APPLE’S RESPONSE TO CMA
PROVISIONAL DECISION REPORT

17 December 2024

I. INTRODUCTION

1. Apple is pleased that the CMA's Provisional Decision Report ('PDR') has provisionally confirmed that the evidence does not support a finding of an adverse effect on competition ('AEC') in cloud gaming. We welcome the CMA's recognition that cloud gaming service providers do not face material challenges in integrating in-app payment ('IAP') and that there is evidence of thriving market entry. Apple has always supported gaming, as well as cloud gaming, and will continue to do so in the future.

2. Apple also welcomes the PDR's increased recognition of the benefits that Apple's approach brings to users and developers, including through the tight integration of WebKit and iOS.[1] Nonetheless, the PDR's analysis remains unbalanced and incomplete in key respects, which leads the CMA to continue to underestimate the pro-competitive and pro-consumer benefits that Apple brings to mobile browsing. A proper reassessment of the evidence will show that no AEC arises in relation to mobile browsing.

3. On remedies, Apple agrees with the PDR's provisional conclusion that it would be inappropriate to impose remedies at the conclusion of this market investigation. Apple considers that remedies are unwarranted as no AEC arises in relation to any element of mobile browsing. Nonetheless, to the extent that the Inquiry Group continues to find any AECs relating to mobile browsing relating to its conduct, Apple does not believe that the remedial options considered by the Inquiry Group are sufficiently specific, proportionate, or considerate of relevant customer benefits ('RCBs') to either warrant immediate imposition of remedies in the form in which they have been set out in the PDR or to allow the CMA Board to implement such proposed remedy options as part of its digital markets regime.

4. For many issues in the PDR, Apple considers that the analysis does not take full and proper account of the effect that the proposed remedy options could have on the user experience that its customers seek, in particular on security, privacy, and performance. While the CMA does acknowledge that the WebKit requirement provides security benefits, it simply asserts that "*it is likely that these risks could be managed in other ways*".[2] If - despite Apple's strong view that there is no AEC in mobile browsing - the CMA is minded to impose remedies (including under the digital markets regime), these and other issues discussed below would need to be more fully explored. The remedy options, if taken forward as set out in the PDR, would result in significant harm to consumers and the vast majority of developers.

5. Apple considers that, on balance, the PDR's substantive assessment leads only to identification of speculative harms, whose ability to impact competition in mobile browsing have been overstated. The potential interventions contemplated in the PDR, on the other hand, would lead to a reduction in differentiation and competition at the device and browser levels. This would harm many developers and users to the benefit of a few market participants, most notably, Google. This response sets out Apple's concerns and offers guidance on how the Inquiry Group might ameliorate the PDR's shortcomings to achieve the best outcome for all UK users and developers.

A. The markets for mobile browsing on iOS are already well-functioning

6. The CMA's market investigation seeks to answer one fundamental question: whether the market(s) under review are "well-functioning".[3] There can be no serious doubt that this is the case for mobile browsing on iOS, where the market is competitive and delivers good outcomes

[1] As set out at paragraph 40-44 below, we note that the CMA has defined "iOS" to mean "iOS and iPadOS" which has not only confused two different OSs but has also likely caused confusion in relation to the CMA's evidence gathering through the use of a defined term to mean something different to its widely understood real-world meaning. However, in order to respond to the PDR, Apple has adopted the CMA's naming convention.

[2] See, for example, PDR, paragraph 4.194(b) Citations to the PDR in this response refer to the public version available on the CMA's website at at 13 December 2024.

[3] Defined as a market without an AEC. See, for example, *Barclays Bank v Competition Commission* [2009] CAT 27, paragraph 104. In the absence of a statutory benchmark against which to assess the market (as is the case for mobile browsers), the CMA's CC3 (Revised) Guidelines for Market Investigations, dated April 2023 ('CC3') require the CMA to benchmark the market being investigated against this "well-functioning market" standard, which it notes "displays the beneficial aspect of competition…but not an idealized perfectly competitive market" (CC3, paragraph 320).

for consumers. Indeed, throughout the market investigation and Mobile Ecosystems Market Study (MEMS), the third party feedback agitating for change has been led by a limited number of vocal market participants and interest groups whose submissions appear driven by commercial interests rather than the interests of UK users.[4]

7. Competition between mobile browsers on iOS is robust, as evidenced by the large and diverse range of available browsers. There are roughly 100 different browsers on the UK App Store with varying features and unique selling points - a range and level of differentiation similar to that available on the Android platform. On iOS, third-party browsers compete strongly with Safari on a level playing field, with effective parity of access to features and functionality, and with the ability to encourage user uptake and switching. Users can choose a preferred browser, be it Safari or another browser, to operate as their default browser and that choice is respected. For developers of native apps who want to offer access to web content via their apps, Apple offers a variety of implementation mechanisms for in-app browsers ('IABs') tailored to their diverse needs and capabilities, whilst preserving the user's ability to instead open that content in their default browser if they so choose. The CMA's own evidence shows that most developers are satisfied with these implementations and it is critical that the CMA does not lose sight of this market consensus.

8. The well-functioning nature of these markets is a natural consequence of the economic incentives and technical framework under which Apple enables mobile browsing on iOS, with competition at the device level fostering competition in relation to mobile browsing:

   - Apple is predominantly a device manufacturer, with device sales representing nearly 80% of total revenue.[5] This is crucial to the CMA's understanding of Apple's incentives and what drives its design decisions - notably, a very different incentive structure from any of Apple's rivals who instead are incentivized to collect user data or engage in other means to monetize their businesses. Apple's brand enjoys high levels of trust and satisfaction,[6] precisely because users understand that its business model does not depend on harvesting personal data, a key differentiating factor for Apple as compared to its competitors.

   - Consequently, Apple's design decisions are driven by the robust competition that it faces from rivals at the device level. Apple offers a rich platform with a variety of features and services to attract developers by: (a) providing hundreds of thousands of APIs that app developers, including web browser developers, can leverage, ensuring a rich and wide array of browsers is available on the iPhone; and (b) prioritizing the factors that its users value, namely privacy, security, and performance. Safari plays an important role in providing a high quality out-of-the-box experience for users in keeping with Apple's overarching principles of design that promote ease-of-use through elegant and user-friendly services. A poor user experience would be fatal to Apple's core business, as changes that harm the user experience would reduce Apple's ability to differentiate its products and compete in the market.

   - The real and constant threat of switching at the device level incentivizes Apple to support developers and enable competitive mobile browsing options on iOS by facilitating entry for all app developers, including browser developers. Apple has designed its platform with that in mind, and continues to invest billions of dollars in innovation and developing safeguards to protect users and developers.

   - At a technical level, the deep integration between iOS and WebKit actually supports the ability of third-party developers to innovate and compete. By prioritizing security, privacy and performance through a common WebKit install, Apple ensures that all developers benefit from an exceptionally high baseline from which to build their apps (whether those are dedicated browser apps or apps incorporating IABs). Apple does not self-preference Safari through WebKit, but provides developers with parity of access to hundreds of features,

[4] As Apple has previously submitted and sets out again below, many of the complaints received by the CMA are unsupported and/or simply factually incorrect.

[5] See Apple 2024 Annual report, page 29.

[6] See, in this respect, the CMA's own finding in MEMS that users' satisfaction with iPhones is high, with 74% of iOS users indicating their degree of satisfaction is between 8 and 10 out of 10 (MEMS Final Report, footnote 148).

and the ability to contribute to the development of WebKit through the open source control repository.[7]

9. In sum, Apple offers users a real choice. Users who are concerned about privacy and security know that they can rely on Apple's privacy-by-design and tightly-integrated architecture to protect them against unscrupulous developers that want to profit from privacy encroachments, as well as bad actors that seek to promulgate malware. Users do not themselves need to become technical experts to have reassurance that the apps they download are private, secure, and will not degrade device performance. This baseline level of reliability offered by Apple devices gives users a real choice at the device level. And, given Safari and WebKit's commitment to these principles, this choice is also offered at the browser level. Apple's recent Safari Privacy campaign, which aimed to contrast specifically with Google, is illustrative of the meaningful contrast between iOS browsers and choices available to users.[8]

10. At the same time, Apple's differentiated approach at the device level fosters competition from other mobile browsers. Developers of all sizes and capabilities can create differentiated apps for iOS that compete on a level playing field with assistance from Apple in providing the security and privacy expected by users on the platform, and without needing to invest in and develop security and privacy expertise themselves.

11. Together, these factors ensure robust competition both at the device level and in mobile browsing.

B. The CMA's underlying premise is flawed

12. The CMA's approach to what would be required for a "well-functioning mobile browsing market" runs contrary to its market investigations guidance.[9] The CMA considers an idealized state of competition as the benchmark and has not properly considered the real-world competitive effects of the measures it considers to lead to an AEC. The CMA's approach assumes a theoretical and unrealistic world in which increased access to iOS or WebKit functionalities for third parties would necessarily lead to better outcomes, whilst (a) ignoring that in material respects developers' commercial interests may be in tension with user interests, and (b) simultaneously presuming that Apple could address the inevitable security and privacy harms that would arise to a degree that has plainly not been achieved on any other platform.[10]

13. Further, by taking this approach, the CMA relegates key considerations of the beneficial aspects of Apple's approach and does not give them due prominence in its analysis. In particular, the benefits described above are not simply efficiencies to be weighed against the presumed harm caused by a lack of alternative browser engines; rather, they are key design elements that create a stronger foundation for the enabling and support of competition at both the device and browser levels, thus preventing competitive harm from occurring in the first place.[11]

14. Without Apple's approach, there would be less competitive differentiation between mobile platforms and the loss for both users and developers of a system that provides wholesale protection against security and privacy risks (as opposed to individualized approaches). This could disproportionately impact smaller developers, who would be less able to bear the financial

[7] As noted below, Chrome itself was originally forked from WebKit.

[8] See, for example, https://youtu.be/0HjDpPnxcP0 . This campaign ran in June 2024 across multiple markets, including the UK, with advertisements on billboards, retail, film and TV, digital and social media, and on Apple's own Privacy, Safari and iPhone online product pages. The campaign demonstrated the superior privacy protections afforded by Safari, along with the tagline "Safari: a browser that's actually private".

[9] See CC3, paragraph 320.

[10] See in particular PDR, paragraphs 11.100, 11.111, 11.174, 11.188, 11.192, 11.196 and 11.217, where the CMA has presumed without evidence that Apple will be able to implement the CMA's remedy options while at the same time ensuring security through imposing unspecified restrictions. We note that, hitherto, Apple has maintained security on the iOS platform with precisely the requirements that the PDR has provisionally determined constitute an AEC.

[11] For completeness, however, Apple notes that, should the CMA continue to consider that there is a negative impact on competition arising from Apple's approach to mobile browsing, it should also have proper regard for the benefits of that approach, which lead to significant rivalry-enhancing efficiencies (within the meaning of paragraph 174 of CC3) in terms of consumer benefits and benefits to developers. Those efficiencies, in turn, further competition in mobile browsing to such an extent that they outweigh any negative effects that could arise from Apple's approach. Thus, a proper consideration of the evidence in relation to the existence of such rivalry-enhancing efficiencies would result in a finding of no AEC on mobile browsing on iOS. If, notwithstanding this, the CMA were to find an AEC, these efficiencies would constitute RCBs of such significant scale and scope to render remedies unwarranted.

and technical burden of considering and actively adopting key security and privacy protections on an ongoing basis if they were to use alternative browser engines. Smaller browser developers would also stand to lose (and thus be less able to compete) if the inherent trust that users have in products and services offered on iOS were to be reduced. Competition through differentiation between Apple and Google would be significantly reduced and competition among browsers and among other apps rendering web content would be reduced in the absence of that choice. Consumers who value security and privacy would be deprived of devices that cater to their preferences.

15. Further, as Apple has demonstrated over the course of MEMS and the current market investigation, owing in part to the patch gap issue on Android, browser security and privacy on iOS is considerably better than on Android, the WebKit requirement ensures that browsers are rapidly patched against exploitable vulnerabilities, and the WebKit versions of Chrome and Firefox in fact perform *better* on the iOS system than they do using alternative browser engines on equivalent devices as demonstrated by multiple test suites.

C. The totality of the evidence does not support the PDR's provisional AEC finding

16. In determining whether there is an AEC, the CMA "*must take reasonable steps to acquaint itself with the relevant information to enable it to answer each statutory question posed for it….*".[12] We are concerned that the CMA has not done so in key respects, and that the evidence does not support the provisional AEC findings.

17. First, the evidence base on which the provisional findings rely is, by the CMA's own description, limited. The PDR sets out that the CMA has communicated with or sought information from "*17 companies which provide mobile browsers, 62 developers of apps and internet content, 17 companies which manufacture mobile handsets, and nine other parties and nine other industry groups and parties involved in mobile browsers more widely*".[13] This is a remarkably thin foundation on which to base provisional findings. To put that in context, Apple engages regularly with over a hundred thousand developers worldwide through multiple fora, including direct communications through its developer relations team, WWDC events and other *ad hoc* developer events.

18. In these circumstances, it is all the more important for the CMA to properly weigh the evidence it has received and place it in its appropriate context. The PDR indicates that the CMA has not done so. Taking the CMA's analysis of access to features and functionality, for example, the PDR provisionally concludes that Safari has greater access to features relative to third-party mobile browsers overall.[14] It reaches this conclusion, despite also finding that "*there is some conflicting evidence and it is not possible to conclude that Apple has restricted or delayed access to all of the above features*",[15] and despite the fact that the complaints it received relate to a handful of the myriad of WebKit features that Apple makes available to third-party developers.[16] Such a limited and inconclusive evidence base cannot reasonably support the PDR's provisional conclusions.

19. Second, and similarly, we are concerned that the provisional findings are heavily influenced by the fact that some of the most vocal participants in the market investigation have their own commercial interests and agendas to promote and are opportunistically using this market investigation process to do so.[17] Meta, for example, whose business model is founded on the monetization of data, seeks to introduce new IAB options resulting from potential CMA

[12] *BAA v Competition Commission* [2012] CAT 3, paragraph 20(3).

[13] PDR, paragraph 1.23(e).

[14] PDR, paragraph 5.57, for example, in relation to user-facing features.

[15] PDR, paragraph 5.57.

[16] As previously submitted to the CMA, Apple continuously releases new features for WebKit, releasing support for 119 new features with Safari 16.4, 105 new features with Safari 17 and 39 new features with Safari 17.2. See Apple's response to the CMA's Statement of Issues, paragraphs 7-8. Apple also provided the CMA with a table setting out significant functionalities that developers have requested over the years and when Apple rolled these features out. See [✂].

[17] For example, the CMA should recognize that whilst browser developers may not want to incur costs associated with developing a version of their browser which runs on an additional engine (see PDR, paragraph 4.55), this has not prevented these browsers from operating on the iOS platform. Additionally, these costs could reasonably be regarded as standard costs of doing business, such as the requirement for games manufacturers to make different versions of a game for PlayStation and Xbox.

intervention that would allow it to better exploit user data, circumventing protections that Apple has specifically designed to protect user data, and that are built into Apple's products today.

20. Despite this, the CMA's provisional finding that Apple's so-called "*ban*" on alternative browser engines for in-app browsing on iOS gives rise to an AEC rests almost exclusively on Meta's self-interested submissions. Further, this finding effectively ignores the fact that: "*app developers are generally content with their current options for implementing in-app browsing on iOS*";[18] "*[m]ost app developers who engaged with this market investigation have not expressed interest in using alternative webviews provided by third-party browser engines or browser vendors on iOS*";[19] and "*the majority of app developers would not be interested in building upon their own custom or forked engine to develop a 'bundled engine IAB' on iOS [including] large app developers that are relatively engaged in developing their IAB.*"[20] The CMA appears to have taken Meta's complaints at face value, and chosen to ignore the views of the majority of developers, and the potential for significant harm to user privacy — all to benefit Meta's position and commercial model of monetizing user data in the form of advertising. The CMA appears to accept Meta's assertions even though Meta itself has publicly recognized the very patch gap problem associated with in-app browsers that the WebKit requirement addresses: users may update some apps, but not others, leaving older apps vulnerable to known security threats.[21]

21. The CMA's imbalanced approach also appears to apply to the evidence submitted by web developers. The PDR, for example, contrasts two sets of feedback from web developers on the costs of ensuring compatibility, and the role of the WebKit requirement in relation to these costs. A small number of specific developers (including at least one browser vendor) submitted concerns.[22] On the other hand, Jigsaw surveyed a "*wide range of web developers working with mobile browsers and mobile browser engines*",[23] few of whom reported any issue with regard to WebKit[24] and most of whom noted that compatibility testing did not take up much time.[25] Despite this, the PDR provisionally concludes that web compatibility issues contribute to the AEC that the CMA has found.[26]

22. Third, the PDR places minimal reliance on the views of users, despite the CMA's surveys showing that on the whole users are satisfied with their browsers and browser engine options on iOS.[27]

23. Fourth, the CMA's provisional conclusions continue to rely to an important degree on material that has not been provided to Apple (or its advisors) and that Apple has not had the opportunity to test or rebut, including in preparing this response. Examples of such material include the advice provided to the CMA by RET2 Inc[28] and information provided by the NCSC.[29] Such information is an important part of the CMA's analysis in respect of the security implications of the WebKit requirement and also the CMA's consideration of possible remedies. We are highly concerned that the CMA continues to consider it appropriate to derive conclusions from such material without providing Apple a proper opportunity to examine it,[30] particularly in light of its tendency in this investigation to accept third-party submissions at face value.

[18] PDR, paragraph 7.86.

[19] PDR, paragraph 7.59.

[20] PDR, paragraph 7.60.

[21] https://engineering.fb.com/2022/09/30/android/launching-a-new-chromium-based-webview-for-android/#:~:text=Our%20in%2Dapp%20browser%20for,Android%20and%20other%20operating%20systems

[22] PDR, paragraph 4.101.

[23] PDR, paragraph 2.50.

[24] PDR, paragraph 4.103.

[25] PDR, paragraph 2.112(c).

[26] PDR, paragraph 10.8.

[27] Most notably, the CMA describes the Verian qualitative user survey as showing that "*respondents felt that there is adequate choice of browsers available to them*" and that "*respondents were typically able to find and download alternative browsers*". PDR, paragraphs 2.54(e) and (f).

[28] Referred to in the PDR at paragraphs 4.165(b), 4.169(d), 4.173(a), 4.175(a), 4.180(c), 4.186(e), 4.191, 11.119 and 11.195.

[29] Referred to in the PDR at paragraphs 4.145, 4.175(b), 4.191, 11.117, 11.118 and 11.120.

[30] The CMA could have provided Apple an opportunity to comment by publishing the reports and responses on its website, as it has with externally commissioned research from Jigsaw and Verian, as well as the various responses to its papers. It could also have disclosed this information to external counsel under a confidentiality ring, as it has with other data. However it has chosen not to adopt either approach.

24. We urge the CMA to reconsider its provisional findings with the above points in mind and to reassess where the weight of evidence actually lies.

D. The remedy options considered could result in significant user and developer harms

25. Should the Inquiry Group conclude that there is an AEC in relation to mobile browsing in the Final Report (which Apple submits would be wholly unwarranted), for the reasons set out further below, Apple does not believe that the remedial steps considered by the Inquiry Group are sufficiently specific, proportionate, or considerate of RCBs to either warrant the immediate imposition of remedies in the form in which they have been set out in the PDR or to allow the CMA Board to implement such proposed remedy options as part of its digital markets regime, without a fuller exploration of their potential risks and harms.

26. That said, Apple recognizes that the DMCC Act regime would provide an opportunity for the DMU to more fully explore any remedial options and to more holistically assess any potential remedies than has been done to date.

27. Apple also notes that the DMU must, should it follow the recommendations of the Inquiry Group, consider potential remedy options objectively and afresh, including appropriately updating and robustly corroborating the evidence base.[31] Nonetheless, Apple understands the findings and the recommendations of the Inquiry Group will form part of the considerations on which the DMU will act. In this response, we therefore highlight key concerns with the remedies proposed in the PDR and their potential impact on users and developers.

28. In particular, we draw the CMA's attention to the Competition Appeal Tribunal's findings in *Tesco plc v Competition Commission* that "*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*."[32] The PDR contains proposed remedy options that are wide-reaching — some even going beyond UK borders — and that are, at best, uncertain in effect. We consider that the CMA has not adequately assessed or taken account of the potential negative impact of these remedies on developers and users, as well as their proportionality.

29. For example, while the CMA acknowledges that "*Apple's dual role as the device manufacturer and operating system provider means it is best placed to determine how the required level of access can be granted to third parties considering any security and privacy considerations that need to be incorporated*",[33] the proposed remedy options nonetheless suggest various elements - such as preventing the use of a separate binary mechanism as part of granting access, and requiring the ability to use alternative browser engines to power Home Screen Web Apps and IABs - that would significantly undermine Apple's ability to ensure the high baseline level of security and privacy which its users expect.

30. The PDR also suggests, in the context of the Google ISA, a proposed global remedy that would go beyond any market remedy that the CMA has imposed or agreed to before and which would exceed what is necessary to remedy any putative AEC in the UK.[34] This would be unnecessary, disproportionate, and contrary to principles of international comity. The CMA's proposed remedy option seeks to terminate the Chrome revenue share in non-UK jurisdictions despite the fact that regulators in those jurisdictions may not have concerns regarding the revenue share or, indeed, consider that the revenue share offers benefits to competition. We address this and other concerns with such a highly intrusive and inappropriately-scoped remedy option below.

31. We urge the CMA to review its remedies analysis in light of the submissions in this response and to adapt the proposed guidance it intends to give the DMU on remedy options accordingly.

[31] As recognized at paragraph 2.65 of the CMA's Draft Digital Markets Guidance, the CMA may only rely on evidence gathered and analyzed in previous cases and investigations where relevant to do so, will be mindful of when and for what purpose evidence was initially gathered, and will consider the weight evidence should be given and the extent to which it should be updated or corroborated.

[32] [2009] CAT 6 at paragraph 139, cited approvingly in *Barclays Bank PLC v Competition Commission* [2009] CAT 27 at paragraphs 20-21.

[33] PDR, paragraph 11.100.

[34] It appears that the CMA may also be considering that, with respect to alternative browser engines and access to features, Apple should not be allowed to impose a geographic limitation on the ability of developers to test new features. Apple submits that this would also be a disproportionate imposition and would not be needed to allow developers to make use of additional functionality within the UK.

II. NATURE OF COMPETITION AND MARKET DEFINITION

32. Apple notes that the PDR's analysis of the nature of competition and market definition is based on the extant CC3 guidance. However, by the time of the Final Report, the CMA is expected to have adopted its revised markets guidance. This is likely to impact the Final Report's analysis, as the PDR assessment is out of step with the CMA's draft Markets Substantive Assessment Guidance in key respects.

A. Product market definition and competition

33. The CMA has applied its CC3 guidance and adopted a narrow product market definition, based on traditional theories of demand-side substitutability and the timing of the user's decision to download a browser. This has limited the CMA's scope to take account of what would, under this framework, be regarded as "out of market constraints", which include, for example, features and innovation on Blink-based browsers. As the CMA notes, Apple expends a lot of time and effort benchmarking these browsers.[35]

34. The CMA's upcoming Substantive Assessment Guidance will allow the CMA to take a less formalistic approach to market definition, and define the market by reference to "the most important constraints on relevant firms providing goods and services subject to the MIR".[36]

35. Apple has repeatedly submitted that one of its key competitive dynamics is device-level competition, which in turn fosters competition at the browser level.[37] A poor browsing experience on the iPhone (whether in the form of reduced security, privacy or performance) would make users less likely to upgrade their devices, and/or more likely to switch to the Android ecosystem when they do. If the CMA's conclusions on minimal competitive constraints on WebKit were to hold true, Apple would have less incentive to innovate and the Safari browser would be considerably lower quality than it is today.

36. The CMA's narrow focus also underplays the competitive dynamics driving the incentives of third-party browser vendors, who predominantly provide their browsers for free and rely on search advertising revenue.[38] Under this model, users are not treated as customers, but rather as products to sell to advertisers. As explained elsewhere in this response, third-party developers that adopt a business model based primarily on advertising/sale of user personal data undervalue the user experience in their submissions to the CMA, a factor which the CMA's narrow approach underestimates.

37. Finally, the CMA's approach misunderstands the impact of the broader app environment (including for browser apps) on Apple's incentives. A large volume of high-quality apps increases the appeal of Apple's devices and boosts device sales. A comparison can be drawn between the impact of app availability on device sales and the impact of aftermarket sales on markets such as aerospace manufacturing, where sellers of the primary product often seek to ensure that customers get a good deal in aftermarket sales of third-party replacement parts, given the impact on sales of the primary product.[39] In a similar fashion, Apple seeks to ensure that the user experience with respect to engagement with third-party apps (including browser apps) is as high-quality, safe and private as possible through rules such as the WebKit requirement. Cultivating a diverse and secure app environment is intended to drive sales of the iPhone (device sales making up almost 80% of Apple's revenue), and self-preferencing in favor of Safari in the manner that the PDR suggests would be contrary to Apple's incentives in that respect.

38. Put differently, Apple, which focuses on device manufacturing, has an incentive to enable <u>all</u> third-party app developers to develop iOS applications. Because Apple does not limit app development to only certain trusted parties, Apple must protect its customers by developing

[35] PDR, paragraph 2.35.

[36] CMA draft Markets Substantive Assessment Guidance, paragraph 11.7.

[37] In this respect, Apple notes that the CMA's view (at PDR paragraph 4.243) that some of the competition between browser engines across iOS and Android devices may take place between desktop browsers (where WebKit and Blink compete on the same platform), rather than on mobile (where WebKit is only present on iOS, and Blink is only present on Android) is unsupported by any evidence or analysis.

[38] In contrast, whilst Apple generates a portion of its revenues from search advertising, via the revenue share arrangements it has with search engine providers, the clear majority of its revenues comes from device sales.

[39] See, for example, the CMA's recent report to the Secretary of State in *Parker-Hannifin/Meggitt* of 18 March 2022, paragraph 7.18.

safeguards designed to prevent third-party apps from jeopardizing the security and privacy of those customers and their Apple-branded devices. The WebKit requirement is a necessary element of those safeguards because it ensures that browsers access the internet via WebKit, which is consistently updated to ensure a high baseline of security and privacy protections.

39. On balance, market dynamics related to browser engines and browsers on iOS only make sense when we consider the broader competitive constraints that have thus far been undervalued by the CMA's overly formalistic and narrow approach. We look forward to the CMA applying a more flexible approach in the Final Report, as required by the new Guidance, and taking greater account of the full range of relevant competitive constraints in these highly complex, dynamic, and innovative markets.

B. The CMA should treat iPadOS and iOS separately

40. The CMA has drawn the conclusion that the product market for mobile browsing on iOS and iPadOS is separate and distinct from desktop browsing and browsing on Android mobile devices. It does so, based on its findings of (a) limited supply-side substitutability between browsers on iOS and iPadOS due to optimization requirements for the different screen size and type of device;[40] and (b) limited demand-side substitutability for users because the use cases for browsing on a mobile device and desktop ultimately differ.[41] However, the same can also be said for iOS and iPadOS themselves.

41. Apple offers separate iOS and iPadOS-specific guidelines,[42] which help developers create apps that offer an optimal user experience on each operating system ('OS').[43]

42. Consistent with those guidelines, app developers tailor their apps for specific Apple OSs, taking advantage of the hardware and software features that are only available on those OSs. Browser developers recognize these key differences between the iPhone and iPad experiences and so develop different versions of their browsers for each platform.

43. With respect to the use cases for browsing on iOS and iPadOS, [✂].[44] The CMA's conclusion on a lack of demand-side substitution between mobile and desktop browsers, which is based on the former being used for "on the go" browsing,[45] would therefore equally be applicable to iOS and iPadOS.

44. Furthermore, the PDR states that the CMA's evidence-gathering has defined "mobile devices" as including both mobile phones and tablets, and defined "iOS" as including both iOS and iPadOS.[46] Apple notes that this conflation of iOS and iPadOS may have confused respondents to the CMA's market investigation. Further, the Verian quantitative survey asked respondents for their experience and interaction with browsers on smartphones only. The CMA has not tested whether that evidence would apply equally to tablets. Whilst the PDR states that "*evidence and views presented in this report … apply to both iOS and iPadOS*",[47] the CMA cannot simply assume that the evidence it has gathered allows it to draw inferences about iPadOS.

C. Geographic scope

45. The CMA's Working Paper suggested that although "*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.*"[48] Based on the evidence, the CMA's initial approach better reflects commercial reality, i.e. that it is most

[40] PDR, paragraph 3.61.

[41] PDR, paragraph 3.62.

[42] See https://developer.apple.com/ios/planning/ and https://developer.apple.com/ipados/planning/

[43] This will, for example, involve adjusting the user interface as users interact with Apple's OSs and corresponding devices in different ways. For example, iPhone users are more likely to use it with one hand or with their thumbs; users will typically hold an iPad with two hands or use an accessory (e.g., an Apple Pencil or a keyboard). The different screen sizes of the two devices also merit different user interface design.

[44] [✂]

[45] PDR, paragraph 3.62.

[46] PDR, paragraph 4.8.

[47] *Ibid.*

[48] See CMA's Working Paper 1, Nature of competition in the supply of mobile browsers and browser engines, dated 27 June 2024 ('Working paper 1'), paragraph 3.67.

appropriate to consider the market on a UK-wide basis. The PDR, however, provisionally concludes that the geographic scope of browser markets is broader. This new, overly expansive definition of the relevant geographic market in the PDR is not supported by the evidence.

46. First, the CMA's approach is inconsistent. The PDR asserts that the product market is platform-specific (including only iOS and iPadOS), but the CMA has considered popular browsers within a UK+ EEA geographic market on a platform-agnostic basis.

47. Second, regarding the CMA's analysis of Apple's internal documents: the CMA's analysis relies on three internal documents that do not support its conclusion. [✄].[49]

48. Third, regarding the CMA's conclusion that the UK and EEA share regulatory similarities which makes them distinct from the rest of the world: the regulatory landscapes of the UK and EEA are no longer aligned in a way that would create a UK+EEA region distinct from the rest of the world. As the CMA recognizes (and highlights[50]), there are substantial and significant differences between the DMA regime and the upcoming DMCC regime.

49. The CMA's provisional conclusion of a UK+EEA geographic scope for browser-related markets is also at odds with its conclusions on geographic scope in cloud gaming, which rightly references jurisdiction-specific storefronts which are available in the App Store as a basis for provisionally finding a national market.[51]

50. The CMA's conclusion is also at odds with how it has chosen to examine the market: it has considered shares of supply on a UK-wide basis,[52] rather than on the basis of its provisionally identified geographic market. In so doing, the CMA has not conducted its AEC analysis for the geographic market that it has identified, but of only a part of that market. This inconsistency casts further doubt on the CMA's provisional conclusions.

51. Finally, regardless of the PDR's provisional conclusions on geographic scope of the market, the Inquiry Group is required to determine and address "*any feature, or combination of features, of each relevant market [that] prevents, restricts or distorts competition in connection with the supply or acquisition of any goods or services* ***in the United Kingdom or a part of the United Kingdom*** *[emphasis added]*".[53] Thus, maintaining a wider-than-UK geographic market in the face of all the evidence to the contrary could create problems with respect to remedial action, both in terms of proportionality and widely accepted rules of international comity. As set out further below:

    - There is no need for remedies to extend beyond the UK to be effective. Apps and services are frequently tailored to different geographic regulatory requirements, and UK remedies would adequately address any notional UK harms in this context.[54]

    - 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.

    - The extra-territorial application of remedies would also impose the CMA's views on markets outside the UK where other regulators may take a different view of competitive dynamics and consumer welfare. An extra-territorial approach to remedies would create conflict of laws situations. Apple's current mobile browsing policies and approach are in compliance with laws around the world. Any requirement by the CMA that purports to require Apple to

[49] Apple further notes that the CMA has not previously tested its interpretation of these documents or the conclusions drawn from them with Apple.

[50] See, for example, the description of the DMCC Act regime as a "*regime uniquely and consciously designed to address harms in a highly targeted way, while keeping innovation-led markets open and contestable to support growth.*" Jessica Lennard, CMA Chief Strategy and External Affairs Officer in a speech to the British Institute of International and Comparative Law ('BIICL'), 26 November 2024.

[51] PDR, paragraph 12.58.

[52] PDR, paragraph 3.141.

[53] Section 134(2) of the Enterprise Act 2002 ('EA02').

[54] The fact that some developers may wish to implement the same remedies elsewhere, for their own commercial benefit, does not provide an appropriate legal basis for the CMA to exercise its powers on an extra-territorial basis. This would go beyond what is necessary for a remedy to be effective in the UK context, purely to the advantage of certain market participants.

alter how we comply with those laws would run the risk of either conflicting with regulatory requirements already in place in another jurisdiction or of preempting regulatory outcomes in other jurisdictions. This suggests a supremacy of UK law that cannot exist within the international legal order and creates clear extra-territorial conflict issues for Apple. From a policy perspective, it would also invite other jurisdictions to similarly impose their views on UK consumers and would be inconsistent with established principles of international comity.

III. THE WEBKIT REQUIREMENT

52. Apple has serious concerns that the CMA has not properly considered the substantial body of evidence submitted during the investigation which demonstrates that the WebKit requirement enables effective outcomes and promotes competition in relation to mobile browsing on iOS.

A. The WebKit requirement is pro-competitive

53. The evidence on the extent to which Apple's approach enables browser developers to differentiate and innovate on iOS has been set out in detail in Apple's response to Working Papers 1 to 5[55] and summarized in the introductory section above.

54. Since the inception of the iPhone, Apple has always required WebKit to deliver the highest quality browsing experience on a mobile device, while maintaining iPhone's high privacy, security, and performance standards that users prioritize. By building the foundation of iOS browsing on WebKit, Apple was able to deliver an exceptional user experience that helped spur the iPhone's success and provide users with a compelling alternative to Android devices.

55. We have also explained in detail during this investigation how using WebKit as the sole browser engine reduces costs for developers, resulting in low barriers to entry for browsers on iOS and fostering mobile browsing competition.[56] The PDR seeks to downplay these benefits by provisionally finding that absent the WebKit requirement, individual browser vendors could still choose to use WebKit and obtain these benefits.[57] This line of reasoning entirely misses the point. The benefits of WebKit are not predicated on the individual use of WebKit as a browser engine, but rather the use of WebKit as the only browser engine on iOS, which provides Apple with the ability to address security and privacy concerns and ensure a high bar of performance across all mobile browsers. This gives users the confidence to try new browsers without fear of compromising their device, hogging device memory, or draining their battery. This confidence encourages engagement with different browsers, particularly those from less well-known developers. Eliminating the WebKit requirement would reduce users' confidence to try new browsers, thereby heightening barriers to entry and expansion for developers and diminishing the competitiveness of the platform overall.

56. It is unclear how, on the weight of evidence before the CMA, mobile browsing on iOS can be viewed as anything but competitive and well functioning.

B. The CMA has adopted an inappropriate benchmark for its assessment

57. By defining a well-functioning market for browsers as one that requires access to alternative browser engines,[58] the CMA effectively considers that, if browsers have access to just one underlying browser engine, competition among browsers cannot lead to effective outcomes for users and developers. Apple strongly disputes such a provisional conclusion.

58. As explained above, the evidence indicates that the vast majority of developers and users are satisfied with current options. It is instructive to consider outcomes on the Android platform, where alternative browser engines have long been available, but where, in practice, the Blink

[55] See, in particular, paragraphs 17 to 28 and 71 to 113.

[56] Relatedly, we note from Google's response to Working Paper 1 that the browser, Chatloop, was launched with just £2.1m in seed funding. This browser is now available on the iOS App Store.

[57] See PDR paragraphs 4.58 and 4.72.

[58] PDR, paragraph 4.257 where the CMA states: "*we consider that in a well-functioning market for browsers on iOS, browser vendors would be able to choose from multiple alternative browser engines in order to best meet their needs in terms of implementing features and improvements in their mobile browsers and reducing their overall costs*".

engine (originally itself a fork from WebKit) has a 97-99% share,[59] indicating a lack of demand among developers (and ultimately users) for diversity in browser engines. Indeed, one would expect that customers (in this case, browsers developers) in digital markets where there are low barriers to switching would gravitate to the best product or service available. Further, the fact that under the CMA's benchmark, the presence of a single alternative with a 1-3% share would be sufficient to render a browser engine environment "competitive" must surely be a strong indicator that the benchmark is inappropriate.

59. Indeed, browser developers do not appear to value diversity in available browser engines: Opera abandoned its Presto engine and Microsoft abandoned its EdgeHTML engine, both in favor of Blink. The PDR does not evidence or suggest a desire in the market for the development of a new browser engine and the purely speculative and self-interested statements from Meta on its possible development of a bundled engine IAB (based heavily on Blink) to support its advertising-led business model should not be viewed as such.[60]

60. Thus, even if the CMA were to implement a remedy opening up the iOS system to all third-party browser engines, the entry of a third, non-Blink browser engine onto the iOS platform is itself far from certain given the outcomes on the Android platform and factors such as Mozilla's financial position.[61] The CMA should not, therefore, expect that remedial action in relation to the WebKit requirement will lead to entry onto iOS by a browser engine other than Blink.[62]

61. In any event, the CMA's desired outcomes - namely the ability to implement features and improvements in their mobile browsers and reduce their overall costs - are, as the evidence shows, already provided by WebKit on iOS.

C. The CMA understates the importance of browsers and browser engine security and privacy

62. Apple welcomes the CMA's provisional views that:

(i) The WebKit requirement provides security benefits by allowing Apple to control updates and features for every mobile browser on the platform;[63] and

(ii) WebKit's integration between device hardware and software provides security benefits.[64]

63. Both of these conclusions are accurate and important.

64. However, we feel very strongly that the CMA's provisional views do not go far enough in recognizing the security benefits that WebKit provides. In particular, the CMA has underestimated the importance of security for mobile browsers, due to a misplaced view of the impact of browser-based attacks which, while less common than alternative vectors such as sideloading, fraud and scams, can have as substantive or even greater net impact.[65] Even if browser-based attacks are less frequent than those risks, the nature of browser-based attacks has the potential to result in catastrophic consequences in terms of compromising a device.[66]

65. In any event, it is unclear how the existence of alternative threats could lessen the importance of the concrete threat of bad actors gaining access to users' personal financial, health and other

[59] Depending on App Annie data (PDR, at Table 3.3) or Cloudflare data (PDR, at Table 3.5).

[60] As set out below, any such entry is highly unlikely to be pro-user and, in fact, is likely to lead to significant privacy encroachment. We note the observation from one stakeholder that "*it does not consider Meta's IAB to be contributing towards 'general purpose web engine development' (eg in web standards forums) and is not aware of any significant work in relation to security and performance in the context of the development of bundled engine IABs. This stakeholder considers that Facebook is interested in tracking user behaviour, such that Meta's development efforts in its IAB may be aimed towards the app's business and facilitating this tracking*." PDR, paragraph 7.70(b).

[61] Mozilla has recently announced that it is laying off 30% of its staff, its second round of layoffs in 2024. See https://techcrunch.com/2024/11/05/mozilla-foundation-lays-off-30-staff-drops-advocacy-division/

[62] Given the outcomes on the Android platform, it is likely, in fact, that far from enhancing competition and diversity of choice, the approach set out in the PDR could help create a Blink/Chromium monoculture as non-Blink engines are unlikely to prove a realistic competitive alternative.

[63] PDR, paragraph 4.194(b).

[64] PDR, paragraph 4.194(c).

[65] PDR, paragraph 4.165. The CMA similarly notes (at paragraph 4.194(a)) that "*Mobile browsers and browser engines are important to the security of mobile devices, particularly given their wide usage, but are not the only threat.*"

[66] By analogy, the CMA's position is equivalent to ignoring aircraft engine safety because hydraulic or pressurization failures are more common.

important information. As such, Apple does not see how the existence of other threat vectors can, in any way, counter or reduce the need to address security threats arising from mobile browsing as the goal of security protections is the minimization of threats across the board. The same holds with respect to the overall privacy-enhancing benefits that Apple's approach brings.

66. Apple has provided extensive evidence of the degree to which browsers and browser engines represent major threat vectors for users, particularly on iOS, given their role in interfacing with unvetted web content and the characteristics of mobile devices.[67] The PDR does not adequately engage with this. Such browser-based attacks today may be less common on iOS, but this merely reflects the fact that all iOS browsers must use the most up-to-date version of the WebKit engine, thanks to the WebKit requirement.

67. On materiality, the CMA's approach ignores the importance of attacks, both for users and the platform as a whole:

- 0-day: Because the CMA's analysis has assumed that browser engines are always kept up to date, even on Android (which our patch gap analysis has demonstrated is not the case), it focuses on so-called "0-day" attacks on browsers, i.e. attacks for which a patch has not been developed.[68] The CMA effectively dismisses these attacks as being very unlikely to target the average user - noting that the development of 0-day exploits can cost millions of dollars and are often state-sponsored efforts to steal the data of targeted individuals.[69] This approach is unnecessarily limited, not least as it ignores the consequences to the British state and the wider public from a successful 0-day attack. State-sponsored attacks are more likely to expose important or classified information, the release of which could cause considerable loss of life, international diplomatic incidents, or severely impact ongoing intelligence operations.[70]

- N-day: Further, the CMA has not appreciated the importance of "N-day" attacks, which exploit known vulnerabilities. N-day exploits are effectively commoditized, as the exploit is publicly known. Large scale botnets, such as the Mirai Botnet, use N-day exploits to take over large numbers of devices from which they can launch attacks on infrastructure as well as Distributed Denial of Service (DDoS) attacks. These attacks rely on the failure of developers (or occasionally users) to update their software to address the exploit. Apple has shown that browsers on Android frequently use engines that are months, if not years out of date, leading to a huge number of potential N-day exploit opportunities. In contrast, a key strength of the WebKit requirement is that it gives Apple the ability to instantaneously update the browser engine for all browsers operating on iOS, avoiding such patch gap risks and N-day exploit opportunities on the platform.[71] The CMA recognizes that such attacks "*are still used to target populations with out-of-date software*"[72] but does not properly take this into account in its assessment of the level of risk posed by browser-based attacks.

[67] See for example, Apple's response to Working Papers 1-5, paragraph 11.

[68] PDR, paragraph 4.165(b).

[69] *Ibid.*

[70] Examples of browser exploits that have given rise to national security risks include: https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/; and https://thehackernews.com/2024/08/russian-hackers-exploit-safari-and.html

[71] PDR, paragraph 4.169(d). For example, Apple's March 2024 UK analysis of browsers on the Google Play Store found that 30 of the 38 most downloaded UK browser applications (78.95%) used an out-of-date engine version. Apple also provided data showing that as a browser goes increasingly out-of-date, the number of known vulnerabilities and the number of confirmed exploited vulnerabilities rises substantially. For example, a browser running Chromium version 61 in March 2024 (i.e., over six years out of date) would be subject to 1781 known vulnerabilities, 48 of which are confirmed to have been actually exploited by malicious actors. (See data provided to the CMA in [✂]).

[72] PDR, paragraph 4.169(d). Even here, the PDR relies on RET2's view that they "are becoming less useful". This is an unwarranted conclusion. First, RET2's statement dates from 2022 and so does not engage with the patch gap evidence Apple has provided. Second, as Apple's March 2024 patch gap analysis reveals, there are significant target populations running out-of-date software, thus indicating that N-day exploits remain an important threat for those populations. For example, as Apple has previously set out, vulnerability CVE-2023-4762 in Chromium has been identified by NIST to render browsers running version 116 or earlier susceptible to remote code execution. (See [✂]). Based on recent analysis, this would affect users of 5 browsers, with a total of 700M+ downloads. A further update of the same analysis reveals that 23 of the 34 reviewed UK browser applications, which together have total downloads in excess of 3 billion (including Samsung Browser, DuckDuckGo and Ecosia), are using engine versions that are 6 months or more out of date and which are vulnerable to at least 3 known exploited vulnerabilities. This includes vulnerability CVE-2024-7971 which is a memory corruption issue that can be exploited via a website.

68. The CMA has, in part, justified its approach by reference to the Verian customer survey data,[73] downplaying its own recognition that security and privacy contribute to positive perceptions of Apple's brand.[74] As [✂] demonstrates, the CMA has also incorrectly downplayed Apple's internal surveys which *do* show security and privacy to be extremely important factors for users' device choice.[75]

69. Our experience is that users highly value security and privacy and that meeting the standard they expect is a necessary precondition to them purchasing an iPhone.

70. We urge the CMA to reconsider its security and privacy analysis and to have appropriate due regard to the extensive evidence on the material security risks that users face, the ability of the WebKit requirement to address such risks, and the importance of privacy for Apple's users.

D. The CMA underestimates the risks of allowing alternative browser engines on iOS

71. In considering that alternative browser engines could achieve similar security outcomes on iOS, the CMA has made several fundamental errors of assessment.

72. First, without seeking to reiterate Apple's extensive prior submissions on WebKit's benefits,[76] Apple recalls that the WebKit requirement provides a high base level of stability, security, and privacy that is more effective than Android for a variety of reasons, including because it does not result in a 'patch gap' which in turn gives rise to "significant security risks".[77]

73. The importance of mandating a high base level of stability, security, and privacy should not be understated. A very recent survey from the UK government's Department for Science, Innovation and Technology ('DSIT') found that very few app developers in the UK are even aware of the voluntary code of practice on mobile app security and privacy for app developers, app store operators and platform developers which DSIT had introduced in 2022.[78] This code of practice effectively provides a minimum security and privacy baseline for app developers,[79] but the survey found that a significant proportion of UK app developers had not introduced processes for security incidents or personal data breaches. There is clear reason to worry that this same gap in awareness would extend to developers embedding a browser engine for IAB or even to browser developers, particularly those with fewer resources or less technical expertise. In the absence of the WebKit requirement, it falls on all such app developers to remain vigilant and take necessary and expedient steps to address security threats and avoid patch gaps. The evidence from DSIT only bolsters the concerns Apple has repeatedly expressed to the CMA throughout the market investigation, concerns that the CMA has thus far discounted.

74. As the CMA has accepted,[80] the patch gap issue that Apple has identified on Android also demonstrates that users do not switch away from browsers because they have security risks (as underlying browser engines are likely to be an even lower-salience item than browsers[81]). Further, no developer advertises their app as operating on an unpatched browser engine with known exploitable vulnerabilities, but this is what our research has found that they do, in some cases without addressing the issue for months or years.

[73] PDR, paragraph 4.231. This is despite the fact that the CMA has ignored the same survey data in relation to choice architecture when the data does not support the CMA's provisional findings.

[74] PDR, paragraph 4.224.

[75] See PDR, Appendix C, paragraph 6.13. In this respect, Apple notes that (i) it is not reasonable for the CMA to place more weight on its own survey because the results superficially differ from Apple's iPhone Buyer Survey; (ii) the CMA did not raise any concerns regarding the methodology used by Apple during the investigation, making it inappropriate to now raise them as a reason to dismiss the results; and (iii) Apple's regression analysis relates to [✂].

[76] See Apple's response to CMA Working papers 1 to 5, paragraphs 72 to 77 and 114 to 144.

[77] PDR, paragraph 4.169.

[78] https://www.gov.uk/government/publications/app-store-security-and-privacy-app-developer-survey/app-developer-survey

[79] As such, it is likely to be insufficient for browser developers, given the threat level that browsers face, as compared to apps that are not exposed to the web.

[80] PDR paragraph 4.191.

[81] PDR, paragraph 5.53(a).

75. Second, while the CMA appears satisfied that certain Blink safeguards have the "same or similar" security functionality to WebKit,[82] this does not address Apple's key argument that many Android browser developers will not adopt the latest *version* of Blink. As a result, the CMA cannot simply assume that Blink safeguards are adequate to ensure an appropriate level of security for the whole platform. The CMA's security analysis[83] is also highly flawed because it only analyses Safari against Firefox and Chrome, i.e. browsers most likely to implement the very latest versions of Gecko and Blink.[84] As Apple has explained throughout the market investigation, effective security protections must be designed with the lowest common denominator in mind because the most outdated browser engine on the platform will be the most vulnerable vector for attack — a weakness that will exist regardless of how many other browser engines are up to date. The CMA's unstated assumption that other third-party browsers would use the latest iteration of their chosen browser engine is demonstrably incorrect: Apple's analysis has shown that the browser engine versions used by many other Android browsers can be months or years out of date.

76. Similarly, the CMA places material weight on the notion that non-WebKit browser engines could achieve effective security outcomes due to their "stringent" approach to testing and fixing vulnerabilities, based simply on assertions from Google and Mozilla that they deploy certain security techniques and identify and fix issues quickly[85] (again ignoring that other browsers would need to implement and deploy such fixes in their own apps - particularly those that modify the engine they use). The CMA is unable to corroborate these assertions, having found its own quantitative analysis of the speed of security fixes is not robust. The CMA also relies on evidence from 2018, which - six years later - is obsolete. It is inappropriate to consider such evidence to outweigh the objective, recent evidence submitted by Apple with respect to WebKit's security outcomes.

77. Third, we are concerned by the inconsistent treatment of evidence on which the CMA relies: for example, when considering why the WebKit requirement is unnecessary from a security perspective - specifically in relation to Home Screen Web Apps ('HSWAs')[86] - the CMA relies on submissions from the UK National Cyber Security Centre ('NCSC') which are adverse to Apple. However, when considering Apple's arguments regarding the importance of the patch gap issue, the CMA makes no reference to NCSC submissions that support Apple's position.[87]

78. The PDR acknowledges that "*some evidence is consistent with fragmentation being a significant security risk*".[88] For the reasons set out above and discussed in detail in Apple's response to the Working Papers,[89] this statement vastly underrepresents the scale and credibility of that evidence, which is derived from an array of sources including independent research, objective data, national security authority analysis, the CMA's own security analysts, and the NCSC. Further, the CMA appears to give greater weight to unsubstantiated assertions to the contrary from Google cited at 4.170, many of which the CMA recognizes as being irrelevant.

[82] PDR, paragraph 4.179. In that regard, Apple notes that the CMA has not disclosed to Apple material details of one of Blink's purported safeguards (in fact, Enhanced Security Mode, the Blink equivalent to Lockdown Mode is only available on Microsoft Edge), such that Apple is not able to meaningfully respond on its purported effectiveness. We note that Enhanced Security Mode disables JIT (but so too does WebKit), and the other features of Enhanced Security Mode that Apple is aware of are irrelevant to browsing on iOS, as they relate to Intel devices and/or the Windows environment. Apple also notes that the CMA is simply assuming that Blink would remain similarly able to address security risks in the future.

[83] PDR, Appendix A.

[84] Likewise, RET2's comment that "*browser exploits are rare for the average user using an up-to-date browser*" (PDR, paragraph 4.165(b)) is based on the current status quo and current major players in mobile browsing (Safari, Chrome, Firefox), which is in-part a result of the WebKit requirement. RET2's comment presumes that a browser kept up to date by the user would only be susceptible to zero-day exploits. As the patch gap analysis demonstrates, this presumption is mistaken, as browser vendors do not necessarily provide updates to users in a timely fashion (even where updates to the browser engine are available).

[85] PDR, paragraph 4.180. While the CMA quotes submissions by Google suggesting that the changes that Google has recently introduced make it harder for an app to open a browser app through the intents system (PDR, paragraph 4.169(e)), we note that this change does not affect the exploitability of a browser app which would have had access to user data.

[86] PDR, paragraph 4.175(b).

[87] The NCSC submissions on patch gap which are supportive of Apple are considered only in relation to possible WebKit remedy options; see PDR, paragraph 11.117.

[88] PDR, paragraph 4.169.

[89] PDR, paragraph 4.192.

79. Similarly, the CMA appears to adopt at face value Google's argument that iOS, as a "*closed system*", "*cannot benefit from contributions from the wider developer community in the way that Android can*",[90] despite the fact that WebKit is open source and its underlying source code (like Chromium/Blink) is open to all third parties, including security researchers, and is equally able to benefit from wider third-party contributions. Third parties, such as Sony Interactive Entertainment[91], Igalia,[92] Red Hat[93] and Figma[94] have all made substantial contributions to the WebKit engine, as indeed has Google[95].

80. In reality, the categorization put forward by Google and reflected in the PDR is oversimplified and misleading. Both iOS and Android have a mix of "open" and "closed" elements. iOS cannot accurately be described as "closed" when it has benefited from the open source nature of its code through third-party contributions, including in relation to security. Large portions of the underlying OS that Apple develops, named XNU,[96] is also open source. As previously stated, Apple also provides a large quantity of APIs to developers, as well as extension points, enabling greater customization of the user experience in each app or across the system. Similarly, Android cannot be accurately contrasted as "open". There are many aspects of the Android platform that are unique to Pixel phones or becoming a much more requisite foundation for the OS, such as Google Play Services.[97]

81. Furthermore, each Android OEM controls the customization and shipping of the version of Android on their devices, as well as when system level updates are available. In other words, even if security vulnerabilities are fixed in the open source main branch of Android, those fixes are not necessarily propagated to all Android devices.[98] As a result, the patch gap or fragmentation problem exists, not only at the browser level on Android phones, but also at the OS level. As such, many of the benefits of being "open source" (such as being able to apply bug fixes in a central common repository of source code) do not in fact apply to Android.

82. From the perspective of browsers specifically, a key difference between iOS and Android is that browser developers can develop a soft fork (i.e. a copy with only small modifications or tweaks to the original version) of the Blink browser engine for use on Android and do not have to share updates to the code that improve security and/or privacy. This can be seen in the license for Blink,[99] which makes no requirement for disclosure of modifications. By contrast, WebKit is licensed under the GNU Library General Public License (LGPL), which states that modified copies of the software may be copied and distributed if and only if modified files carry "*prominent notices stating you changed the files*", and the modified software may itself be "*licensed at no charge to all third parties under the terms of this License*". These soft forks result in browser engines with limited feature differences that are nonetheless vulnerable to exploits that target the Blink engine more generally.

83. The CMA's conclusions are therefore substantially backwards in this key regard: WebKit is the more open system as improvements are shared immediately for all iOS devices and all browsers, whereas developers can keep improvements to themselves on Android and even improvements in the main branch of Android may not be propagated by the many OEMs to the many different Android devices. This indicates an unbalanced approach to the consideration of evidence, which

[90] PDR, paragraph 4.192.

[91] For example, Fuji Hironori, a developer attached to Sony Interactive entertainment, made 826 contributions in 2023 and had made 637 contributions in 2024 up to November 7. See https://github.com/fujii

[92] For example, Carlos Garda Campos, a developer attached to Igalia made 648 contributions in 2023 and had made 885 contributions in 2024 up to November 7. See https://github.com/carlosgcampos

[93] For example, Michael Catanzaro, a developer attached to Red Hat made 515 contributions in 2023 and had made 606 contributions in 2024 up to November 7. See https://github.com/mcatanzaro

[94] For example, Devin Rousso, a developer attached to Figma, made 151 contributions in 2023 and had made 357 contributions in 2024 up to November 7. See https://github.com/dcrousso

[95] Prior to the development of Blink as a fork from WebKit, Google was one of the top contributors to the engine. See https://appleinsider.com/articles/13/02/11/apple-google-nearly-tied-as-top-contributors-to-webkit-as-adoption-expands

[96] https://github.com/apple-oss-distributions/xnu

[97] See https://arstechnica.com/gadgets/2018/07/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/

[98] See https://www.android.com/everyone/#:~:text=There%20are%20now%20nearly%201%2C300,Android%20Fragmentation%20Visualized%20%2D%20August%202015 (boasting over 1,300 brands that have produced over 24,000 different devices).

[99] https://chromium.googlesource.com/chromium/blink/+/master/LICENSE

is particularly concerning given that Google would be the primary beneficiary of any degradation in iOS's position as the safest and most private platform.

84. Finally, the CMA ignores without justification relevant Apple submissions on bounty price data, which show that the majority of iOS exploits are demonstrably more expensive than similar exploits for Android, in part because it is more difficult to create and perpetuate exploits on iOS.[100] Given the attractiveness of the iOS platform as a target (including because of its use by governments due to its recognized level of security[101]) it is inevitably of high interest to attackers, leading to greater demand. The PDR here strays into uncritically repeating arguments that bounties are higher and CVEs correspondingly lower because Google has made greater efforts to discover attacks (rather than the supply of exploits being plausibly higher on Android) and that the CMA should draw the opposite conclusion to that indicated by the evidence, despite both Apple and Google maintaining mature security teams and bug bounty programs.[102] This would clearly be wrong. In the absence of compelling evidence suggesting that WebKit is less secure (which the PDR has not found), the CMA should draw the straightforward conclusion that the bounty data indicates it is more difficult to successfully attack iOS, and that, at a minimum, iOS is no less secure.

85. Apple urges the CMA to revisit its consideration of the evidence on security outcomes, and its approach to the weighting of such evidence, in line with the submissions above.

E. The CMA's assessment of HSWAs is inconsistent and flawed

86. Apple welcomes the CMA's findings that there is limited evidence that WebKit's approach to fixing bugs and security issues has an adverse impact on web developers,[103] a complaint which has been raised in the context of HSWAs in particular. Apple has explained that it releases updates to fix bugs and security issues in a regular and timely manner that is responsive to both developers' requests and the seriousness of the issues at hand.[104]

87. Nonetheless, the CMA's provisional findings on HSWAs, which it refers to as Progressive Web Apps ('PWAs'), do not reflect the entirety of the evidence and are substantively flawed.

88. Contrary to the CMA's provisional findings,[105] Apple has identified limited appetite from browser vendors for HSWAs. This reflects the apparent limited user desire for HSWAs, with evidence submitted by Apple showing that in November 2023, HSWAs represented [✂] of all time spent on iPadOS and iOS.[106] This suggests that HSWAs are not a material parameter of competition. Further, and contrary to the CMA's provisional findings on this point, the WebKit requirement does not suppress innovation or HSWA development.

89. The CMA refers to outdated evidence from 2022 to support its conclusions on Apple's support for HSWAs.[107] In fact, Apple has made numerous investments to lower the overall costs of development on iOS, and to HSWAs in particular. This includes offering an array of tools and documentation and conducting outreach with developers.[108] Further, as the CMA noted, in iOS 11 Apple introduced support for key web app and HSWA technologies and in iOS 17 Apple added further support for HSWAs.[109] Apple has recently significantly extended functionality for web app

[100] The CMA has not recognized the connection between the price of exploits and the patch gap issue. In particular, once vulnerabilities are in the public domain there is essentially infinite supply of that vulnerability, such that the price goes to zero. Market forces are therefore likely to significant increase the chances of patch gaps being exploited.

[101] iOS is currently the only mobile platform certified by Germany's BSI (the German federal office for information security) for handling classified information: https://support.apple.com/guide/certifications/national-regulations-security-certifications-apc37dae516c6/web

[102] PDR, paragraph 4.171.

[103] PDR, paragraph 4.120.

[104] The CMA's evidence on bug and feature requests at paragraph 4.60 of the PDR conflates requests for bug fixes and requests for new features. The third party comments on bugs in the paragraph do not refer to specific bugs, and therefore Apple has been prevented from effectively responding to these accusations.

[105] PDR, page 19.

[106] [✂].

[107] PDR, paragraph 4.108.

[108] Apple's response to Working Papers 1-5, para 101-105.

[109] PDR, paragraph 4.87.

developers (which includes Push Notifications, Badging, Offscreen Canvas and Screen Orientation), all of which has been very well received by the developer community.[110]

90. Importantly, while the PDR notes Apple's security and privacy concerns with HSWAs, it does not give due regard to the legitimacy of such considerations when determining the appropriate level of access for HSWAs. This is inconsistent with the PDR's analysis of access to browser features, where it expressly recognizes that in a well-functioning market security and privacy considerations may impact the approach to granting access to third parties.[111]

91. One of the risks identified with respect to HSWAs is that they create "*trust and safety risks*" because they may be "*malicious and fake apps that look like legitimate apps*".[112] This simple statement significantly understates the concern that Apple has with respect to HSWAs. Apple has expended enormous effort to earn its reputation as a high-quality, safe and trusted platform on which to download and interact with digital content. Key to that reputation is Apple's curated approach to app distribution subjecting all apps to App Review. From its inception, this requires that, for apps made available on the App Store, all app functionality is reviewed before an app can be made available to users. Users have come to rely on this level of protection. HSWAs do not go through App Review and thus bypass Apple's App Review protective measures.[113] Nonetheless, as Apple has demonstrated to the CMA, they have the "look and feel" of a native app and, based on over a decade's worth of positive experience with downloading native apps on iOS, users may have an unwarranted sense of security with respect to HSWAs which can open them up to considerable risk of fraud and malicious activities.[114]

92. HSWAs also create additional risk vectors. For example, HSWAs are also potentially capable of accessing a user's microphone, camera, or location.

93. Further, the evidence the CMA relies on concerning the security implications of HSWAs is unsound. Importantly, the NCSC submissions should not be considered probative as regards iOS, as the NCSC explicitly caveats that its views are "*not based on knowledge of any specific platform, and as such does not address issues posed by potential architectural changes that might be required to implement PWA interoperability with alternative browser engines on iOS in particular*".[115]

94. With respect to iOS, the CMA's reliance on the RET2 statement that web apps are not necessarily riskier than native apps because web apps "*are better protected against memory corruption attacks than native apps, a protection due to the different types of programming language they use*" is misplaced and ignores the substantive threats from fraudulent or malicious web apps,[116] which are much more common than memory corruption-based attacks. In any event, the statement is also technically incorrect in the vast majority of cases. On iOS, native apps are now regularly written using the Swift programming language, which is a memory safe language that has existed since 2014. Browsers themselves are still primarily written using non-memory safe languages such as C++, and attackers are regularly able to exploit memory safety issues across multiple engines - despite the "sandbox" that technologies such as Javascript and WebAssembly provide. The regular exposure of browsers to untrusted data from the internet also leads to a much broader attack surface than the vast majority of native apps.

95. Apple is not alone in having concerns regarding the security risks associated with HSWAs. For example, the security concerns arising from features that HSWA developers would like access to, such as Web Bluetooth, WebNFC and WebUSB, are such that Mozilla has determined that it will

[110] Supplemental Response to Statement of Issues, dated 23 February 2024, paragraph 9.

[111] PDR, paragraph 5.97.

[112] PDR, paragraph 11.113(c).

[113] This issue is misunderstood or consciously ignored by, for example, OWA's complaint that simply because the WebKit sandbox is more stringent than the sandbox for native apps, there is no justification for providing less access to functionality than to native apps (PDR, paragraph 4.174(a).

[114] For example, this report from a security firm sets out case studies of malicious uses of HSWAs purporting to replace users' bankings apps, being spread through phishing techniques: https://www.welivesecurity.com/en/eset-research/be-careful-what-you-pwish-for-phishing-in-pwa-applications/

[115] See PDR, footnote 2016.

[116] See PDR, paragraph 4.175(a).

not support these features on its browsers.[117] With respect to Web MIDI, Mozilla has indicated that support is limited to cases where the user has deliberately installed a site-specific add-on to enable the capability and not in the *"casual and low trust context of ordinary websites"*.[118] This demonstrates the risks of giving unrestricted access to HSWAs of features which are available to native apps: a native app, which is deliberately installed by the user and has been pre-approved by the App Store can be trusted by the user to a much greater extent than an ordinary website.

96. For iOS, therefore, the CMA is wrong to conclude that web apps do not raise significant security concerns as compared to native apps. Given the above, we urge the CMA to revisit its consideration of HSWAs and acknowledge the reasonableness of Apple's approach in providing feature support for and access to such apps.

F. WebKit fosters competition on privacy and prevents a race to the bottom

97. Apple welcomes the CMA's recognition that WebKit provides benefits both to users and developers in establishing a baseline protection of device-level privacy.[119]

98. However, the CMA does not appear to appreciate the important role that this plays in constraining those developers who, absent the WebKit requirement, would likely offer apps on iOS with lower privacy protections when browsing the web (for example, advertising-led businesses such as Google and Meta).[120] The PDR states that such flexibility may be *"particularly relevant where users may have different preferences around privacy, which are not in line with Apple's approach."*[121] This assertion conflicts with the evidence Apple has provided that users choose iPhone and iOS in large part because of Apple's commitment to high security and privacy protections.[122] The WebKit requirement therefore precludes a "race to the bottom" on privacy.

99. That assertion also reflects the CMA's idealized "well-functioning market", which builds in an assumption that competition on privacy based on multiple browser engines will <u>necessarily</u> lead to better outcomes. However, the PDR contains quantitative evidence concerning privacy outcomes across browsers on iOS and Android which cuts across that assumption, further validating Apple's approach. Based on the CMA's interpretation of test results from 'PrivacyTests.org' the PDR states that *"[s]even out of the nine [browsers] that are available on both platforms passed more tests on iOS than on Android, indicating that the WebKit restriction ensures these mobile browsers provide greater privacy protections."*[123] It further states that the worst scoring browser on iOS passed significantly more tests (36) than the worst scoring browser on Android (28). The PDR does not recognize the clear implications of this evidence, namely that the real conditions of competition demonstrate that the WebKit requirement promotes competition and leads to better privacy outcomes.

G. Conclusion

100. Apple is concerned that the CMA has not given due weight to the possibility that the WebKit requirement can lead to effective outcomes because it has adopted an unrealistic and idealized benchmark against which to assess Apple's approach. Under this approach, the CMA has overlooked significant issues that would arise in its chosen counterfactual such as the patch gap

[117] See https://mozilla.github.io/standards-positions/ This page was originally brought to the CMA's attention at paragraph 107 to Apple's response to the MEMS Interim Report. For example, Mozilla's rationale for not supporting Web Bluetooth is set out as follows: *This API provides access to the Generic Attribute Profile (GATT) of Bluetooth, which is not the lowest level of access that the specifications allow, but its generic nature makes it impossible to clearly evaluate. Like WebUSB there is significant uncertainty regarding how well prepared devices are to receive requests from arbitrary sites. The generic nature of the API means that this risk is difficult to manage. The Web Bluetooth CG has opted to only rely on user consent, which we believe is not sufficient protection. This proposal also uses a blocklist, which will require constant and active maintenance so that vulnerable devices aren't exploited. This model is unsustainable and presents a significant risk to users and their devices* (https://mozilla.github.io/standards-positions/#web-bluetooth).

[118] https://mozilla.github.io/standards-positions/#webmidi

[119] PDR, paragraph 4.198.

[120] To the extent developers such as Brave have raised issues around the ability to implement privacy-related features, this is a matter of feature access and/or support rather than a reflection of Apple forcing developers to adopt its 'view' of privacy, as the CMA asserts. Apple's responses to such issues are set out in Section IV.

[121] PDR, paragraph 4.199.

[122] Apple's ordinary course survey evidence shows that the vast majority of users place a high priority on the parameters of privacy and security. Factors such has "Security and privacy of your information" are consistently ranked as "extremely important" by the majority of iPhone buyers and iPhone users.

[123] PDR, paragraph 4.200.

issue and effectively relegated the consideration of WebKit's security and privacy benefits to a possible countervailing "efficiency". This inevitably means that the CMA's assessment falls short of the requirement to consider these key factors with appropriate "depth and sophistication", as required under applicable caselaw.[124]

101.We urge the CMA to recalibrate the benchmark it uses to assess the WebKit requirement and to take proper account of its security and privacy benefits as part of an analysis that is more grounded in market realities. We feel strongly that if the CMA continues down its current path, it risks causing significant harm, to competition at both the device and browser level, by removing an essential competitive differentiator between the iOS and Android platforms and limiting user choice.

IV. ACCESS TO BROWSER FUNCTIONALITIES

102.As set out above, Apple's driving economic incentive is to make its devices as attractive to users as possible by providing them with access to a wide range of high-performing, safe and useful apps, including third-party browsers. Put simply, Apple has a vested interest in the success of third-party browsers and third-party browser developers. The PDR's assessment of access to browser functionalities is simply inconsistent with this overarching incentive and with the objective evidence.

A. The CMA's analytical approach is fundamentally inaccurate

103.The analysis in the PDR contains two fundamental omissions which result in a wholly one-sided and inaccurate view of Apple's approach to providing third-party access to browser functionality. First, the CMA does not sufficiently consider the vast array of functionalities that Apple makes available to third-parties (enabling them to develop their own features both to compete with - and differentiate from - Safari). Second, the CMA does not acknowledge features and functionalities developed by Apple for the benefit of third parties using WebKit, that are not available on other browser engines, such as Blink.

104.The CMA's analysis turns on a handful of features for which developers have raised complaints, the majority of which have already been addressed by Apple in the ordinary course of business (demonstrating no persisting competition issue and no need for remedial action).[125] To put this in context, Apple has provided the CMA with a list of over 300 WebKit features and enhancements which were made available in Safari between March 14 2022 and April 2 2024, of which only one feature (for which third parties had alternative means of implementing) was not made available to third parties at the same time.[126] The vast majority of features made available to third-party browser vendors have not been the subject of any complaints and are, and have always been, available to third parties in the same way as they are to Safari. Further, third party access to Background Upload and Download was recently introduced as part of the iOS 18.2 release, addressing any possible concerns in relation to that feature. The above demonstrates that the already *de minimus* number of features where third parties do not have access is continually decreasing.

105.These features either give developers access to the same functionality as Safari or enable them to build equivalent functionality. Not only can they offer the same features as Safari, but also they can go further and offer additional functionality. Examples include: (i) automatic free VPN capacity (offered by Brave, Opera, Microsoft Edge); (ii) advanced customization options (offered by Vivaldi, Arc); and (iii) advanced ad blocking facilities (offered by Brave), as well as UI focused functionalities such as side tabs, favorites, bookmarks, extensions, and profile management.

106.There is no reasonable basis for concluding - as the CMA does - that the impact of the small number of features about which developers complained and on which the CMA focuses would

[124] *Barclays Bank plc v Competition Commission* (2009), CAT 27 (paragraph 21); citing *Tesco v Competition Commission* (2009), CAT 6 (paragraph 139).

[125] For completeness, Apple disagrees with the CMA's provisional conclusions (PDR paragraphs 5.56, 5.73, and 5.88) that equivalent access to a number of these features has not been provided or that the evidence relating to such access is unclear.

[126] [✂]

outweigh the competitive importance of the hundreds of features that Apple has added and that have never been the subject of any complaint. The notion that Apple is holding back the development of competing mobile browsers on iOS is further in clear tension with the fact that approximately 100 browsers are present on iOS in the UK, each advertising and promoting its own feature set.

107.The fact that Apple allows functionality on WebKit that is not available on Blink or was later developed in Blink is further evidence that the CMA's view that Apple has held back access to functionality is unwarranted. For example:

- WebKit provided support for additional media formats such as JPEG XL when Blink had refused to;[127]
- WebKit was first to support developer-revised Shadow DOM;[128]
- WebKit was first to integrate support for accessibility standards for users that have vestibular disorders,[129] over a year before Blink/Chromium;[130] and
- WebKit developed the first implementation of the "has" operator in CSS that allowed developers flexibility in design.[131]

108.Further, recent analysis carried out on behalf of Apple demonstrates that the iOS (i.e. WebKit) versions of Chrome and Firefox are faster than the Android versions (i.e. Blink and Gecko) on comparable devices.[132]

B. *The CMA's approach to the timing of access is inconsistent and unsupported*

109.The CMA's own provisional conclusions recognize that, in fact, Apple does provide equivalent access to the majority of the features that the CMA has considered in the PDR.[133] As a result, the CMA cannot have concerns about the current state of access to those features.

110.Further, the CMA acknowledges that in a well-functioning market for mobile browsers on iOS, equivalent access to functionality in limited circumstances may permit a delay[134] to mitigate security risks. Apple agrees that functionality cannot always be immediately made available to third parties. Releasing an API to third-party developers is a significant commitment. In the first instance it involves developing and thoroughly testing the API. It also entails committing to: (a) providing the functionality for the long term; (b) documenting the API; (c) not arbitrarily changing the underlying code; and (d) creating a consistent endpoint that developers can rely on. These commitments must reflect the fact that Apple must support the broad set of use cases for which it anticipates third-party developers may want to use an API, which can often differ greatly from the use case for which Apple originally developed the API. Accordingly, there is sometimes a delay in rolling out APIs while Apple ensures that it can satisfy these commitments.

111.Further, some features are more difficult to make available to third parties than others. This is particularly true of features that have the potential to impact users' security and privacy. Such features usually require rigorous testing before they can be safely deployed to third parties. This is because, unlike with Safari, Apple cannot control how this functionality will be used by third parties. This is particularly problematic if the functionality provides a level of device or OS access that could be abused by bad actors, creating a significant risk vector.

112.As a concrete example, an independent study found that there were two distinct ways websites could exploit service workers to determine which third-party websites a user has already visited and/or has an account for. Although the CMA acknowledged the study,[135] the impact of this issue has been hugely understated. Knowing what websites a person visited and has an account for

[127] https://www.theregister.com/2023/06/07/apple_safari_jpeg_xl/

[128] https://webkit.org/blog/6017/introducing-safari-technology-preview/

[129] https://webkit.org/blog/7551/responsive-design-for-motion/

[130] https://chromium.googlesource.com/chromium/src.git/+/53c0f16b7423f39b2b55bd6896c3d6a2c5800bd4

[131] https://developer.mozilla.org/en-US/docs/Web/CSS/:has#browser_compatibility

[132] Analysis undertaken using https://browserbench.org/Speedometer3.0/

[133] See PDR paragraphs 5.56, 5.73, and 5.88.

[134] PDR, paragraph 5.126.

[135] PDR, paragraph 4.172.

can be a huge breach of privacy.[136] Notably, the independent paper found that WebKit was the only browser engine that was ***not*** vulnerable to these attacks. This significance of this privacy protection should not be underestimated.

113.Further, while the CMA recognizes in principle that sometimes a delay is warranted to address a feature's security or privacy risks, it does not recognize the practical realities of software development timelines. The time to find and implement the correct approach will clearly depend on the feature in question. We note that it took Google over eight years to develop its site isolation feature for Android.[137] Further, releasing features too early can result in harm to users:

- Android Play Services: a recent update on Android Play Services resulted in apps not being supported. This meant that users were no longer able to use apps after the update.[138]
- Chrome: an update to Google's password manager resulted in the password manager being unavailable for an estimated over 17 million users.[139]

114.The CMA's view on timing is affected by its lack of engagement with how certain features are developed: "*[t]his chapter does not seek to specify the level within the software stack that access may be required for particular functionalities…it does not affect the analysis of the impact on competition set out below*".[140] An example of the complexities of feature development is Smart App Banner functionality. As Apple has previously set out, this functionality relies on the ability to identify the apps installed on a user's device, which creates a significant threat vector due to the risk of "fingerprinting". Certain apps, like those for dating, pregnancy, health conditions, and political views by their very presence on-device reveal highly personal information. Revealing this information to third-party app developers presents substantial privacy risks. And, if bundled engine IABs are allowed on iOS, ***any*** app, not just web browsers, would be able to identify apps on a user's device. Apple is not aware of a ready way to implement this functionality without providing enhanced access to all apps or any way to mitigate the associated risks, regardless of the amount of development time allotted.

115.Third parties, such as Meta, who have made submissions to the CMA, are also incentivized to advocate for greater ability to track and fingerprint users' activities on their devices beyond what they are currently able to do, for the purposes of targeted advertising. We note that these third parties are likely to consider the possible threat vector consequences of greater access as a secondary issue (if at all) to tracking users' activities on their devices.

116.The CMA effectively ignores the important fact that Apple has granted access to the majority of features with which the CMA is concerned: it provisionally finds that Safari having earlier access to some such features "*is likely*" to contribute to a perception that "*it is a better mobile browser to use to access more innovative features on iOS*"[141] making it more difficult for competing browsers to attract users. This conclusion is not supported by evidence, and is inconsistent with the realities of market development and user behavior in digital markets such as this, where capabilities are constantly improving and users move to "the next new thing" with ease. The PDR does not point to survey data or other evidence which backs up the CMA's views on the perceptions of users. It is also inconsistent with the PDR's approach to cloud gaming, where the CMA rightly recognizes that recent developments in Apple's App Store Guidelines have facilitated market entry and removed any concern of an AEC. In a market investigation, which is fundamentally forward looking (as compared, say, to an investigation under the Competition Act 1998, which is focused on past conduct), this is clearly the correct approach. The assessment of access to features is fundamentally at odds with this.

[136] For example, many websites can reveal personal information about the user, such as websites for dating, political views, healthcare, and pornography or other inappropriate content. Infamously in July 2015, the website Ashley Madison was hacked and many users seeking extramarital relationships were revealed. The same kinds of revelations are possible using the service worker vulnerabilities discussed in the study.

[137] The site isolation study cited by the CMA in footnote 494 of the PDR dates from 2017, i.e. it is over seven years old. If site isolation really was one of the most important security features that a web browser should have, as the study suggests, then there would have been tangible harm to iOS users that the CMA or third parties could point to as a result of it not being supported. There is none.

[138] https://www.forbes.com/sites/zakdoffman/2024/11/04/gmail-suddenly-stops-working-new-warning-as-google-update-goes-wrong/

[139] https://www.theregister.com/2024/07/29/google_password_manager_outage/

[140] PDR, paragraph 5.9.

[141] PDR, paragraph 5.102.

C. *The CMA's approach incorrectly assesses the competitive importance of features*

117.The CMA itself recognizes that some of the features to which Apple has not granted access or to which it has only granted access after some time, are unlikely to be of equal competitive significance: "*some of these features may, taken individually, be less important than others*".[142] However, the CMA suggests that the relative importance of some of these features can be bolstered by their "*cumulative impact*"[143] on access to browser functionality. This does not follow. The CMA cannot simply add a series of unimportant - and in many cases, unrelated - features together and presume that they collectively become significant without further analysis. Users will not develop more regard for insignificant features, simply because there are more of them. The fact that third parties may not be able to access some insignificant features will not have a negative impact on competition. The insignificance of the respective features should have been reflected in the CMA's analysis.

D. *The CMA's provisional findings on developer engagement and transparency do not reflect the available evidence*

118.The CMA's provisional conclusion that Apple does not provide sufficient documentation and support for APIs on iOS does not reflect the evidence available. Apple provides hundreds of thousands of pages of documentation and the source code for WebKit is open source (i.e. freely available to the public).[144] It is unclear what more can be expected: the PDR suggests that Apple's documentation is insufficient, but does not provide a benchmark comparison to that of other platform operators. Nor has it provided any other indication of what sufficient documentation should look like. For example, the PDR does not evidence a better track record on the part of Google or Firefox in terms of engagement on the Blink or Gecko platforms which would provide a basis for the CMA to conclude that documentation would necessarily be better in a counterfactual where the WebKit requirement is absent. The approach in the PDR suggests that the CMA has not properly considered the issue and does not, therefore, have any real basis on which to reach its provisional conclusion.

119.As Apple has shown, it invests vast resources into developer engagement and transparency. This is a core principle of Apple's approach to app development and is reflected in its approach to API and WebKit documentation.[145]

120.Further, the evidence cited by the CMA to support its findings applies an unrealistic standard for developer engagement and transparency. For example, the CMA refers to a "*mobile browser vendor*" which complains about the "*extra effort*" required to implement features.[146] In support of this complaint, the vendor claims it is disadvantaged because Safari can "*liaise directly with the teams creating or updating APIs*".[147] Apple demonstrably <u>does</u> have a wide range of developer relations contact with browser vendors, which allows for one-to-one conversations about technical development of features and functionality for browsers on the iOS system, particularly for those features that may not be sufficiently self-explanatory and/or sufficiently covered by the documentation on Apple's developer web pages. Apple's extensive outreach to developers includes blog posts, iOS and Safari release notes documentation, WWDC homepages, developer sessions and forums, webpages, and the Beta Software Program. However, to expect Apple to have exactly the same level of internal and external communication is a wholly unrealistic and inappropriate standard by which to assess Apple's support for developers.

E. *Access to browser extensions*

121.With respect to browser extensions, Apple disagrees with the CMA's underlying provisional conclusion that there is limited support for browser extensions on iOS. It also disagrees with the CMA's provisional view that this is an outcome of the limited competition between browsers on iOS and the suggestion that Apple faces limited competitive constraints on Safari and therefore

[142] PDR, paragraph 5.57.

[143] PDR, paragraph 5.57.

[144] https://developer.apple.com/documentation/webkit; https://webkit.org/getting-the-code/

[145] Apple's response to Working Papers 1-5, paragraph 156-158.

[146] PDR, paragraph 5.92.

[147] PDR, paragraph 5.92.

has less incentive to compete vigorously for users by offering features such as browser extensions.[148]

122.Safari supports dozens of browser extensions. Further, as Apple has detailed in previous submissions, developers are able to build web extension functionality on WebKit.[149] In certain limited circumstances, to protect users' safety, security, privacy, or device reliability, Apple will implement additional safeguards for the introduction of web extensions. These safeguards are necessary and proportionate to mitigate such risks.

123.However, Apple agrees with the CMA's provisional finding that there is limited evidence that browser extensions could act as an entry route into mobile browsers for developers and that, as such, the evidence does not show that limited support for extensions on mobile platforms increases barriers to entry.[150] This demonstrates that in any case the CMA's concerns are, at best, theoretical.

F. Conclusion

124.The CMA's provisional findings are wrong to suggest that Safari has "*wider and more immediate*" access to functionality in a way that harms competition. The CMA has only identified a de minimis number of features that are not available to third parties, could not be built by third parties or that have been made available with a delay. The vast majority of necessary capabilities or features sought are provided to browser developers in the ordinary course of business. There are appropriate security justifications for Apple's approach, which warrant material weight given their recognition within the CMA's description of the well-functioning market. The CMA has, in any event, not shown how the features about which it has concerns are likely to adversely impact competition. The CMA must contextualize its analysis taking due account of these factors in order to reach an objective and proportionate view.

V. CHOICE ARCHITECTURE

125.Apple welcomes the CMA's conclusion that the inability to uninstall Safari does not contribute to an AEC. As previously submitted, this theory of harm was speculative and without foundation.

126.However, we note that the CMA has provisionally concluded that the choice architecture both in terms of the factory settings of an iOS device and the switching journey contribute to the AEC that it has provisionally identified in the market for mobile browsers on iOS. Apple reiterates its previous submissions that its existing choice architecture provides a seamless and intuitive user experience and that the CMA's evidence base does not support the provisional conclusions it has reached.[151] The CMA's provisional findings appear to benefit browser vendors at the expense of users, contrary to the CMA's overarching policy goals.

A. A choice screen is not a precondition of a well-functioning market

127.There is no foundation for the provisional conclusion that presenting users with a choice screen when they first use a mobile device is an essential characteristic of a well-functioning market.[152] Instead, in a well-functioning market one would expect that users are presented with products that meet their preferences and expectations.[153] This is already the position with respect to iOS and the evidence does not show that changes are warranted.

128.Further, it is possible that the user experience would be degraded by a choice screen. As the CMA points out, "*prompts may require users to take immediate action (known as 'forced action')*

[148] PDR, paragraph 6.22.

[149] Apple's response to Working Papers 1-5, paragraph 152.

[150] PDR, paragraph 6.15.

[151] For example, the ability to change the default browser is in the "settings" tab of every browser, as well as in the new single "defaults" settings page launched with iOS 18.2 (see paragraphs 149-150 below), which makes changing the default settings on a browser extremely straightforward. Apple users also quickly become familiar with how to use the App Store to access apps with additional functionality to that made available upon installation, and as the CMA has shown, the average user is aware of alternative options, *before* they search for a browser (see PDR, paragraph 8.44(a)). See also [✂]

[152] PDR, paragraph 8.121.

[153] For this reason, the CMA should have tested if iOS users are happy with the current choice architecture or would prefer an alternative one - but despite Apple's suggestion to elicit user preferences in the CMA's consumer research, the CMA did not do so.

(…) and may lead [users] (…) to accidentally making less effective choices".[154] Users who are not already familiar with the selection of mobile browsers presented in the choice screen may therefore select a browser at random in order to get on with using their device, and then realize later that they want to return to their original browser. In such a case, they would thus have been "forced" to make unwanted changes rather than having the ability to use the best browser for them straight out-of-the-box. Independent research suggests that in circumstances like these, consumers are likely to be better off if no choice screen is shown.[155]

129.Outside the mobile context, the browser choice screen agreed in the EC's *Microsoft (Tying)* case[156] provides an illustration that market structure is primarily driven by browser quality, not by forced choice architecture. Several studies found that the imposition of a choice screen in this case did not have a significant impact on browser choice.[157] One comprehensive study[158] found that the choice screen had a negligible impact on Internet Explorer's market share using browser market share changes in United States, Canada, New Zealand, and Australia as a control group. Another study[159] noted that Internet Explorer's market share was already declining before the EC's remedy was implemented in early 2010 and continued to decline at around the same rate, implying that the choice screen itself had limited impact.[160]

130.This further supports the view that it is incorrect for the CMA to proceed on the basis that choice screens are somehow an essential characteristic of a well-functioning market or are necessary for users to be able to determine which browsers they would like to use.

B. The CMA's analysis of pre-installation of third-party browsers is purely theoretical

131.While the PDR recognizes that the out-of-the-box experience resulting from Safari being pre-installed carries some benefits to users, it concludes that Apple's practices of pre-installing only Safari contributes to low user awareness of other browsers.[161] Not surprisingly, the PDR remains vague as to how it arrives at this conclusion. While it discusses findings on browser use and installations in great detail, it does not present reliable evidence showing that the mobile browser usage patterns would be driven by lack of awareness. Instead, it disregards the evidence suggesting that about 95% of iOS users are aware of alternative browsers,[162] and most Safari users simply prefer Safari over other mobile browsers or saw no reason to switch to another one. The CMA appears to devalue this evidence based on a small proportion of seemingly inconsistent responses observed in the Verian survey,[163] which, however, do not affect the results and conclusions meaningfully.[164] The only conclusion supported by the evidence therefore is that iOS

[154] PDR, para. 8.30.

[155] Jacob Goldin, Daniel Reck; Optimal Defaults with Normative Ambiguity. The Review of Economics and Statistics 2022; 104 (1): 17–33. doi: https://doi.org/10.1162/rest_a_00945

[156] Case AT.3953. Microsoft Windows users who had Internet Explorer as a browser were provided with a browser choice screen, which was designed to give users an effective and unbiased choice between their existing default and competing web browsers. From March 2010 until the end of 2014 (apart from a brief period where the Choice Screen was not presented), Internet Explorer users were presented with the option to download one of five alternative browsers (see the commitments agreed in December 2009 https://ec.europa.eu/competition/antitrust/cases/dec_docs/39530/39530_2550_8.pdf).

[157] Apple notes that, while the case is used as an example in the CMA's choice architecture paper, the paper contains no evaluation of the effectiveness of the remedies.

[158] Duque, Active Choice vs. Inertia? An exploratory assessment of the Europe Microsoft Case's Choice Screen, Journal of Competition Law & Economics, 2023, 19, 60–74. This study also pointed to Firefox's market share in 2009 and 2010 as evidence that if users really do prefer a non-default browser then they will switch to it regardless of the choice screen.

[159] Heiner, "Microsoft": A remedial success? Antitrust Law Journal, 2012, Vol. 78, No. 2 (2012), pp. 329-362.

[160] Post-2014 no choice screen has been present on desktop browsers, however the market has not returned to the status quo as Microsoft has been unable to reestablish with Internet Explorer and, subsequently, Edge the market share which it previously enjoyed prior to the introduction of a choice screen.

[161] PDR, paragraph 8.124.

[162] Verian Report, Mobile Browsers Quantitative Consumer Research Findings, slide 31: over 95% of Apple users questioned had heard of 2 or more browsers when prompted. Were a user to search the App Store for a "browser", they would be prompted with various options.

[163] PDR Appendix C, paragraph 4.2 and 4.3.

[164] [✂] contains an analysis of the Verian Survey results at issue, which that finds those results are robust to the exclusion of the allegedly inconsistent or unclear responses, indicating that they are not impacted by systematic biases or other methodological issues that would suffice to disqualify or discount them as non-probative. As such, those results are robust despite the limited number of potentially unclear or inconsistent responses. We note that the PDR does not even attempt to apply any meaningful correction or sensitivity testing in this regard.

users are already aware of alternative browsers and that pre-installation therefore has limited to no effect on browser awareness levels.

132.The CMA's analysis also recommends addressing this unsupported concern by making a browser choice screen available immediately on device set-up. This would significantly worsen the user experience by forcing users to make a browser choice at an unwanted time. Apple believes that, when setting up a new phone, users want to use the phone as soon as possible. Apple therefore attempts to ensure that users have as few steps as possible between turning the phone on and being able to use it. The CMA's proposed approach would worsen the user experience for the hypothesized and hypothetical benefit of browser vendors, which would be contrary to its pro-consumer objectives.

C. Treating newly-downloaded browsers in the same way as other new apps does not disfavor them

133.The CMA has also suggested that the prominent placement of Safari results in users being less aware of alternative browsers and less likely to engage with them at device setup.[165] The evidence does not support such a provisional conclusion.

134.Such a conclusion would also be at odds with the evidence relating to other apps. On device setup, four apps (Phone, Messages, Music and Safari) are placed in the Dock. The success of alternative messaging apps such as WhatsApp and alternative music apps such as Spotify belies any reasonable suggestion that mobile browsers are unable to compete effectively with Safari due to Dock placement.[166]

135.The CMA relies on a series of papers that address the impacts of placement on behavior in various circumstances, such as stock picks, surnames and trading behavior.[167] However, there is no basis on which to argue that behavior in such unrelated circumstances would be probative for its analysis of browsers. Where the CMA has cited sources considering browser usage[168] these are equally uninformative, as they do not address the issue the CMA is considering, namely user behavior and expectations following the conscious choice to download and test out a browser.

136.The CMA's presumption that users who consciously downloaded an alternative web browser (via some choice screen or the App Store) would fail to put it into a salient and easily reachable location on their home screen is based on weak evidence. As with any other app, newly downloaded browser apps appear in the next available slot on a fully customizable home screen. This is exactly where users (who are likely to download numerous smartphone apps on Android or iOS) will expect to find them.

137.As the Verian survey clearly shows, the vast majority (77%) of users who downloaded a browser repositioned it,[169] which is fully consistent with users capable of customizing their home screen[170] and inconsistent with the CMA's assertion that users are essentially unable to put their browser (like any other app) in a convenient location without assistance.

[165] PDR, paragraph 8.129.

[166] Apple's research demonstrates that in the UK (a) WhatsApp enjoys a greater share of supply in terms of daily active users than Messages; and (b) Spotify enjoys a greater share of supply on iPhone than Apple Music by minutes listened to. See https://www.apple.com/newsroom/pdfs/the-success-of-third-party-apps-on-the-app-store.pdf, pages 22 and 27.

[167] PDR, paragraph 8.19.

[168] PDR, paragraph 8.21. Notably these citations are not independent research papers and consist of a paper by a CMA board member and the CMA's own discussion paper.

[169] Verian Final Report, section 7.2. The qualitative interviews in the Verian survey also indicated that users at each end of the competence scale were least likely to be affected by the pre-existing position of a browser: indicating that, if there are a significant number of users who are not confident changing the position of their browser on their home screen, this does not affect their browsing behavior.

[170] For example, it would be wrong to assume that all users would want to arrange apps in the same way (for example based on usage). Users may want to arrange by other factors, such as aesthetic appeal and use the built in search functionality when locating an app. See, https://medium.com/macoclock/ive-sorted-my-apps-by-colour-e7b053f3a4e3; https://apps.apple.com/us/app/color-harmony-apps-organizer/id1510226740

D. The CMA mischaracterizes the evidence that it has received regarding users' ability to switch

138.Apple provides ample ability for developers to encourage users to switch their default browsers after installation, should they want to. Survey data from both Verian and the ACCC, as well as Apple's own AppleCare UK records also confirms this (see further below). Disappointingly, the CMA appears to have favored the assertions of third-party browser vendors over this evidence.

139.This is evident from the CMA's downplaying of the evidence submitted by Apple on customer feedback received between July 2021 and July 2024 on the default browser on iPhone. While these records represent less than [✂] of all AppleCare UK records over the period, the CMA notes only that "some" users have difficulty switching defaults and uses this to support its conclusion that complexity and friction in changing the default browser on iOS devices is likely to prevent users from switching.[171] It is plainly inappropriate and misleading to draw a general conclusion from the small proportion of users reporting issues with switching rather than the overwhelming majority of users who have not.

140.Likewise, the CMA has dismissed out of hand survey evidence which shows that users find switching default browsers easy, including:

- The CMA's Verian survey, which found that 78% of iOS respondents are confident that they could definitely or probably change their default mobile browser, while 89% of those who had switched reported this switching to have been "easy";[172] and
- An ACCC survey, which found that 80% of respondents know how to change their default browser while 84% of those who had switched reported this switching to have been "easy".[173]

141.Despite the extremely clear-cut nature of these survey results, the CMA has dismissed them, making general remarks on potential psychological biases of users, without showing that these are relevant in the present case.[174] This is highly concerning, as it is difficult to see how any survey data could be sufficient to overturn the CMA's provisional finding that users find switching difficult.

E. The CMA's concerns on changing default browser settings are unfounded

142.The PDR acknowledges that defaults are not necessarily problematic in isolation but considers that they prevent users from making an active choice at initial device setup when used in combination with pre-installation and placement.[175] This is inconsistent with the CMA's admission in the same paragraph that it "*cannot make direct causal inference about the impact of* [the use of defaults] *on user behaviour*".[176]

143.To demonstrate the potentially harmful competitive effect of Safari's position as default browser, the PDR refers to various studies on defaults, including a meta-analysis which suggests that a default option is 27% more likely to be chosen out of two options. However, the PDR does not consider the relevance of this meta-analysis to the current circumstances; it merely makes the point in general terms. As set out in the analysis of desktop browser market shares in the 2010s above, where a superior new product is released on this kind of market, users react quickly (given the low barriers to switching) and market shares change rapidly.

144.The PDR refers to a research study, submitted by a browser vendor, which suggests that users may not actively choose the default browser selected on their mobile device and that the system

[171] PDR, paragraph 8.175.

[172] PDR, paragraph 8.145.

[173] Australian Competition and Consumer Commission (ACCC). Consumer views and use of web browsers and search engines. Final report. Published: September 2021, Table 4.

[174] PDR, paragraph 8.148. The CMA merely suggests that the Verian qualitative research would have shown that self-assessed technical confidence may not reflect actual technical ability. However, the fact that these interviews were conducted in an artificial setting and the low number of users interviewed heavily discount the relevance of this evidence. While the CMA focuses on difficulties of finding the settings page, the prompts shown by alternative mobile browsers take users directly to this page.

[175] PDR, paragraph 8.26.

[176] PDR, paragraph 8.26.

default plays an important role in future browser usage.[177] As the CMA has not disclosed this report or the methodology it uses Apple cannot properly engage with or address the underlying analysis and the appropriateness of the CMA's reliance on it. Nonetheless, the PDR summary of this document ascribes "laziness" as a potential reason for users not changing defaults,[178] which belies an attitude that users should serve developers' interests rather than the other way around, itself a concerning indication of the CMA's approach to the weighting of evidence.

145.The PDR also suggests that those of the 39% of total iPhone users who have downloaded an alternative browser but who have not changed their default browser may have been deterred from switching their default browser due to friction in the user journey and a lack of switching prompts. This is a misinterpretation of the facts.

146.Apple's design of the default status is pro-consumer and pro-competitive, with limited and clear steps to change the default browser. As shown above at paragraph 140, users report high confidence in changing browser default settings and those who have done it have found it easy. This is inconsistent with the CMA's case that there are meaningful frictions preventing users from changing browser. Much of the evidence that the CMA has gathered in favor of an AEC appears to come from vocal browser vendors with a vested interest.[179] Further, the CMA's criticism of the user journey downplays the degree to which prompts shown by browser apps encourage users to switch, and instead selectively focusses on perceived difficulties with switching via the iOS settings menu.[180]

147.On prompts, while browser vendors may value a greater ability to push their marketing to users, the benefits for those users are considerably less clear. Indeed the CMA itself confirms that prompts can adversely affect users' browsing experiences and may lead them to accidentally make less effective choices.[181] Indeed, it criticizes Google's use of prompts on the Android system to nudge users back to Chrome.[182]

148.In any event, the PDR analysis shows that browsers are *already* able to prompt users to change their default browser, detailing the prompts shown by Google on various iOS devices, as well as DuckDuckGo, Microsoft Edge and Firefox[183] which seek to get users to change their default browser. Given that users are already being prompted to switch their default browsers, it is unclear what additional benefits to users a more intrusive prompt could provide.

149.Regardless, many of the CMA's concerns (even if valid) are addressed by iOS 18.2, which Apple released on 11 December 2024. iOS 18.2 adds a new section in Settings -> Apps, which is referred to as "Default Apps". Here, the user can change the browser default settings and the default apps for email, messaging, calling, call filtering, passwords and codes, contactless payments and keyboards.

[177] PDR, paragraph 8.115.

[178] *Ibid.*

[179] PDR, paragraph 8.140.

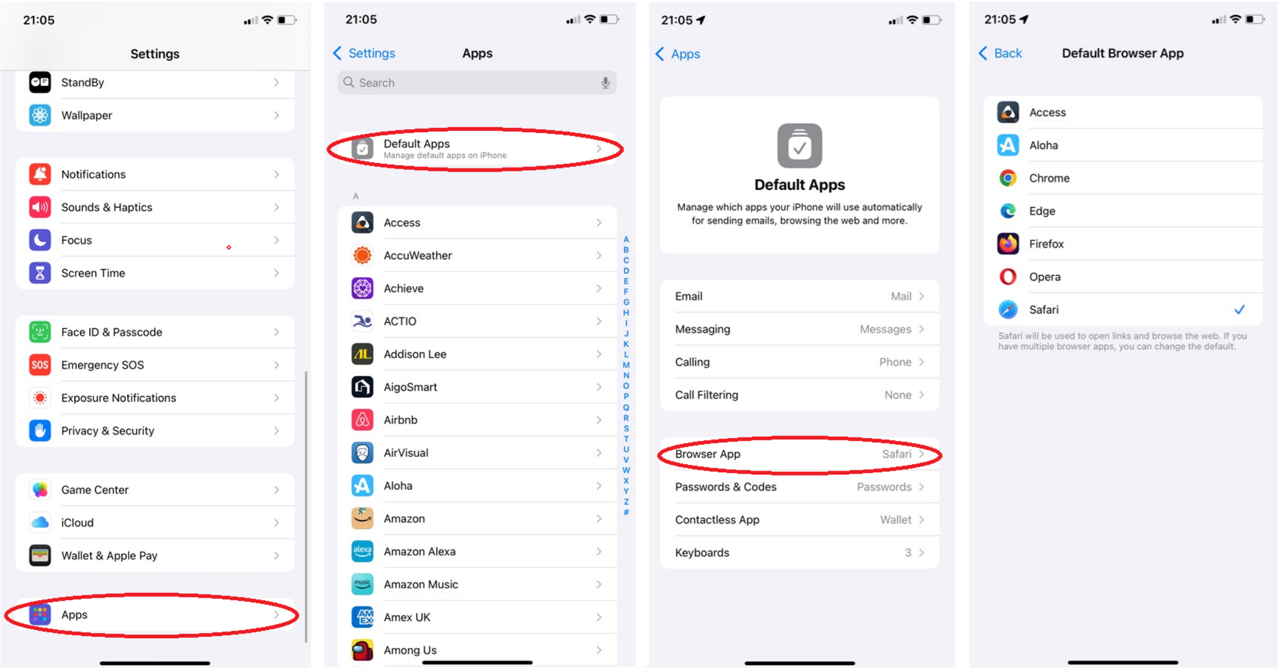
[180] The PDR recognizes that most iOS users who switched default browser saw such a prompt (PDR, paragraph 8.65).

[181] PDR, paragraph 8.30.

[182] PDR, paragraph 8.263.

[183] PDR, paragraphs 8.156 - 8.163.

Figure 1: Process for change default apps on iOS 18.2



Manage which apps your iPhone will use automatically for sending emails, browsing the web and more.

Email: Mail
Messaging: Messages
Calling: Phone
Call Filtering: None
Browser App: Safari
Passwords & Codes: Passwords
Contactless App: Wallet
Keyboards: 3

Safari will be used to open links and browse the web. If you have multiple browser apps, you can change the default.

150.As this change further addresses concerns set out in the PDR, the notion that default settings contribute to so-called "AEC 2" is even more suspect; there simply remains no need for the CMA to continue to pursue this element of its theory of harm in the Final Report.

F. Conclusion

151.The PDR's provisional conclusions on choice architecture are not supported by the evidence base. Apple is concerned that the PDR has sought to downplay and dismiss the conclusions from real-world data that users are able to quickly and easily switch their default browser if they want to, and urges the CMA to reconsider its provisional findings in light of the totality of the evidence.

VI. IN-APP BROWSING

152.Apple welcomes the CMA's provisional conclusion that no competition concerns arise in relation to the customizability and functionality of IABs based on WKWebView on iOS. However, the PDR's analysis with respect to the remaining elements of IAB competition remains incorrect in material respects, leading to unwarranted and unsupported provisional conclusions.

153.On the other aspects of the supply of 'in-app browsing technology on iOS" which the PDR addresses, the evidence shows that Apple's approach meets developers' existing demand and fosters competition. That evidence, which Apple does not seek to reiterate in full in this response, demonstrates that Apple currently offers various IAB implementation solutions to developers on iOS, with increasing degrees of control and customization.[184] Developers have a plethora of options for IAB: from a simple out-the-box functionality like SFSafariViewController through to a custom SDK.

154.Having corrected the Working Paper's misguided focus on user choice by noting in its assessment of market definition that app developers are "*the primary customers*" of in-app

[184] In brief: SFSafariViewController offers a simple "plug and play" offering with some customization, while WKWebView enables developers to create IABs with functionality equivalent to a dedicated browser. Third parties also have the ability to offer their own custom IAB offering to developers using SDKs. This is a material and relevant potential basis for entry into "in-app browsing technology" to which the CMA does not have proper regard in its analysis. It is therefore not the case as the CMA states that "*Apple's policies on in-app browsing mean that only Apple can provide IABs.*" See, for example, Apple response to Working Papers 1-5, Paragraph 168.

browsing technology,[185] the PDR's analysis should have placed significant weight on its provisional finding that "*app developers are generally content with their current options for implementing in-app browsing on iOS*".[186] That finding is a clear vindication of Apple's current approach and provides a compelling basis on which to find that no concerns arise in relation to in-app browsing technology on iOS. However, the PDR's provisional conclusions do not acknowledge this reality.

155.We note that the PDR has, in part, conflated the separate issues of remote tab IABs and bundled engine IABs. We address them separately below and request that the CMA reevaluate them separately.

Remote-tab IABs

156.As with its analysis of the WebKit requirement, the CMA's approach to its assessment does not take proper account of the benefits of Apple's SFSafariViewController IAB implementation, or of the crucial security and privacy considerations which are as applicable to IABs as to dedicated browsers.

A. There is no "ban" on remote-tab IABs

157.Apple has explained that iOS was not designed to permit a remote-tab IAB solution. There has been no affirmative action taken to limit or restrict remote-tab IABs on iOS.

158.The CMA's assessment instead proceeds on the basis that Apple has a "policy" to "ban" remote tab IABs, which is highly misleading and inaccurate.[187] First, as a matter of principle, we note that "remote tab" IAB is a solution which Android has chosen to implement for in-app browsing. It is not an objective benchmark against which mobile in-app browsing implementations should be considered. The "remote tab" formulation in the PDR is symptomatic of the CMA's Android-tinted perception and analysis of the iOS platform.

B. There is no demand from non-browser app developers for a custom remote-tab implementation on iOS

159.The PDR suggests that no browser vendor has sought to develop or distribute a custom SDK on iOS, indicating a lack of demand for such an implementation on the part of non-browser app developers. The implication of this is that, far from being insufficiently flexible for developers, the iOS environment in fact offers optionality beyond what developers are interested in utilizing for IABs.[188]

160.The CMA's provisional conclusion on remote tab IABs ignores the above and instead reaches the theoretical conclusion that allowing remote tab IABs would lead to "increased competitive pressure" on Apple's in-app and dedicated browsing offerings.[189] As Apple has previously explained, Safari is separate and distinct from SFSafariViewController, such that Safari derives no competitive advantage from app developers' choice to use SFSafariViewController. In such circumstances, it is clear that: (i) Apple has no vested interest in excluding rival "in-app browsing technologies"; and (ii) users and non-browser app developers cannot currently be experiencing harm from a lack of "competitive pressure".

161.The CMA's inclination towards finding concerns relating to demand for remote tab IABs is shown by its provisional conclusion that "*[app developers'] general lack of concern may depend on Apple's outright ban on remote tab IABs, which may contribute to them not being fully aware of the potential benefits of using this in-app browsing technology. Their lack of concern might also relate to the fact that those who use SFSafariViewController are looking for a relatively low-cost,*

[185] PDR, paragraph 3.89(c). As Apple has previously explained, It is app developers who decide whether and how they want to incorporate web content in their apps and, having made that determination, app developers that choose their preferred mechanism for accessing that web content during an in-app browsing experience. Indeed, most end-users are likely unaware when they are engaged in-app "browsing," and this is largely by design. Apple's response to the Working Papers 1-5, paragraphs 164-166.

[186] PDR, paragraph 7.86.

[187] PDR, paragraphs 7.93 to 7.95.

[188] PDR, paragraph 2.72.

[189] PDR, paragraphs 7.138(a) and (b).

easy-to-implement solution, so they may be less engaged in this area in general."[190] This reflects a strikingly paternalistic bias against the legitimate preferences of app developers. It also demonstrates a wholly theoretical approach to the assessment, ignoring the obvious conclusion that Apple's approach offers a low-cost, easy-to-implement solution to developers, which is appreciated by developers (i.e. the "*primary* customers" of IABs) and can only promote competition.

C. There are serious security and privacy issues with offering remote tab IABs

162.Apple has identified significant issues with offering a custom tabs-type approach, as this would expose communications between the relevant native app and browser app to potential exploitation by an attacker.

163.Additionally, Figure 7.1 from the PDR (reproduced below) demonstrates the significant privacy risks that can occur. Android "Custom Tabs" or remote tab IABs allow browsers to "share state" with the IAB, meaning that the browser can collect data about the user from within a third-party app and can profit from that data. Remote tab IABs place the commercial interests of browser vendors over the privacy interest of users. This contrasts with SFSafariViewController and WKWebKit, both of which provide robust privacy protections.[191]

Figure 2: Privacy risks with IAB implementations

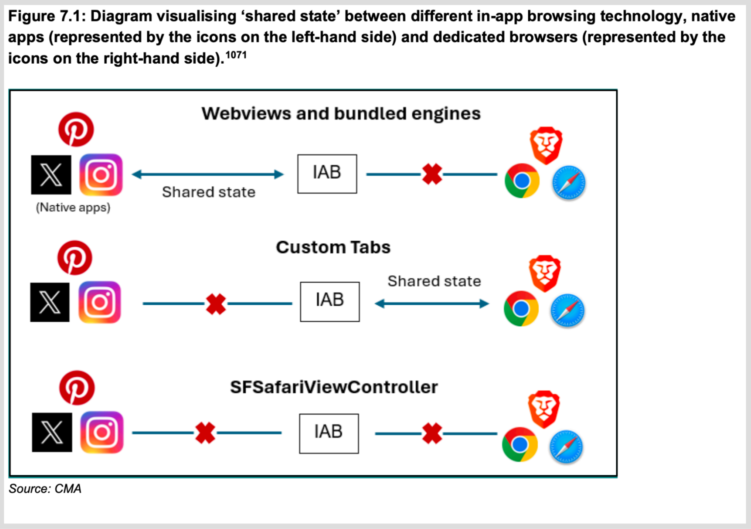


Figure 7.1: Diagram visualising 'shared state' between different in-app browsing technology, native apps (represented by the icons on the left-hand side) and dedicated browsers (represented by the icons on the right-hand side).[1071]

Source: CMA

164.The evidence base before the CMA therefore demonstrates that Apple's concerns regarding remote tab IABs do not amount to a "policy" ban on a competitive alternative but instead reflect a legitimate attempt to avoid significant security and privacy concerns. We urge the CMA to adopt a more neutral analytical framework for the assessment of remote tab IABs so that proper regard can be given to Apple's legitimate concerns about that type of IAB implementation.

Bundled Engine IABs

165.Similar to its provisional conclusions on remote tab IABs, the CMA's assessment of bundled engine IABs provisionally concludes that a "well-functioning market for in-app browsing technologies" must allow entry by third parties with bundled engine IABs.[192] This provisional conclusion is heavily based on submissions by Meta and preferences the commercial interests of Meta over user privacy.

[190] PDR, paragraph 7.138(d).

[191] For example, if a user navigates to a page during an in-app browsing experience based on SFSafariViewController, click-through advertising would be measured in a privacy-preserving way with Private Click Management. WKWebView includes the protections of ITP by default and these can only be turned off with user consent.

[192] PDR, paragraph 7.137.

A. There are serious privacy concerns related to bundled engine IABs

166.As noted above, the CMA's anticipation of possible entry based on bundled engine IABs (and indeed the desire to see such entry) is heavily based on self-interested submissions from Meta, the only company to have indicated "substantial interest"[193] in developing a bundled engine IAB. Given the paucity of corroborating evidence, it would be reasonable to expect the CMA to apply a particularly high degree of scrutiny and skepticism to Meta's submissions. However, to the contrary, the CMA's analysis appears to preference an idealized version of possible entry by Meta, and displays an alarming lack of consideration for the real-world implications of such entry.

167.For example, the CMA considers that the evidence before it "*suggests that security and privacy risks associated with bundled engine IABs depend on the app developer and can be mitigated by them if they have sufficient resources to take on this responsibility*."[194] This position, particularly as regards to privacy, is divorced from the evidence. First, the question of whether security or privacy risks are addressed by developers is, at heart, a question of commercial incentives, not resources. Apple has seen no evidence that Meta has developed any safeguards for privacy, or that it has any plans or intention to do so in future. This is unsurprising, given that Meta's advertising-led business involves maximum extraction of user data. Meta's track record shows that it has often flouted privacy laws to further such extraction.[195]

168.Apple is not the only party to raise alarm bells regarding this issue. The OWA also argue that "*bundled engine IABs present significant privacy and security concerns*"[196] and another third party raising concerns regarding Meta's own interests in this area.[197] Tellingly, even Meta itself has recognized security issues surrogating embedded browsers, and has deprecated support for Facebook login on embedded browsers,[198] presumably due to concerns regarding the inherent patch gap issue with embedded browsers.[199]

169.The CMA's analysis of the potential impact of bundled engine IABs on adjacent browsing markets is equally speculative. The CMA observes that "*if Meta offered its browser engine to third parties (ie by making the code for its browser engine open source), this would represent entry into the browser engine market, where very little entry occurs*."[200] Again, Apple has seen no evidence to suggest that Meta has such plans. Rather, as another stakeholder has observed, it is likely that "*Facebook is interested in tracking user behaviour, such that Meta's development efforts in its IAB may be aimed towards the app's business and facilitating this tracking*."[201] The CMA should take a clear-eyed view of the evidence, and of Meta's obvious commercial interests in propounding an unrealistic, hypothetical future state.

170.As the above makes clear, the CMA fails to engage at all with the real-word implications of the contemplated entry by Meta, including in particular the very real and significant harms to users' privacy that can be expected to result from such entry. The CMA's current analysis is highly theoretical and speculative, and risks leading to highly disproportionate outcomes and harm to users. It should therefore revisit its analysis afresh and recalibrate its weighting of the evidence, having proper regard to Meta's track record of privacy abuses.

171.A number of other developers have suggested to the CMA that they are not interested in developing their own bundled engine IAB, due to the complexity and size of the task.[202] Given that these companies do not consider that developing their own bundled engine IAB would be

[193] PDR, paragraph 7.62(d).

[194] PDR, paragraph 7.72.

[195] See "Select fines issued to Meta for EU data protection and privacy violations as of September 2024" available at https://www.statista.com/statistics/1192794/meta-fines-from-eu-and-dpc/, which records EUR 2.4bn in fines having been imposed during the period March 2022 to September 2024.

[196] PDR, paragraph 7.71(c).

[197] PDR, paragraph 7.70(b).

[198] https://developers.facebook.com/blog/post/2021/06/28/deprecating-support-fb-login-authentication-android-embedded-browsers/ .

[199] https://engineering.fb.com/2022/09/30/android/launching-a-new-chromium-based-webview-for-android/#:~:text=Our%20in%2Dapp%20browser%20for,Android%20and%20other%20operating%20systems

[200] PDR, paragraph 7.66.

[201] That stakeholder has further noted it it is not aware of any significant work in relation to security and performance in the context of the development of bundled engine IABs. PDR, paragraph 7.70(b).

[202] PDR, paragraph 7.60.

worthwhile, it is difficult to see who, aside from Meta, could benefit from the CMA's proposed remedy option.

172.Apple therefore asks that the CMA apply the appropriate degree of scrutiny to Meta's submissions about its plans for using such an IAB implementation and take seriously the obvious risks to users' privacy that would result.[203]

B. The patch gap issue identified for browsers is multiplied significantly for IABs, particularly for bundled engine IABs

173.The patch-gap issue that creates significant risk of harm where alternative browser engines are used by dedicated browsers[204] would be significantly higher with respect to bundled engine IABs, given the number of apps that could be impacted.[205] The recent DSIT survey referred to above at paragraph 73 shows how few app developers in the UK are even aware of the the voluntary code of practice on mobile app security and privacy for app developers. As the code is designed for general app developers (thus assuming already an implicit lower level of specialism or understanding of security and privacy), the results of the survey highlight the scale of the risk here. It would be impossible for Apple to adequately police this if apps were able to incorporate their own bundled engine IAB (a task which presumably the CMA would be even less equipped to take on).

C. Conclusion

174.The evidence before the CMA shows that Apple offers an array of competitive IAB implementations that meet user demand and are welcomed by users of IAB technology. There is little to no demand for the remote-tab or bundled engine implementations suggested by the PDR, and what demand there is raises significant concerns with respect to security and consumer privacy protection.

175.Further, the PDR's provisional conclusions display a wholly speculative approach, as they acknowledge that entry in a well-functioning market would likely be limited due to the high costs of entry and the high security requirements for IABs based on alternative browser engines, but nonetheless provisionally consider that a well-functioning market would enable significantly more competition in the supply of in-app browsing technology on iOS than we see at present.[206]

176.We urge the CMA to revisit its provisional conclusions, taking due account of the evidence of app developer satisfaction, the real security concerns with respect to remote-tab IABs and the privacy harms that could be caused by the bundled engine IAB option put forward by Meta.

VIII. GOOGLE ISA

177.The PDR chapter on the ISA is heavily redacted for confidentiality. Apple has therefore not been given sufficient insight into the evidence on which the CMA proposes to draw its conclusions or the arguments raised by other parties to be able to fully respond to the CMA's provisional findings on this subject.[207] Nonetheless, as set out below, it is apparent that the information made available to Apple does not support the CMA's provisional conclusions.

178.The PDR's concerns regarding the ISA focus on the Chrome revenue share. The CMA considers that Apple and Google may have offered a lower quality, less innovative product to consumers, as the loss of a user to their main competitor has less impact than it would absent the revenue sharing agreement, compared to a "*well-functioning market in which Apple and Google would not have reduced financial incentives to compete resulting from revenue sharing agreements*".[208]

[203] In the unlikely event that the converse is true, the CMA has not considered the implications for device storage of multiple apps installing their own browser engine.

[204] As the patch gap analysis shows, even third-party browser developers have insufficient awareness of the privacy and security risks to update the browser engines- sometimes for years at a time.

[205] PDR, paragraph 3.147.

[206] PDR, paragraph 7.87.

[207] Apple's requests for additional access to be granted within the confines of the confidentiality ring were rejected.

[208] PDR, paragraph 10.18(c).

179. Contrary to the CMA's assessment, and as Apple has highlighted, revenue-sharing agreements are legitimate and standard business arrangements between platform operators and third-party service providers. The platform operator creates an opportunity and an established user base, which it maintains and grows over time. This ensures an ongoing benefit to the service provider who, in turn, shares a portion of the revenues it generates via the platform with the platform operator. The Chrome revenue share is no different. Google has benefitted from the investment that Apple has made in relation to iOS and WebKit, and it is therefore reasonable for Apple to recoup some element of that investment via a revenue share arrangement. The CMA's underlying premise that the revenue share is incompatible with a "well-functioning" market is wholly misconceived and fundamentally undermines its analysis of the ISA.

180. The CMA's analysis is fundamentally wrong in key respects. The PDR states that the key theory of harm being considered is that Apple and Google earn significant revenue when their key rival's mobile browser is used on iOS, reducing their financial incentives to compete.[209] As Apple has explained to the CMA, Apple does not earn revenue when users use the Chrome browser on iOS. It earns revenue only with respect to qualifying searches. As a general matter, when users browse the web on Chrome, rather than Safari, Apple gains no benefit whatsoever. This is a significant error in the premise underlying the PDR's assessment, as it leads the CMA to draw unwarrantedly wide conclusions regarding Apple's incentives to compete as a mobile browser operator.

181. The evidence submitted by Apple clearly shows that the purpose of the ISA is to ensure that Safari benefits from best-in-class search, a factor that increases competition between Safari and Chrome. It also shows that the purpose of the Chrome revenue share is [✂].[210] The purpose of the ISA is therefore pro-competitive.

182. The CMA itself accepts that there is competition between Safari and Chrome and that "*there is no way for us to observe how strongly Google and Apple would compete in the counterfactual*".[211] The CMA nonetheless relies on factors entirely separate to the question of competition between Safari and Chrome - such as rival browser share and support for web apps and browser extensions - to assess the impact on competition between Safari and Chrome in the absence of the ISA or the Chrome revenue share.[212] Whilst it is correct that the ISA operates in the context of a number of other issues being explored as part of the market investigation, the CMA places undue reliance on such factors to shore up its assessment that the ISA agreement must have an impact on the parties' incentives to compete in relation to mobile browsing.

183. Further, and vitally, the CMA continues to misunderstand the magnitude of the impact that the agreement has on Apple's and Google's financial incentives to compete and has failed to demonstrate at all that, even assuming an impact on the parties' financial incentives, there is a downstream impact on competition. Indeed, the PDR's assessment confuses financial elements relating to the overall ISA with the competitive impact of the Chrome revenue share (which is only one part of the ISA), despite the fact that the CMA does not consider that the Safari element of the ISA warrants remedial action.[213] The CMA also continues to hold to and rely on the mistaken conclusion that the "*substantially similar*" level of the revenue share [✂] is sufficient to limit the parties' financial incentives to compete.[214] Apple has previously explained in detail why this is not the case.[215] Indeed, the CMA's flawed analysis leads it to discount the fact that Apple would [✂] an approach that would be commercially irrational.

184. In this respect, the CMA cannot escape its obligations by simply stating that "*our guidance is clear that we are not required to quantify effects, especially when scale of the harm is material*",[216] when it has demonstrably failed to show a material harm to competition. Indeed, as

[209] PDR, paragraph 9.75.

[210] [✂]

[211] PDR, paragraph 9.92.

[212] PDR, paragraph 9.92.

[213] PDR, paragraph 11.228.

[214] PDR, paragraph 9.131.

[215] [✂]

[216] PDR, paragraph 9.130(c).

noted above, the CMA's provisional conclusion goes no further than an assertion that Apple and Google "***may have** offered a lower quality, less innovative product to consumers* [emphasis added]".[217]

185. As well as incorrectly assessing the impact of the ISA on Apple's incentives to compete with respect to mobile browsing, the CMA effectively ignores the fact that Apple's ability to compete in mobile browsing has not been impacted by the existence of the ISA. To the contrary, Apple has negotiated amendments to the ISA specifically to ensure competition between Safari and Chrome is not affected. Whilst the CMA recounts Apple's submission that it would have been entirely illogical for Apple [✂],[218] the CMA does not draw from this the obvious conclusion that competition between Apple and Google has not been undermined by the ISA.

IX. REMEDIES

186. For the reasons set out above, Apple disagrees with the CMA's provisional decision on AEC. Even if the Final Report were to find (contrary to Apple's submissions) that a notional AEC exists within any of the markets identified on iOS, there is no basis for the CMA to take or recommend remedial action, taking into account the impact of any practicable remedy on RCBs, and considerations of effectiveness and proportionality.

A. Relevant customer benefits should be properly taken into account

187. In Apple's view, this this is clearly a case in which "*RCBs accruing from the market features are both large in relation to the AEC and would be lost as a consequence of any practicable remedy*."[219] Without seeking to reiterate Apple's extensive prior submissions,[220] there is a considerable body of evidence before the CMA demonstrating that mobile browsing on iOS is competitive and delivers good outcomes for consumers. The significant scale and scope of the RCBs arising from the WebKit requirement is clear from such evidence. Further, Apple has consistently explained throughout its submissions that WebKit is a critical component of its integrated offering and that the various benefits arising from such integration (as noted in paragraph 55 above) would be significantly reduced or lost in the absence of the WebKit requirement. WebKit's benefits therefore constitute RCBs for the purposes of EA02 and the CMA must have proper regard to the likelihood those RCBs could be lost following its recommendations and the remedy options which it considers in detail.[221]

188. The CC3 guidance states that the CMA will at least turn its mind to whether any remedial steps (including recommendations to another body to take action, such as to consider certain remedy options) should be modified to account for any identified RCBs.[222] The need to do so is particularly important in this case, given the significant scale and scope of the RCBs at issue. Contrary to this requirement, section 11 of the PDR on remedies does not assess the impact on RCBs of the CMA's provisional recommendations, despite setting out in detail certain "design considerations" relevant to the remedy options set out in Part 2 of that section. The CMA must revisit its remedies assessment to provide adequate consideration of the RCBs arising from the WebKit requirement which should lead to a change of the remedy options set out in Part 2 of section 11 of the PDR.

B. Remedy options 1 to 3 are unnecessary and disproportionate

189. First, the CMA has not properly considered the impact of the geographic scope of its remedy proposals, leading to a related lack of acknowledgement that remedy proposals applying to Apple's conduct outside of the UK would be unnecessary and/or disproportionate:

[217] PDR, paragraph 10.18(c).

[218] PDR, paragraph 9.54(h).

[219] CC3 guidance, paragraph 354(c).

[220] See Apple's response to CMA Working papers 1 to 5, paragraphs 72 to 77 and 114 to 144.

[221] We note that the CMA's draft Markets Remedies Guidance states at paragraph 3.53 that benefits to privacy and security may constitute RCBs if they constitute improvements in quality. This means that there can be no question that the benefits arising from WebKit demonstrated in Apple's submissions constitute RCBs for the purposes of section 134(7) and 134(8) EA02.

[222] CC3 guidance, paragraph 367.

- There is no basis for remedies to extend beyond the UK for them to be effective. First, apps and services are frequently tailored to different geographic regulatory requirements. Even if the CMA identifies harms to UK consumers, it is appropriate that those harms be addressed on a UK basis only.[223] The fact that some developers may wish to implement the same remedies elsewhere for their own commercial benefit, does not provide an appropriate legal basis for the CMA to exercise its powers on an extra-territorial basis. This would go beyond what is necessary for a remedy to be effective in the UK context, purely to the advantage of certain market participants.

- 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.

- Third, the extra-territorial application of remedies would also impose the CMA's views on markets outside the UK. Such remedies could run the risk of either conflicting with regulatory requirements already in place in another jurisdiction or of preempting regulatory outcomes in other jurisdictions, creating a significant conflict of laws situation.

- Finally, well-established principles of comity would argue strongly against such an approach. The CMA would undoubtedly consider that international comity principles would appropriately prevent remedies mandated by other jurisdictions with different competition-law priorities and approaches from affecting UK citizens.

190.Second, the descriptions of the possible remedies in the PDR raise further significant concerns around effectiveness and proportionality.

191.In Apple's view, the evidence before the CMA demonstrates that no *"detrimental effect on customers"* within the meaning of section 138 of the EA02 has resulted (or may be expected to result) from any notional AEC identified by the CMA.[224] To the contrary, it is clear that mobile browsing on iOS is characterized by good outcomes for both users and developers. Even if the CMA considered there to be detrimental effects arising from the AECs it has identified, the evidence shows that any such effect would be insufficient to support the imposition of the highly intrusive interventions considered in Part 2, particularly when RCBs are properly taken into account:

- On Remedy option 1, the PDR states that documentation provided on APIs would need to be clear, complete, and up to date.[225] However, as Apple already provides extensive documentation and WebKit is open source, it is wholly unclear what is insufficient about its current documentation and what further would be required and the PDR provides no indication in this respect.

- Remedy option 1 also requires enabling access in a way which respects the technical architecture of alternative browser engines. However, Apple does not know the architecture of third party browser engines, what their technical architecture may require or even if it would be possible to support them. For example, WebKit and Blink have two fundamentally different approaches to JavaScript execution (JavaScriptCore versus V8), the latter being more memory intensive, slower to start up, and potentially not compatible with Apple's OS.

- It is not clear what it means to "*manage progressive web apps (PWAs)*"[226] and what permissions/access to PWAs would be required for this to happen.

- Remedy option 2 requires access to"any features and functionalities to be used by Safari" "by default" in a "timely" manner.[227] This could be read as reducing Apple's ability to test

[223] 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.

[224] Section 138(5).

[225] PDR, paragraph 11.102(a).

[226] PDR, paragraph 11.84(e).

[227] PDR, paragraph 11.132.

new functionality to fix any bugs and ensure that security and privacy are not impacted. In other words, this proposed remedy option could require that any time Apple wants to add features or functionalities to Safari, it must permanently introduce new APIs without first making sure they cause no issues. This cannot be a sensible proposition.

- In relation to both remedy options 1 and 2, the PDR states that Apple would need to provide third browser vendors with “equal access" to iOS and WebKit functionality, respectively. Such requirements are extraordinarily broad, with no limiting principle contemplated beyond the vague exception for “significant" new PWA functionalities and where required solely for integration with first-party services on iOS (under remedy 1). They are also highly disproportionate as they fail to take into account the reality that third parties already have the ability to build most material functionality.
- Remedy options 1 and 2 amount to an open-ended obligation on Apple to make substantial ongoing investments in order to develop every single feature that third parties wish to have but are unwilling to invest in building themselves, regardless of user demand or the security, privacy and performance implications for the platform. This is most apparent with respect to remedy 2, which specifically contemplates a requirement on Apple to provide access to all future WebKit or iOS features that Safari uses free of charge. This cuts across Apple’s legitimate interests in commercializing its platform and recouping expenses when developing and maintaining new technologies that are used by third parties. It goes significantly beyond what could be considered reasonable and proportionate. It would also lead to market distortions in the form of free-riding and underinvestment on the part of third parties, which would ultimately chill browser innovation, and harm competition among browsers on iOS. It would also adversely impact Apple’s incentives to invest in the development of new features and technologies, or at least its incentives to roll out such features and technologies in the UK.
- In relation to remedy option 3, clear issues of effectiveness and proportionality arise. The evidence shows that app developers are generally content with the current IAB implementations on iOS. The lack of any clear demand for a custom-tabs type implementation or a bundled engine implementation on iOS, with the sole exception of Meta’s interest in the latter implementation, calls into question the need for the contemplated intervention. Remedy option 3 would also in practice lead to very significant privacy and security risks on iOS, most obviously in relation to bundled engine IABs, including the impact of the patch gap issue.

C. The Google ISA remedy option is unnecessary and disproportionate

192.Apple’s concerns with respect to the CMA’s assessment of effectiveness and proportionality is particularly acute in respect of remedy option 4 relating to the ISA, where the PDR considers imposing a global remedy removing the Chrome revenue share, very much akin to a financial penalty. Apple considers that this would be misguided as well as both inappropriate and disproportionate, as it would impose a highly intrusive and commercially significant remedy which goes far beyond the CMA’s statutory duty to consider and correct adverse effects on competition within the UK.

193.The CMA’s reasoning as to why a global remedy would be necessary to effectively address the incentives of the parties to compete is unsound, for the reasons set out in Section VIII above. In particular, the CMA has fundamentally misunderstood the commercial incentives of the parties, as well as the pro-competitive impact of the Chrome revenue share. The harms to consumers arising from the removal of the current arrangement (which promotes the search experience and competition between browsers across iOS) would outweigh any purported benefit from the remedy. Further, even assuming that remedies were warranted, the CMA’s incorrect understanding of the commercial impact of the Chrome revenue share undermines its view that a wider-than-UK remedy would be required to be effective. Finally, for the reasons discussed above, a global remedy would also be inconsistent with well-established principles of international comity and would give rise to the significant risk that the CMA would pre-empt regulatory or other action in jurisdictions outside the UK. Users in other jurisdictions would be affected by the termination of the Chrome revenue share despite the fact that regulators in those jurisdictions may have no concerns regarding the revenue share or, indeed, consider that the revenue share benefits competition.

194. More generally, the prohibition of the Chrome revenue share without altering the other ISA obligations (as envisaged by the PDR)[228] would also fundamentally unbalance the commercial relationship between Apple and Google, as well as the competitive interaction between Google and its competitors, creating a serious risk of distortion. Unintended consequences would likely arise from the CMA's proposed remedy option to the detriment of UK Apple users. We note that Google has previously been held to be in a dominant position with respect to internet search in several jurisdictions, including in the UK.[229] Providing a financial windfall to Google through removal of the Chrome revenue share would likely strengthen Google's dominant position in internet search in the UK (and beyond).

195. Finally, removing the revenue share would be an unwarranted intrusion on Apple's ability to monetize its platform and obtain proper compensation for the value that it brings to Google through the countless product improvements that bring users to the iPhone and create a user-friendly, safe and trusted environment for users to search the web. This would be an inappropriate expropriation of property rights.

D. Further areas for consideration with respect to the remedy options

196. In the event that, notwithstanding the above factors the CMA adopts its recommendations in its Final Report, as part of the DMU's review of the mobile browsing market, it will be important for it to consider any potential remedy options objectively and afresh. As demonstrated, both by the impact of the change in the App Store rules on cloud gaming, and the effect of the iOS 18.2 updates to the user journey for changing default settings, the iOS ecosystem is continuously evolving in order to incorporate new technologies and provide a better user experience. This may, as in those cases, completely or very significantly address any prior concerns. More generally, the CMA's position has itself evolved as it has gathered more information on the markets in question and gained a better understanding of the relevant issues (for example, in relation to SFSafariViewController and the uninstallation of Safari). This is likely to remain the case.[230]

197. Whilst neither we, nor the CMA, can prejudge any future assessment of remedies by the DMU, Apple sets out below some high-level considerations regarding access to functionality, security and privacy that will be necessary for such future assessment to take into account.

198. On access to functionality, Apple would emphasize that its incentives as a device manufacturer, which guide it to invest and develop iOS to the benefit of UK users and developers, presume adequate recognition of its legitimate interests in commercializing its platform and in recouping its expenses in developing new technologies for use by third parties. Remedy options 1 and 2, and in particular the aspects which would require the development of new technologies free of charge, would significantly impinge on those interests in a way that goes beyond the objectives of the DMCC and which, for the reasons noted in paragraph 191 above, is ultimately detrimental to UK users and developers as well as the UK economy.

199. On security and privacy, the CMA acknowledges that "*Apple's dual role as the device manufacturer and operating system provider means it is best placed to determine how the required level of access can be granted to third parties considering any security and privacy considerations that need to be incorporated*".[231] The CMA also recognizes that Apple should be entitled to set out minimum security and privacy requirements for the introduction of third-party browser engines as it has done in response to the DMA.[232] Apple welcomes these

[228] PDR, paragraph 11.261.

[229] Commission Case AT.39740, paragraph 271.

[230] As noted above, the CMA must exercise caution when relying on evidence from prior cases and do so only where relevant, bearing in mind the purpose for which the evidence was originally gathered, considering the weight it should be afforded, and carefully considering whether it should be updated or corroborated. DMCC Draft Guidance, paragraph 2.65.

[231] PDR, paragraph 11.100.

[232] PDR, paragraph 11.123.

acknowledgements and considers that they are key to the consideration of the reasonableness and proportionality of any future remedies.

200.In particular, given the very significant concerns that remain with respect to security and privacy, as demonstrated by the DSIT survey showing a widescale lack of awareness on the part of UK app developers of what would amount to no more than minimum standards in these respects, it is vital that Apple should be given sufficient leeway to determine exactly what third-party developers must demonstrate in terms of capability, intention and accountability before they can be allowed to offer alternative browser engines or use them in their apps on iOS.

201.Unfortunately, there are a number of areas where the CMA nonetheless appears to pull back from these important acknowledgments and to consider that Apple should not be entitled to take the security precautions that it considers necessary to properly protect users and developers. This exacerbates concerns that the remedy options contemplated in Part 2 of section 11 of the PDR would lead to a loss of the RCBs identified above. For example:

- In relation to remedy options 1 and 2, the CMA suggests that it may be "unduly onerous" for Apple to require third-party browsers using alternative engines to provide a separate binary when doing so.[233] As Apple has explained to the CMA, separate binaries are commonly used to address different technical or regulatory requirements and do not impose an undue burden on developers. They are also necessary to ensure that a remedy imposed in the UK would not (deliberately or inadvertently) be used in other regions by virtue of developers enabling features globally.[234] Finally, separate binaries ensure that users are informed of the change in engine: there is an inherent contradiction in the CMA's position that a choice of browser engine is an important one for users to be able to make, while at the same time users should not have a say when their browser developer makes that choice for them.
- Remedy option 3 regarding remote tab IABs would equally give rise to the significant security and privacy concerns identified above at paragraphs 162-164.
- Remedy option 1 contemplates a requirement on Apple to allow third-party developers to use alternative browser engines to power HSWAs. This would significantly undermine Apple's ability to ensure the necessary level of security and privacy on iOS. Apple has set out in detail the security concerns relating to HSWAs and the specific architecture that it has created to mitigate those risks.[235] That remedy option, as currently set out, would negate those mitigations and open up iOS (and users) to significant additional risks.

202.Apple urges the CMA to revisit its assessment of the remedy options in Part 2 of section 11 of the PDR in light of the significant RCBs arising from the WebKit requirement and the other factors flowing from the requirements of effectiveness and proportionality set out above.

X. CLOUD GAMING

203.Apple welcomes the CMA's provisional conclusion that there is no AEC in the market for the supply of cloud gaming services. Apple also welcomes the CMA's recognition that cloud gaming service providers do not face material challenges implementing IAP into their apps and that there is evidence of successful market entry. In particular, the CMA recognizes that service providers can integrate IAP and that the evidence does not suggest that the commission level is limiting the availability of cloud gaming apps on the App Store.[236] It also points to recent market entry by Antstream, as well as a number of additional service providers who are considering launching a cloud gaming app on iOS.[237]

204.Apple nonetheless wishes to make two observations on the PDR's analysis of cloud gaming services.

[233] PDR, paragraphs 11.109 and 11.200.

[234] Apple's response to the CMA Working Paper on Remedies, paragraph 12 to 15.

[235] [✄].

[236] PDR, paragraph 12.156(e).

[237] PDR, paragraph 12.156(f).

205.First, we note that the PDR sets out in some detail cloud gaming service providers' concerns about Apple's App Review Guidelines.[238] Even if taken at face value, which would be inappropriate, many of these are not competition issues, but commercial disputes.

206.Second, the PDR's provisional product market definition states that the market on which Apple operates is at least as wide as the supply of services to cloud gaming services app developers that enable the installation, distribution and operation of native apps on iOS devices in the UK.[239] The PDR then posits an even wider possible market definition which may also comprise the supply of such services to all app developers, but does not fully analyze such a putative market.[240] As such, Apple can only comment that such a provisional market definition would be an inappropriate starting point on which to base any future regulatory action.

207.For the reasons outlined above, these aspects of the PDR's analysis should be revisited afresh in any future regulatory proceedings.

XI. CONCLUSION

208.CMA guidance states that the market investigation process is characterized by an "investigative and inquisitorial, not accusatorial" outlook. It states further that the CMA "*makes no presumption that there are market features that harm competition*."[241] The Inquiry Group must bring an appropriately open mind to the in-depth investigation of the highly technical and dynamic markets referred to it.

209.The CMA's phase 2 investigation must also be grounded in a thorough interrogation of the actual conditions of competition within the referred markets[242] to be achieved through the adoption of a realistic benchmark for the CMA's analysis which "*displays the beneficial aspects of competition…but not an idealized perfectly competitive market*."[243]

210.In this case, there is a very considerable body of objective evidence, including from the CMA's own research and third parties, demonstrating that outcomes are highly positive, to the benefit of all stakeholders:

- There are roughly 100 different browsers on the UK App Store with varying features and unique selling points - a range and level of differentiation similar to that available on the Android platform;
- There is effective parity in the access to material features and functionality between Safari and third-party browsers;
- The CMA's own evidence shows that the vast majority of developers are satisfied with the various implementation mechanisms that Apple provides for IABs, which can be tailored to their diverse needs and capabilities;
- WebKit and Safari are characterized by a high rate of innovation, which is driven by Apple's significant and long-standing investments in those products;
- Users are informed and able to make effective switching decisions; and
- Extremely high rates of satisfaction persist amongst iPhone users, reflected in survey evidence.

211.Apple has provided extensive submissions in a collaborative effort to assist the CMA in understanding how these outcomes are achieved in practice. In particular, we have explained that these outcomes are a natural reflection of: (a) Apple's incentives as a device manufacturer; (b) robust competition at the device level including the real and constant threat of switching, which incentivizes Apple to foster competition at the browser level; and (c) the reality that, at a

[238] PDR, Table 12.1.
[239] PDR, paragraph 12.89(a).
[240] PDR, paragraph 12.89(a)(i).
[241] CC3 (Revised), paragraph 21.
[242] *Ibid*, paragraph 101-102.
[243] *Ibid*, paragraph 320.

technical level, the deep integration between iOS and WebKit ensures that all developers benefit from an exceptionally high baseline of performance, security, and privacy from which to build their apps, fostering their ability to innovate and compete. In light of the above, there can be no concerns with the underlying 'source' of the positive market outcomes observed. Indeed, these outcomes are entirely consistent with a "well-functioning" market in mobile browsing.

212.Further, a clear-eyed view of the issues raised by developers in relation to mobile browsing reveal many of these to be based on an erroneous understanding of the facts (for example conflating SFSafariViewController with Safari or identifying a lack of access to certain features where access is in fact available), explained by commercial factors (for example, Google and Meta's claims that Apple's approach are not sufficiently flexible for the purposes of their advertising-led business models) or factors unrelated to Apple conduct (for example, the reality that any software development will involve costs, whether the WebKit requirement is applied or not).

213.We welcome the CMA's recognition that the essentially commercial issues raised by a few large developers in relation to cloud gaming are outweighed by objective evidence which shows that (a) cloud gaming service providers do not face material challenges in integrating IAP; and (b) that there is evidence of thriving market entry in cloud gaming. The CMA's provisional conclusion that no AEC in cloud gaming arises is the only reasonable position in light of that evidence and Apple's strong track record of support for gaming, including cloud gaming. We ask that the CMA applies the same healthy degree of scrutiny to the issues raised by developers in relation to mobile browsing.

214.In addition, we ask that the CMA revisit its analytical approach to mobile browsing. The PDR essentially benchmarks Apple's conduct against an "idealized" version of an OS in which all of the notional benefits of multiple browser engines are present but none of the very serious security, privacy and performance issues identified in Apple's submissions arise (or, if they arise, can be dealt with through hypothetical measures that would be as effective as Apple's existing approach). In so doing, the CMA has not given due weight to the possibility that a platform with a single browser engine can produce effective outcomes, contrary to its guidance and the objective evidence of positive outcomes. This is entirely inappropriate given the gravity of the considerations at issue from the perspective of users, which include not only individuals but also institutions such as government departments. Further, it has caused the CMA to stray from the facts in preference of a speculative analysis in which unsubstantiated complaints carry greater weight than objective technical evidence.

215.We strongly believe that a proper consideration of the evidence of positive outcomes and of third party issues, by reference to the relevant economic and technical context, and against any realistic benchmark, can only reasonably return a conclusion that no AEC arises in mobile browsing on iOS.

216.Finally, Apple submits that remedies are unwarranted as no AEC arises in relation to any element of mobile browsing. Should the Inquiry Group conclude, to the contrary, that there is an AEC in relation to mobile browsing in the Final Report, for the reasons discussed in detail, Apple does not believe that the remedial steps considered by the Inquiry Group are sufficiently specific, proportionate, or considerate of RCBs to either warrant the immediate imposition of remedies in the form in which they have been set out in the PDR or to allow the CMA Board to implement such contemplated remedy options as part of its digital markets regime, without a fuller exploration of their potential risks and harms. Apple is particularly concerned by the willingness in the PDR to consider: (a) extending the scope of the market and potentially recommend imposing remedies beyond the UK, as it has specifically indicated in relation to the ISA; and (b) impinging on Apple's legitimate interests through requirements to develop technologies for use by third parties free of charge. Apple considers that such an approach would be wholly disproportionate, risk conflict of laws situations, and would be inconsistent with principles of international comity.

217.We look forward to continued constructive engagement with the Inquiry Group and the CMA in this final stage of the market investigation.