/en/pdf.

a different view of competitive dynamics and consumer welfare. As above, the well-established principles of comity would argue strongly against such an approach.[12]

3. Links between different remedy options as part of a wider mobile 'ecosystem'

16. The CMA posits that the potential remedies could impact the wider Apple ecosystem in a number of ways.[13] While the CMA's focus is on whether this could cause the potential remedies to be less effective, the CMA must carry out a balanced assessment of the impact of potential remedies and consider whether this could render the potential remedies unreasonable or disproportionate.

17. Apple notes, for example, that remedies extending beyond the limited cloud gaming concerns identified by the CMA[14] would impact app distribution more generally. This would clearly be disproportionate. It would be similarly unreasonable for the CMA to impose a remedy aimed at providing access to specific mobile browser functionality that would unnecessarily open up the wider iOS framework to significant security risks.

18. The CMA's remedies also risk impacting negatively on each other and reducing any possible effectiveness. For example, remedies which increase security or privacy risks for users or which make iOS less user-friendly would erode user trust and confidence in the Apple platform and the App Store, which may ultimately undermine any remedies intended to promote app adoption, including of cloud gaming apps.

4. Risks relating to the level of specification of certain proposed remedies

19. The CMA notes that some potential remedies may require extensive and dedicated monitoring.[15] It also notes that there is a risk of remedies being too prescriptive.[16]

20. Apple agrees that these are significant concerns for many of the proposed remedies, which will likely render them both ineffective and disproportionately burdensome. The CMA must therefore give proper additional consideration to these remedies and their attendant risks.

5. The need for testing and trialing of certain user-choice based remedies

21. The CMA currently considers that choice architecture remedies may benefit from some form of testing and trialing before being implemented to "*maximise the prospect that they will be effective in achieving the intended aim*".[17]

22. If such testing and trialing is required, this would make the proposed remedies ill-suited for the remedial processes envisaged under the current market investigations regime. Among other things, it would likely make the current statutory time limits unworkable.[18] This is likely to make such remedies inappropriate for further consideration as a reasonable outcome of this investigative process.

[12] The CMA would undoubtedly consider that these principles would appropriately prevent remedies mandated by other jurisdictions with different competition-law priorities and approaches from affecting UK citizens.

[13] Working Paper 7, paragraphs 3.13 to 3.16.

[14] See Working Paper 6, paragraphs 5.2 and 5.3.

[15] Working Paper 7, paragraph 3.19.

[16] Working Paper 7, paragraph 3.18.

[17] Working Paper 7, paragraph 3.22.

[18] The statutory time limits require the CMA to accept final undertakings or make a final order within six months of the date of publication of the market investigation report (Section 138A of the EA02). Apple notes that there is currently no indication as to when the new powers under Schedule 9 of the Digital Markets, Competition and Consumers Act 2024 will come into force.

23. Further, the CMA has not established well-defined aims for the proposed remedies. This is unsurprising, as it has not carried out the necessary evaluation of an appropriate counterfactual to allow it to do so.[19] In the absence of well-defined objectives, evaluating the effectiveness of any given approach is impracticable and, as a result, repeated testing cannot measure the effectiveness of any proposed remedy. On the contrary, any testing is likely to simply result in additional cost and burden for all parties as the CMA, Apple and other stakeholders debate the need for, and impact of, iterative changes.

C. Potential remedies addressing Issues 1 and 2 (WebKit Requirement and Access to Functionality)

24. The WebKit requirement is a key pillar of iOS platform security, privacy and performance. The requirement to use WebKit as the sole rendering engine for browsers on iOS provides a stable and trusted platform on which third-party browser vendors can develop competitive browsers. The benefits of the WebKit requirement for competition and for users are set out in detail in section IV.A to section IV.C of Apple's response to Working Papers 1 to 5. Further, as set out in detail in section V of that response, iOS provides effective parity to third-party browsers for almost all the features that raise "concerns" in the CMA's Working Paper 3.

25. There is therefore no need for remedy Options A1 to A3.

26. Further, as with its substantive analysis, the CMA's analysis of the proposed remedies fails to properly consider the security and privacy risks that would inevitably arise from introducing alternative browser engines on iOS, and the consequent loss of choice for consumers that value security and privacy. The CMA also ignores the negative consequences that removing the WebKit requirement could have on mobile browser performance. By so doing, the CMA is proposing remedies that are not only disproportionate but also would actively harm UK consumers. Such an outcome cannot reasonably be considered appropriate.

27. Nonetheless, Apple provides below responses to the specific questions raised by the CMA on these proposed remedies.

1. <u>Are there any alternative remedy options that we have not considered in this paper that could address Issues 1 and 2 as effectively as those set out above?</u>

28. The evidence base for the WebKit requirement and Apple's practices regarding access to features and functionality does not support a finding of harm to competition in mobile browsing sufficient to justify the proposed remedies. The CMA has also not demonstrated harm to consumers. On the contrary, the WebKit requirement serves the interests of users by enabling Apple to maintain a secure, stable and safe platform. There is therefore no need for remedy Options A1 to A3. It is axiomatic that there are no further or alternative remedy options that could be legally required.

2. <u>Do you agree with our emerging assessment that Options A2 and A3, as described, could address both Issue 1 and Issue 2?</u>

29. As explained above, neither remedy option is necessary. Moreover, Apple has concerns about how the CMA describes these remedy options.

30. First, there is a considerable lack of detail and clarity on how the CMA expects these remedy options to be implemented. The CMA provides that Remedy Options A1 to A3 "*aim to: (a) enable browsers operating on iOS to use a browser engine other than WebKit, should they wish to do so, and to access the necessary functionality to do so (addressing Issue 1); and (b) provide equivalent access to key features and functionalities that Safari has access to, including the*

[19] See Apple's response to Working Papers 1 to 5 at paragraph 209 *et seq.*

ability to configure and customise these features (addressing Issue 2)".[20] It is unclear what the CMA means by "the ability to configure and customise those features". Does the CMA envisage that Apple should be required to make changes to WebKit to enable functionality that Safari does not have in order to address unsubstantiated complaints from third-party browser vendors? Such an approach would be wholly disproportionate.

31. There are similar difficulties with determining what the CMA means by providing "equivalent access" either to iOS or to APIs when discussing Options A2 and A3. As Apple has explained to the CMA, third-party browsers already have access to or the ability to replicate the vast majority of features that Safari accesses because they can build their own equivalent features using WebKit. Additionally, many browser features do not require interaction with the browser engine, which means that browser developers can build equivalent (or unique) features relative to Safari, independent of WebKit.

32. While Apple is committed to providing developers with very wide-ranging functionalities to facilitate browser competition on iOS, it is not Apple's role to develop every single feature that third parties wish to have but are unwilling to invest in building themselves – and nor should it be. To require Apple to do so would go significantly beyond what could be considered reasonable and proportionate. Doing so would lead to free-riding and underinvestment on the part of third parties, chill browser innovation, and overall harm competition among browsers on iOS.

33. On the specific design and implementation of the remedy options, Apple notes that Options A2 and A3 would require very significant engineering efforts by Apple across multiple teams to redesign existing interfaces. This would not only involve significant cost, but would also in effect prevent Apple's engineering teams from focusing on efforts to develop new WebKit features and maintain its high security and privacy standards for existing features. Such remedies would therefore be unreasonable and disproportionate, and ultimately harm UK consumers.

34. Finally, Apple notes that Issue 2 (access to functionality) does not require a remedy, never mind one as intrusive as mandating additional browser engines on iOS. As the evidence shows, Apple opens up access to features and functionalities as widely and quickly as possible,[21] subject to the overriding need to protect the integrity and performance of the platform as a whole. The CMA has not demonstrated that Apple's timing for doing so has any actual adverse impact on competition or causes harm to developers (and ultimately consumers).[22] In the absence of such evidence, it would be manifestly disproportionate and harmful to users to impose such an intrusive remedy on Apple.

3. <u>As part of remedy design of Options A1-3, are there significant parameters that browser engine providers and browsers would require to be made available to ensure equivalence of access to iOS, in addition to those set out in paragraphs 5.25 to 5.57 above?</u>

35. Remedy options A1 to A3 are unnecessary. The evidence base shows that the WebKit requirement and Apple's practices with respect to third-party access to functionality do not

[20] Working Paper 7, paragraph 5.13.

[21] Apple has clarified that virtually all the features or functionalities identified as "concerns" in WP3 are available in some form to third-party browsers today (see further Section V(D) of Apple's response to Working Papers 1 to 5).

[22] The CMA has provided no evidence to demonstrate its theoretical concern at paragraph 3.64 of Working Paper 3, repeated at paragraph 5.7 of Working Paper 7, that "*even a small-time advantage for Safari can have an impact on competitiveness of third-party browsers*", and no meaningful effort to specify how those purported "advantages" would have an adverse impact on competition in the real world.

prevent, restrict or distort competition among browsers. In fact, they actively benefit consumers by reducing their exposure to privacy and security risks. Mandating third-party engine access to iOS is not only unwarranted, it would affirmatively harm users by increasing their exposure to privacy and security threats, reducing Apple's ability to effectively counter such threats, and negatively impacting the high degree of performance achieved by the Webkit requirement.

36. Nonetheless, the CMA goes even further and suggests at paragraph 5.40 that "*any new APIs created by Apple or existing APIs that are made public under Options A1-3 to provide access to iOS should be kept up to date and maintained to a similar level and standard to APIs used by WebKit and Safari at no additional cost to browser vendors*". This would be clearly disproportionate. Indeed, in the absence of a workable limiting principle, this requirement would directly harm competition by requiring Apple to provide free access to any APIs that its competitors consider relevant to mobile browsing, prohibiting Apple from legitimately recouping the costs of its investments in iOS and encouraging free riding on those investments (including by large and well-resourced browser vendors such as Google). Changes to comply with the CMA's remedy options will necessarily incur a cost, likely on an ongoing and long-term basis. There is no principled reason why Apple, as the undertaking incurring all these engineering costs, should not be entitled to recoup some of them. Further, the CMA has provided no evidence to suggest that third-party browser vendors could not contribute to such costs or that such a contribution would harm competition.

37. The CMA also suggests that "*Apple would need to extend access to a full range of metrics to allow all browser vendors on iOS to measure the performance of their respective browsers*".[23] But this ignores the fact that Apple already provides a wide range of analytics to third-party browsers, and to all third-party apps available on the App Store for that matter.[24] The CMA has provided no analysis or evidence to explain how current levels of support are insufficient. There is therefore no need to further "extend access" to analytics data.

4. <u>Which security and privacy requirements, if any, are reasonable for access to additional iOS functionalities necessary for browsers?</u>

38. The CMA must show how its remedies will not compromise Apple's current high standards of protection of its users.

39. The CMA recognizes that, if a remedy is imposed that allows third-party browser engines on iOS, Apple will need to take action to mitigate the attendant security and privacy risks.[25] It references the requirements for browser vendors under the WBEE, which is available in the EU as part of Apple's DMA compliance.[26]

40. Whilst Apple welcomes the CMA's acknowledgement of the security and privacy risks raised by Remedy Options A1 to A3, it emphasizes that no requirements Apple could impose on browser developers (or browser engine developers) would be sufficient to fully mitigate the harms that would arise from removal of the WebKit requirement. Apple has acknowledged this publicly in its communications on similar DMA requirements.[27] The CMA cannot

[23] Working Paper 7, paragraph 5.42.

[24] See https://developer.apple.com/help/app-store-connect/measure-app-performance/overview-of-reporting-tools/.

[25] See Working Paper 7, paragraph 5.44, where the CMA states that "*[u]nder Options A1-3, Apple may seek to impose certain security and privacy requirements on browser vendors wishing to use alternative browser engines on iOS.*"

[26] Working Paper 7, paragraph 5.46. Note that Working Paper 7 incorrectly states that the WBEE is available in the EEA (rather than the EU).

[27] See https://www.apple.com/legal/dma/dma-ncs.pdf.

therefore simply assume that replicating the security and privacy procedures under the WBEE or EBEE would be sufficient to mitigate any risks.

41. It is also unclear whether the CMA considers that it should specify the security requirements that Apple would be entitled to impose on browser vendors and browser engine vendors. If this is the CMA's intention, Apple vehemently objects on the grounds that this would be inappropriate and unworkable. Given the fast-paced development of security threats, a competition authority such as the CMA is simply not able to effectively delineate appropriate security mitigations or ensure that they adapt as needed to evolving threats. Setting static security requirements would create enormous risks for Apple, developers, and users. Apple — widely recognized as creating the most secure mobile platform — must be allowed to determine what security requirements should be deployed in response to threats as Apple sees them. These risks would not be confined to mobile browsing; the CMA's proposed approach would limit Apple's ability to improve security and privacy for iPhones as a whole. The measures Apple takes to ensure security and privacy in relation to mobile browsing involve hardware and software innovations in the iPhone and iOS, such as PAC. Apple's ability to innovate and develop new iPhone/iOS features that enhance security and privacy overall should not be constrained by the need to engage with the CMA on browser-related mitigations (not least as CMA engagement could not take place ahead of such innovation, thus creating a wholly unworkable "chicken and egg" scenario).

42. Similarly, given the recognition by the CMA of the important role played by Apple's high baseline of privacy protection,[28] it would be unreasonable to prevent Apple from mandating certain privacy requirements for browser and browser engine vendors. Otherwise, some browser developers would take advantage of any relaxed protections to advance their own commercial interests. This would cause significant harm to UK consumers, who have come to rely on the protections afforded by the iOS platform, attributable in large part to the WebKit requirement.

43. It would also actively harm competition. Apple has provided ample evidence demonstrating the importance of privacy as a competitive differentiator between iOS and Android.[29] By hampering Apple's ability to ensure a high baseline of privacy protection on iOS devices, this key competitive differentiator would be lost, stifling an important choice for UK consumers.

5. <u>Are there any other commercial or other terms that we have not considered that could undermine the effectiveness of the remedy options set out above?</u>

44. At paragraph 5.57, the CMA lists hypothetical terms that may "*introduce frictions or barriers which may undermine the effectiveness of the proposed remedy*".

45. First, several of the CMA's terms are so vague that they do not allow for any proper consideration. For example, the concern that Apple may impose "*commercial and business terms which are highly restrictive, which do not similarly apply to Apple's own Safari browser, making launching a competitive browser using an alternative browser engines significantly more difficult*"[30] lacks sufficient detail such that Apple is unable to engage in meaningful dialogue or propose a less harmful alternative. What is the appropriate threshold for "highly restrictive"? To what element of browser competition might these "commercial and business" terms apply? What would render launch of a competitive browser "significantly more

[28] Working Paper 7, paragraph 5.49.

[29] See, for example, the recent research in the field of industrial organization referred to at footnote 7 of Apple's response to Working Papers 1 to 5, which demonstrates that Apple's model encourages greater privacy protections than would prevail on ad-funded models, such as Google/Android. See also the recent privacy-harming outcomes on Google highlighted at paragraph 10 of Apple's response to Working Papers 1 to 5.

[30] Working Paper 7, paragraph 5.57(c).

difficult"? Without any sense of what the CMA is referring to by this statement, Apple cannot sensibly comment or propose a solution.

46. On geographic application, it would be unwarranted and disproportionate for a remedy to extend beyond the UK, as explained in Section B.2.[31] Any terms that prevent unwarranted extra-territorial application would therefore be justified.

47. On commercial terms, the CMA has provided no evidence to support its concern that Apple would impose unduly burdensome commercial terms on browser vendors in the UK, nor has it given any reason for why it considers that Apple has any incentive to do so.

6. What are the main monitoring and enforcement risks, and how could they be mitigated?

48. As explained above, Apple has significant concerns with the high-level and vague description of Remedy Options A1 to A3, which make it difficult to understand exactly how the CMA envisions their practical implementation.[32] Consequently, and leaving aside the fact that the proposed remedy options are not necessary in the first place, Apple is not in a position to comment on monitoring and enforcement risks without a more precise articulation of what the CMA intends to require of Apple.

7. What are the potential costs or lost relevant customer benefits (RCBs) of remedy Options A1 to A3 that we should consider?

49. Remedy Options A1 to A3 would completely remove the benefits of the tight integration of WebKit into iOS, which mandates the use of a single browser engine for all apps rendering web content on iOS. These benefits include:

- Apple's ability to prioritize security at a platform level in a comprehensive, effective, and efficient way, such as by providing a mechanism for the universal adoption of new browser engine mitigations without requiring developers to have a high degree of browser-related security expertise or a resource-intensive commitment to browser-related security concerns.

- Users' ability to trust that all apps on Apple's platform provide a high, baseline level of security and privacy protections across all web browsing experiences, reflecting Apple's "privacy by design" approach.

- Developers' freedom to invest in developing other innovative features and content without the need to actively monitor threats and implement mitigations on their own, or constantly update the versions of the browser engine they use; this particularly benefits smaller developers and new entrants that may not have the expertise or resources to do so.

50. As a result, there are significant RCBs that users currently enjoy, which would be lost if Options A1 to A3 were imposed. These include:

- The higher quality mobile browsing experiences that stem directly from Apple's WebKit requirement, and ensure a high level of baseline protection that dynamically addresses ongoing and novel security and privacy threats. These protections currently pertain to all mobile browsers on iOS, but would be lost if third-party browser engines were permitted on iOS and failed to meet the same standards, or if third-party browser developers failed to implement their own security and privacy mitigations.

[31] See above, paragraphs 12 to 15.

[32] See above, paragraphs 30 and 31.

- Higher quality mobile browsing experiences due to performance benefits that WebKit provides to all browsers on iOS, such that even Chrome performs better on iOS than on Android.[33] This redounds to the benefit, not just of browser developers, who can incorporate this high performance baseline into their app development, but also to users who then benefit from the attendant performance improvements and increased ease-of-use and functionality.

- A greater variety of mobile browsing and wider mobile ecosystem experiences, given the role the WebKit requirement plays in differentiation between iOS and Android on the key parameters of security and privacy. If Options A1 to A3 were imposed, this differentiation would be lost and users who choose iOS on the basis, in whole or in part, of its approach to security and privacy would lose that choice.

- Lower-cost browsing and better ecosystem-wide experiences because of the role of the WebKit requirement in reducing incidences of fraud and other malware on iOS.

51. The cost of losing these RCBs would be significant. UK consumers would face reduced competition, lower quality browsing experiences on iOS and greatly increased risks of malware, fraud and privacy-threatening behavior.

52. Apple would incur significant initial and ongoing development and support costs in allowing third-party browser engines on the App Store. Developers (both browser developers and other app developers) are also likely to suffer the negative consequences of increased malware and fraud on iOS devices in the absence of WebKit. And all parties would suffer from the likely loss of user trust, which would result in lower rates of app downloads and user engagement. Such harms would be particularly acute among smaller, non-incumbent developers.

8. What is the appropriate geographic scope of Options A1-3?

53. As explained in Section B.2, the appropriate geographic scope of any remedy should be no wider than the UK.

9. Under Option A4, would enabling the WebAPK minting feature alone be sufficient to level the playing field relative to Chrome for all third-party browsers on Android?

54. Apple does not have views on this question.

D. Potential remedies addressing Issues 3 to 6 (In-App Browsing)

55. The CMA's considerations of remedies for in-app browsing are wholly misconceived. The proposed remedies are predominantly aimed at enabling third-party browser vendors to offer remote tab IABs on iOS for app developers to "*enhance browser vendors' ability to compete with SFSafariViewController on iOS*".[34]

56. The premise of the proposed remedy reveals a misunderstanding of what SFSafariViewController is. SFSafariViewController is not a remote tab implementation, nor does it invoke Safari at all. Safari and third-party browser vendors operate at parity in in-app browsing use cases, and therefore there are no restrictions on competition or AEC to remedy.

[33] See Apple's response to Working Papers 1 to 5, at paragraph 93.

[34] Working Paper 7, paragraph 6.5.

57. Further, the CMA's underlying assumption that remote tab IABs improve the security (and privacy) of the in-app browsing experience is unfounded. While only vaguely articulated, the CMA's concern appears to be based solely on the fact that remote tab IABs on Android largely rely on dedicated browsers installed on the device, in contrast to the approach on iOS.

58. Remote tab IABs do not provide better security or privacy outcomes. Compared to Android custom tabs, which do not isolate the browsing session state within the custom tabs session from the dedicated browser app, SFSafariViewController is a private sandbox container that offers a "firewalled" web view. This means neither the third-party app, nor Safari, gain access to browsing session state.

59. Apple's approach also avoids exposing its users to the Android "patch gap" problem, where browsers may run on outdated versions of browser engines and thus expose users (including those who use the browser to run a remote tab in-app browsing implementation) to known, but unmitigated security risks.[35] SFSafariViewController therefore offers better security and privacy protection than the remote tab implementation alternative that the CMA seeks to impose.

60. Moreover, the CMA's own research reflects that users have little appetite or interest in specifying the in-app experience.[36] And in the one circumstance where they might, i.e. where a user wishes to punch out of in-app browsing to open a link in a dedicated browser, Apple already offers a way for users to do exactly this. There is, therefore, no conceivable harm to consumers that would justify the imposition of a remedy for in-app browsing.

61. Working Paper 7 does not ask any specific questions on proposed Option B3, which is not a remote-tab implementation but a requirement to allow alternative webviews. The working paper recognizes that, not only is this potential remedy likely to have limited interest, it would also raise even greater security and privacy risks than the remote tab implementation.[37] For the reasons set out in its response to Working Paper 4, Apple considers that a remedy such as Option B3 would be wholly unwarranted, and this view is not changed by anything in Working Paper 7. It would also be clearly disproportionate, as (a) it would not achieve its stated aim (lack of demand means it would not foster entry); and (b) it would produce adverse effects which are disproportionate to that aim (a mere theoretical enabling remedy is outweighed by clear and serious risks to users).

62. It is clear, therefore, that the CMA's concerns about in-app browsing are misplaced. The CMA has provided no evidence that non-browser app developers seek the CMA's proposed remedies, that users would want them, or that there is any actual competition problem that could be solved by them. The proposed remedies are therefore completely unnecessary and highly disproportionate.

63. Nonetheless, Apple responds below to the CMA's specific questions on the proposed remote tab implementation remedies.

[35] See the discussion of the patch gap problem at paragraphs 120 to 122 of Apple's response to Working Papers 1 to 5.

[36] As the CMA's research shows, "*overall users have very low levels of awareness of in-app browsing. Respondents had not thought about in-app browsing before or whether they were using a browser. Respondents also did not normally think about in-app browsing or what was happening operationally 'behind the scenes' when they viewed web content within an app.*" (Working Paper 4, paragraph 4.49)

[37] See, for example, Working Paper 7, paragraph 6.23 ("*Interest in providing alternative webview IABs by browser engine providers also appears to be limited*") and 6.25 (*we have also seen evidence from several parties indicating that webview IABs could have weaker security and privacy protections relative to remote tab IABs and dedicated browsers*).

1. What technical considerations would need to be considered when extending remote tab in-app browsing to third-party browsers on iOS?

64. As noted above, SFSafariViewController is not a remote tab implementation and, despite its name, it *does not invoke or involve Safari at all*. The CMA's proposed Option B1 remedy would therefore mandate functionality for third-party browsers that Safari itself does not currently have. Such a remedy would require Apple to rearchitect its in-app browsing implementations and create entirely new functionalities and would be wholly disproportionate.

65. Option B2 would go even further, requiring Apple to allow third-party browser engines on iOS and then create additional functionality to allow third-party browsers to use those engines when offering a remote-tab implementation. This would involve enormous engineering work, poses tremendous security and privacy risks, and has never been contemplated in the context of Apple's iOS operating system.

66. Aside from the significant technical burdens the proposed in-app browsing remedies would impose on Apple, the fact that these remedies would require Apple to invest significant engineering resources to create functionality that is not currently available to Safari, is of — at best — limited interest to other browser developers, and is based on a fundamental misunderstanding of Apple's technology, would render these remedies entirely disproportionate.

2. What are the likely costs that would be incurred by Apple, app developers and third-party browser vendors to enable remote tab IABs on iOS?

67. Please see the response to question 1 above. Whilst Apple does not have an estimate of the investment required, creating this new functionality would be an enormous undertaking. It would also introduce unintended additional costs by creating a new vector of attack for malware and bad actors, and degrading the protections currently afforded by SFSafariViewController. These additional costs would be borne by Apple, developers and ultimately UK consumers. The costs of the proposed remedy are also set out further in response to question 3 below.

3. What are the benefits and drawbacks in extending users' default browser choice to remote tab IABs (ie always implementing remote tab IAB using users' dedicated browser)?

68. The CMA's proposed remedies are designed purportedly to cater for the stated desires of browser vendors. However, they ignore the benefits that Apple's in-app browsing implementations provide the much larger set of app developers, namely: choice and control over the experience they want to give users in their apps, and critical protections against the risks and vulnerabilities inherent in accessing web content. Creating a remote tab implementation that extends the users' default browser choice in all circumstances would remove this control. Developers would be forced to code for the "lowest common denominator" browser functionality because the in-app experience would be wholly dependent on user settings.[38] And implementing these remedy options would harm thousands of app developers to benefit a limited number of browser vendors, whose concerns with respect to in-app browsing are, in any event, overstated.[39]

[38] This would create a unique and unprecedented situation in which developers cannot test "out of the box" in iOS. Developers would have to test their app not just against the ways users can configure their system settings (font size, etc.) but also against arbitrary third-party implementations of browsing views. It would be incredibly complex for a developer to determine whether their app sufficiently supported all such possibilities. This would cause significant uncertainty and complexity for developers.

[39] See paragraphs 177 to 185 of Apple's response to Working Papers 1 to 5.

69. Further, Remedy Option B5 (implementing changes to the user interface or using disclosures) would harm the user experience and likely be unworkable. This is because it is incredibly difficult for an operating system to differentiate between an app rendering in-app content in a WebView and an app using an in-app browser, which would make it almost impossible to know when to surface a disclosure to users. From the user perspective, having a pop up every time one visits a new page and an app renders web content would be incredibly intrusive and significantly degrade the user's experience in that app.

4. <u>What are possible remedy options, if any, to address Google's webview IAB policy (Issue 5)?</u>

70. Apple does not have views on this question.

5. <u>In relation to Option B6, should user-based awareness and consent for inapp browsing be increased and if so: (i) Which design considerations should be taken into account?; (ii) Should the user be prompted to consent to in-app browsing at a: (1) System-level (phone settings) (2) App-level (each app's settings) (3) At both the system and app levels?; (iii) Should the default setting be set as opt-in or opt-out in each of the cases above, and why?</u>

71. There is simply no need for more user awareness and additional consent prompts for in-app browsing. The in-app browsing use case is a very specific one, where users engage with limited web content in the context of a native app. The aim of in-app browsing is to provide this type of curated engagement without forcing the user away from the particular app experience. The CMA's survey evidence does not suggest that users want greater engagement with in-app browsing or that they have been harmed by the current options available to developers. Even the CMA's own working paper recognizes that increasing the visibility of the IAB experience (Options B5 and B6) might not lead to expected or immediate benefits for users, and might worsen the user experience overall.[40]

E. Potential remedies addressing Issues 7 and 8 (Choice Architecture)

72. Remedies are not necessary in choice architecture for the reasons set out in Apple's response to Working Paper 5. In sum, Apple's choice architecture is pro-consumer and pro-competitive, actively supports third-party browsers, and promotes user choice. Apple's choice architecture does not lower user awareness of, or engagement with, browsers. And the CMA's own survey evidence dispels any notion that Apple's choice architecture provides a competitive advantage to Safari.

73. This is confirmed by Working Paper 7, at paragraph 7.4, where the CMA's conclusions are based on theoretical generalities and amount to nothing more than hypothesis layered upon hypothesis: "*[t]hese practices <u>may</u> mean that users <u>may</u> make fewer effective choices about which browser to use on their mobile device, or experience difficulty or friction in exercising choice or switching between the use of different browsers. Overall, this <u>may</u> mean that fewer consumers are likely to switch between browsers, and therefore, drive browser competition*". There is simply no basis in the factual record for the CMA to find that browser competition is being prevented, restricted or distorted, such as to result in an AEC finding; and accordingly, there is no basis for the imposition of remedies, particularly ones which on balance are more likely to result in user harm.

74. Nonetheless, Apple responds below to the CMA's specific questions.

[40] Working Paper 7, paragraph 6.44.

1. <u>What are your views on the three proposed choice architecture principles for remedy design?</u>

75. The three proposed principles would require significant and careful consideration to ensure that they do not negatively affect consumers' ease-of-use and the overall consumer experience. Taking each principle in turn:

- <u>Targeted.</u> The CMA states that this means choices are presented in "*the right place, at the right time, with the right frequency*".[41] It notes that users should be given the opportunity to make choices more than once but not too often. However, this would require very careful balancing of what "not too often" means, and such balancing would necessarily vary depending on the choice the user is presented with. Where users engage routinely with an experience (such as mobile browsing), it is more likely that repeated "choice" presentations would interfere with the user's experience and result in consumer harm.

- <u>Understandable.</u> The CMA considers this to mean that the layout or presentation of choices should be sufficiently clear.[42] Apple agrees that this is an important principle for choice architecture, as the user interface of its devices has long been a fundamental consideration driving Apple's design decisions. Apple provides users with the information they need to make informed decisions when choosing an app such as a browser, including ratings, reviews, and privacy labels. When considering a potential remedy, Apple requests that the CMA takes due account of the considerable work Apple has already done in this space and ensure that users are able to make informed decisions.

- <u>Balanced.</u> The CMA describes this as finding the "*right amount of friction for users – minimising unjustified friction and understanding where friction can be positive (eg confirming an important action) or protecting users from potential self-harm*".[43] Apple agrees, and considers that the need for appropriate consideration of ease-of-use and the potential for prompt fatigue and other consumer harms is particularly high here. This principle therefore clearly runs a significant risk that a potential remedy would not find the correct balance and would create unjustified friction. The CMA should also take care not to target users of a specific browser to the exclusion of others. Targeting prompts or choice screens only at users of Safari, for example, would clearly be an example of unjustified friction.

2. <u>Which, if any, of the remedy proposals described above do you think will be most effective and proportionate should an AEC be found?</u>

76. For the reasons summarized at paragraph 72, the evidence does not show harm to competition from Apple's choice architecture. The proposed remedy options are therefore unnecessary and, as a consequence, cannot be considered "effective".[44]

77. The proposed remedies are also disproportionate — each one is onerous and creates significant disadvantages disproportionate to its aim. This is because the CMA has given undue weight to academic theories based on behavioral economics that cannot, and should not, be a substitute for real-world design insights and practices that Apple has developed from decades of experience in designing products and services praised for their user-friendliness and accessibility.

[41] Working Paper 7, paragraph 7.6(a).

[42] Working Paper 7, paragraph 7.6(b).

[43] Working Paper 7, paragraph 7.6(c).

[44] Even if there were an AEC in choice architecture, the CMA's failure to consider an appropriate counterfactual with respect to any of the elements of choice architecture means that it cannot meaningfully assess the effectiveness of its proposed remedies, as it has no basis on which to do so.

78. Option C1 (pre-installation of competing browsers) is unnecessary because the survey evidence demonstrates that users are already aware of alternative browsers and their ability to switch.[45] Preinstallation of third-party software would impose an overly onerous burden that would require Apple to introduce third-party software on iOS devices at the point of manufacture, and hence significant changes to its supply chain. Doing so would create significant disadvantages, some of which – such as harms to the user experience and compromised storage capacity – are recognized by the CMA.[46] But others, such as security risks resulting from Apple being unable to guarantee that each browser does not have security vulnerabilities prior to shipping, are not. These unrecognized disadvantages are equally important and have the potential to cause significant harm to UK users.[47] For example, if Apple were required to pre-install third-party browsers on devices, the minimum support period that the iPhone could provide to users would be set at the shortest period that a pre-installed browser vendor would commit to.[48] This would give browser vendors (some of whom compete in the smartphone market) undue influence over Apple's ability to compete and potentially to comply with relevant relegation in that market (such as the UK's Product Security and Telecommunications Infrastructure Act 2022). Imposing a remedy that could result in such a myriad of harms to competition and to consumers would be unreasonable and disproportionate.

79. Option C2 (browser choice screen on set-up) is simply not practical. Forcing users to immediately choose a browser and preventing them from accessing the internet until they do so would create a jarring and confusing user experience, as recognized by the CMA.[49] Reducing the choice to a subset of browser apps on a choice screen at set-up would raise difficult questions about the criteria and process for determining which to include and which to exclude. The unintended harms of this proposed remedy include the exclusion of smaller competing browsers, the reinforcement of the market position of larger competitors, and user dissatisfaction and confusion.

80. Option C3 (placement of a competing browser in the dock or home screen) is unnecessary. Apple has demonstrated that competing browsers can already be automatically placed on the home screen when they are downloaded and users can easily move browsers in and out of the dock.[50] The risks identified above for pre-installation and choice screens are equally applicable here.

81. Option C4 (default is followed across all browser access points) is unnecessary, as all circumstances in which Apple's apps in iOS, and iOS itself, launch a web browser app launch the user's default browser. To the extent that the CMA considers its IAB remedies to be relevant, for the reasons discussed at paragraphs 55 to 62, these remedies are entirely misplaced and unnecessary.

82. Option C5 (browser choice screen after set-up) is unnecessary as the survey evidence demonstrates that users are already aware of alternative browsers and how to switch to them should they choose to do so, with the majority of users having two or more browsers installed

[45] See paragraph 190 of Apple's response to Working Papers 1 to 5, which references the CMA's survey results showing that 60% of iOS users said they are "definitely" able to download alternative browsers, and 27% said they "probably" can do this without help. Only 9% said they "probably" cannot and only 2% said they "definitely" could not download alternative browsers.

[46] Working Paper 7, paragraph 7.15.

[47] See paragraph 192 of Apple's response to Working Papers 1 to 5.

[48] In contrast, Apple currently offers market-leading support for devices at present, as highlighted in Apple's response to Working Papers 1 to 5, at paragraph 110.

[49] Working Paper 7, paragraph 7.58(a).

[50] See paragraphs 195 to 197 of Apple's response to Working Papers 1 to 5.

on their phone.[51] The CMA itself recognizes that this could lead to user harms and would require careful consideration, particularly on the timing, frequency and design of the choice screen.[52]

83. Option C6 (adaptations to the user journey) is also unnecessary. Apple has already demonstrated the ease with which users can select different default browsers and with which developers can prompt users to do so.[53] The CMA's focus on a maximum number of steps ignores this and fails to recognize that a setting that is, for example, two taps away but hard to find would be worse from a user engagement perspective than a setting that is, five taps away but clearly signposted and easy to follow. The CMA's consideration of "minimum standards for visibility" also fails to take account of Apple's existing Human Interface Guidelines and could negatively impact accessibility.

84. Option C7 (requirement to share user data) is wholly unnecessary.[54] There is no competitive disadvantage for third-party browser developers today, and in fact Apple already provides them relevant aggregated analytics. Further, whilst the CMA pays lip service to data protection rights and user control,[55] it does not adequately consider the implications of this proposed remedy on the user experience as a whole, and the user's interest in avoiding unwanted prompts from browsers seeking to be the default.

85. Option C8 is a remedy requiring a limitation on frequency of prompts. As a preliminary point, Apple notes that it does not prompt users to change default browsers on iOS and so this remedy is unnecessary with respect to its practices. Moreover, the proposed remedy recognizes that there are significant risks to the user experience if browsers could frequently prompt them to change their defaults.[56] It would be far more effective and efficient for the CMA to avoid requiring unnecessary prompts in the first place, rather than encouraging those prompts, and then attempting to limit the resulting harm by imposing limitations on their usage.

86. Option C9 (uninstallation of Safari) is wholly unnecessary. The concerns that this remedy seeks to address are entirely speculative. Neither third parties nor users have suggested that any of these are likely to occur, nor has the CMA provided any evidence in support of these speculations. In the absence of any need for such a remedy, it must be considered entirely disproportionate. Further, the CMA has not demonstrated that the ability to uninstall Safari would, in practice, have the effect of fostering competition between mobile browsers, which means that the proposed remedy would, in any event, be ineffective.

3. Which remedies are likely to be effective?

87. Please see the response to question 2, which demonstrates that none of the CMA's proposed remedy options are likely to be effective. As noted above, the CMA has not established well-defined objectives for its proposed remedies. Accordingly, evaluating their effectiveness is extremely difficult; the effectiveness of any remedy should be ascertainable, reflect concrete and pro-competitive aims, and must not arbitrarily determine winners or losers in the market. Otherwise, the remedies threaten to distort competition rather than safeguard it, running contrary to the CMA's stated purpose.

[51] The CMA's survey evidence found that 40% of users had two browsers installed and 15% had three or more installed (see Verian Mobile Browser Consumer Research Report, page 43).

[52] Working Paper 7, paragraph 7.35.

[53] See paragraphs 199 and 206 of Apple's response to Working Papers 1 to 5.

[54] See paragraph 207 of Apple's response to Working Papers 1 to 5.

[55] Working Paper 7, paragraph 7.45.

[56] See Working Paper 7, paragraph 7.48, which notes the "*potentially 'nagging' nature of prompts that users are exposed to*" and "*the fatigue that an overload of prompts and notifications can produce*".

4. Which of the remedies listed above is least intrusive for users? Please explain your answer.

88. As set out in response to question 2, some of the proposed remedy options risk imposing unnecessary frictions and intruding on the user journey in unhelpful ways. Others merely preserve the status quo; for example, and as explained in paragraph 85, Apple does not prompt users to change default browsers on iOS, so the imposition of Option C.8 as a remedy would not serve to change Apple's conduct.

89. Apple's response to Working Paper 5 sets out the clear benefits to users of its choice architecture design and implementation. Apple creates a framework for users that is easy to understand and operate, allowing them to exercise choice when they wish to do so. The CMA's proposed remedies would interfere significantly with this and force users to disengage from tasks they are actively trying to carry out to deal with "choices" that they have not sought out. This would create significant frictions and would harm the user experience of mobile browsing on iOS devices.

5. Which, if any, of the remedy proposals described above would offer opportunities for increasing user awareness and engagement?

90. There is already sufficient user awareness of, and engagement with, mobile browsers. Rather than identifying a problem that needs to be addressed, the CMA's survey evidence shows that browsers on iOS work broadly as intended in providing users with seamless access to the web. This is consistent with the intended purposes of Apple's choice architecture, its incentives as a platform operator to ensure that the highest quality browsers are available on its devices, and the CMA's own recognition that choice architecture can be pro-user and pro-competition.

91. In these circumstances, none of the remedy proposals are necessary to increase user awareness or engagement.

6. How important is regulatory alignment and cohesion with existing regulation (eg DMA) when considering choice architecture practices?

92. For the reasons set out at paragraphs 12 to 5, the CMA should not seek to extend remedies beyond the territory of the UK. Moreover, if the CMA ultimately deems remedies to be necessary, it must give due consideration to relevant factors, including: (i) the significant implementation resources that may be required by developers and Apple; (ii) avoiding conflicting regulatory requirements; (iii) the need for and expectation of a consistent user experience; and (iv) principles of comity.

F. Potential remedies addressing Issues 9 and 10 (Cloud Gaming)

93. No remedies are necessary in cloud gaming for the reasons set out in Apple's response to Working Paper 6. Apple's App Review Guidelines do not restrict or prevent cloud gaming services, nor does IAP impose a barrier to cloud gaming. Remedies aimed at the Guidelines, generally, or IAP, in particular, are therefore unwarranted.

94. Nonetheless, Apple responds below to the CMA's specific questions on these proposed remedies.

1. Do you consider that the remedy options above and/or any other remedies are likely to be effective?

95. There is no AEC in cloud gaming to address. The proposed remedy options are therefore unnecessary and, as a consequence, cannot be considered "effective".

96. Apple supports developers in their efforts to monetize their apps and seeks to address issues that may arise in doing so. If, contrary to Apple's experience, developers find that the Guidelines or the IAP requirement create difficulty with respect to cloud gaming, Apple already has effective mechanisms in place to address such concerns through the App Review process and developer relations (for example, the Guidelines state that developers can submit an appeal if they disagree with the outcome of a review, and provide a link for developers to suggest changes to the Guidelines "*to help [Apple] improve the App Review process or identify a need for clarity in [Apple's] policies*."[57] Apple has demonstrated that it listens to developer concerns and evolves the Guidelines, including for cloud streaming games, when it can do so while maintaining Apple's core user experience and guarantees of privacy and security. This further underscores that the CMA's proposed remedy options are unnecessary. For the reasons set out below, they are also unreasonable and/or disproportionate.

97. Proposed Option D1 (review and amendment of the Guidelines) is entirely speculative. The CMA has identified no Guideline that contains technical or other forms of restrictions on cloud gaming apps. The speculative nature of the remedy is compounded by its purported application to any hypothetical "new restrictions" that could have an equivalent, but unspecified, effect.[58] Such a vague remedy would be impractical and unworkable, as Apple would have no means to determine how to ensure compliance with such an obligation.

98. The accompanying requirement to submit regular reports on its rejection of cloud gaming apps from the UK App Store[59] would impose an unnecessary burden on Apple, not least as the proposed remedy contains no limiting principles on the categories of rejection. Nor does it clearly delineate which gaming apps may qualify as "cloud gaming" apps in such a scenario and for reporting purposes. Finally, it would require the CMA to involve itself in highly technical decisions relating to app functionality which, as a competition authority, it is ill-equipped to consider.

99. Remedy option D2 (enabling cloud gaming native apps to operate on a 'read-only' basis), is not only unnecessary but also would, as the CMA recognizes, actively reduce the monetization opportunities for cloud gaming services and negatively impact the user experience.[60] These unintended consequences would outweigh any potential benefits, especially because Apple has demonstrated that the IAP requirement does not provide a barrier to cloud gaming, is consistent with the approach of other platform providers, and ensures a consistent approach between cloud gaming apps and other apps on iOS.[61] Game apps have never qualified for "reader" treatment under the Guidelines, and this has not hampered their popularity or financial success. As such, there is no reason to apply this rule to a small segment of the game app category.

100. Similarly, remedy option D3 (allowing cloud gaming apps to incorporate their own or third party in-app payment systems for in-game transactions) would create a unique exception to Apple's longstanding IAP requirement for a single category of app. This would be contrary to the underlying ethos of the App Review Guidelines, which is centered on equal treatment of all apps, and would result in the CMA mandating an unfair and unbalanced outcome for cloud gaming apps compared to all other app types.

101. The options under consideration are therefore unwarranted, unreasonable and/or disproportionate.

[57] Available at: https://developer.apple.com/distribute/app-review/#contact-us.

[58] Working Paper 7, paragraph 8.4(b).

[59] Working Paper 7, paragraph 8.4(c).

[60] Working Paper 7, paragraph 8.8.

[61] See paragraphs 26 to 35 of Apple's response to Working Paper 6.

G. Conclusion

102. The evidence base does not demonstrate that there is harm to competition in either mobile browsing or cloud gaming sufficient to warrant the imposition of the intrusive and wide-ranging proposed remedies. As shown above, these remedies are unreasonable or disproportionate. Some are simply unworkable; others would impose significant burdens on Apple without corresponding benefits to developers or users; still others would actively harm developers and users, and create significant market inefficiencies. Apple therefore submits that none of the proposed remedies should be imposed.

****