PREISKEL & CO

Preiskel & Co LLP
4 King's Bench Walk
Temple
London EC4Y 7DL
United Kingdom

t +44 20 7332 5640
e info@preiskel.com
www.preiskel.com

Competition and Markets Authority
The Cabot
25 Cabot Square
London
E14 4QZ

For the attention of:
[redacted]
browsersandcloud@cma.gov.uk

By email only

[redacted]
13 December 2024

Dear Sirs,

Re: Mobile browsers and cloud gaming – Provisional Decision Report (22 November 2024) – Comment from Movement for an Open Web (MOW)

As you know, we are writing on behalf of Movement for an Open Web ("**MOW**"), a consortium of digital markets players, seeking an open and decentralised web. We write further to the CMA's provisional decision report dated 22 November 2024[1] ("**Provisional Report**") to provide MOW's response. References to page numbers and section numbers throughout this response are to the pages and sections of the Provisional Report respectively, unless stated otherwise.

Our response is split into the following sections:

(a) Introduction
(b) Additional Factors
(c) The Duty to Remedy Adverse Effects
(d) Remedies that may apply now and those that may reasonably be assessed later under the DMCCA
(e) Web Standards as part of Remedy Design
(f) Conclusions
(g) Further comments and considerations
(h) Appendix A: Rebutting pretextual claims to "improving privacy"

(a) Introduction

We agree and support the CMA's analysis and applaud the willingness to tackle major issues in technically challenging markets. These markets are fast moving in the sense that billions of people are engaged in millions of transactions using Google and Apples products and platforms at every hour of the day and night, worldwide.

[1] https://assets.publishing.service.gov.uk/media/67406fe502bf39539bdee865/Provisional_decision_report2.pdf

The anticompetitive nature of the practices and agreements identified are truly global and require an urgent and significant response. The scale of the [redacted] that has been uncovered is probably unprecedented in modern times. The careful assessment in the report should not let it obscure the enormity of its findings.

We outline below additional factors the CMA may have overlooked, followed by our views on the duty to remedy adverse effects and our assessment of the effects and how they should be remedied now. Some adverse effects on competition can be remedied now, others may be more suitable for remedy under the Digital Markets, Competition and Consumers Act 2024 ("**DMCCA**"). That is why we are suggesting a combination of some simple remedies to remove the anti-competitive restrictions in the agreement between Google and Apple that can apply now and others that may be more suitable for the future.

To proceed on the all or nothing basis as indicated in the Provisional Report would otherwise raise a risk of placing all proposed remedies in jeopardy – allowing Apple the opportunity of appealing them and considerably delaying any remedy for the United Kingdom (UK), while the world looks on and applies remedies under parallel proceedings in other jurisdictions.

(b) Additional Factors

We consider the following factors affect Apple's incentives and must now be considered by the CMA:

- The CMA has identified that Google shares 36% of its search advertising revenue with Apple. To Apple this is pure profit which carries virtually no cost of sale. This is referred to as being worth $20bn[2] by the United States (US) Court in the United States vs Google LLC. It represents about 20% of Apple's EBITDA and free cashflow[3][4].
- It is, in effect, an exclusive agreement that prevents competitors to Google from engaging with users of Apple's operating system, iOS, and being promoted to Apple users on a non-discriminatory basis.
- The CMA assesses the amount of the payment as "*26% of Apple's total global revenue coming from the Services category*".[5] This is strategically and financially significant since Apple's pivot to services and away from its hardware roots in 2018, whereby it sought to reduce the risks inherent in the business of constantly refreshing devices[6]. Since many executives own considerable Apple stock, they are highly motivated to avoid loss of income from Google for any reason[7].
- Google in practice obtains exclusive use of Apple user's data for advertising through the operation of the Information Services Agreement ("**ISA**") and prominent display of Google Search on Apple devices, the anticompetitive effect is felt by other browsers, search and display advertising businesses and publishers.

---

[2] *USA vs Google* para 299 "In 2022, Google's revenue share payment to Apple was an estimated $20 billion (worldwide queries). Tr. at 2492:22–2493:6 (Cue). This is nearly double the payment made in 2020, which was then equivalent to 17.5% of Apple's operating profit. Id. at 2492:2-8 (Cue); id. at 5727:20–5728:4 (Whinston) (discussing UPXD104 at 19)."
[3] Apple Free Cash Flow 2010-2024 | AAPL | MacroTrends
[4] Apple EBITDA 2010-2024 | AAPL | MacroTrends
[5] Para 9.98
[6] Breaking Down The Drivers Of Apple's Booming Services Business see also Apple's Shift to Services and Wearables: A Strategic Diversification
[7] These are Apple's top shareholders as of December 2024 also https://www.sec.gov/Archives/edgar/data/320193/000119312522225365/d366128dex101.html

- The deal creates economic inter-dependence between the two companies. (The CMA appears to have been provided with the same number as the US Court[8] - which, at the end of 2024, is unaccountably now out of date and which should be rectified in the final analysis and CMA findings).[9]
- The Apple executives run its business and have a considerable personal incentive to delay the application of any remedies that affect the [redacted] income from Google.

The scale of the payment from Google by comparison with income from Apple's other business makes Google Apple's biggest customer and source of profit. This significantly alters Apple's incentives and operates as a major impediment to competition across browsers and all other aspects of the two companies' businesses. While the incentive is narrowly described by the CMA as "*so large that the revenue share they earn from their competitor's product is lower but similarly significant to the revenue share they earn from their own, so that the incremental revenue from winning customers, and therefore the financial incentive to compete, is limited*", that understates the significance of the anticompetitive incentives on both companies' entire businesses[10], [redacted].

This is competitively highly significant. It is more accurately described as a horizontal revenue sharing agreement between the two leading global competing browser and technology ecosystem businesses[11]. The effects of the restrictive provisions are identified as matters to be investigated in para 46-48 of the CMA Issues Statement[12]. The Provisional Report's assessment of the ISA's impact on Competition is provided from pages 441- 447 with the scale of impact from 447. The CMA considers the anticompetitive impact significant. Those impacts arise from the provisions of the agreements that generate these outcomes but overlook the nature of the restrictive provisions and how, if those restrictions were prohibited in the short term, competition could be improved. The precise restrictions are public and detailed in the Judgment of 5th August 2024 at page 102 et seq. In particular, they include:

- The ISA requires Apple to set Google as the default search engine on Safari for all its devices. Id. at 793
- Under the ISA, a "*Default*" search engine is one that "*will automatically be used for responding to Search Queries initiated from the Web Browser software*"
- "*Search Query*" under the ISA is defined as any user input seeking information that is entered on Apple's voice assistant, Siri; its on-device search, Spotlight; **or Safari**
- In return for these default placements, Google pays Apple [26 %][13] of its ad revenue on Safari and Chrome, including queries initiated through Safari's default bookmarks. JX33 at 793, 797–98; JX24 at 822. Google pays revenue share on Chrome queries, notwithstanding the fact that Apple does not preload Chrome onto its devices. See JX33 at 796–98

As can be seen from the above, the language of the ISA includes the browser, "Safari". This is because browsers can be search access points. The CMA should not consider browsers and remedies that relate

[8] See para 9.4 footnote 1685
[9] Google: Revenue, by year | Statistico
[10] See further USA vs Google Section E p21 et seq.
[11] See CMA Mobile Ecosystems Market Study 2022
[12] https://assets.publishing.service.gov.uk/media/63984ce2d3bf7f3f7e762453/Issues_statement_.pdf
[13] From CMA sources we believe this is 26% for Ad revenue generated from Safari. The revenue generated from browser histories is unknown and we believe the 26% may be an under estimate because there is no verification available to Apple or otherwise of the underlying source of revenue. This lack of verification derives from the fact that Google controls all search ad revenue from Safari and Chrome and [redacted]. We suggest the CMA enquires further into the verification for the ad revenue source with Google.

to browsers as something divorced from the agreement. The definition in the agreement restrict competition with relation to software functionality wherever it is placed in the technology platform.

The CMA focuses on the incentives that are necessarily derived from the outcomes of these agreements. But for the agreements there would be no anticompetitive outcomes and incentives would differ – and it is the terms of the agreements that are restrictive. If, for example, the above default settings and provisions that create effective exclusivity over search access points were removed, Apple could mitigate its dependency on Google and consumers would receive the benefits of more competition between search offerings, browser suppliers, and others. We consider that these are changes that severely limit competition and require remedy now. Competition would be increased and incentives improved.

Importantly, the CMA refers to both companies as competing in the provision of browsers – but recognises that their businesses are not browser businesses; they use browsers as part of their business of running technology platforms, or ecosystems. The ISA creates incentives that adversely affect these businesses and the supply chains with which they compete worldwide not just the provision of browsers, but necessarily in the provision of browsers as a central element.

The CMA has found no objective or economic justifications for either party's anticompetitive conduct. Their privacy and security arguments are found to be insubstantial. Serious adverse effects on competition are found to require serious remedies - so significant in fact that the CMA considers the remedies need to be taken under the new DMCCA.

However, the position that applies now, before the full application of the DMCCA if introduced, remains unaddressed.

(c) The Duty to Remedy Adverse Effects

We suggest that the CMA needs to consider further the following points on taking measures now addressing the restrictive provisions of the ISA pending the introduction of further measures under the DMCCA:

1) Under Part 4 of the Enterprise Act 2002, the CMA is required to investigate and remedy the effects of any features of the referred markets, including agreements between undertakings, which it finds result in an AEC: it has made those findings and is satisfied they are robust. It is now duty bound to remedy their effects.[14]
2) We respect the assessment of risks to the application of the Enterprise Act 2002, remedies that are considered in S11 but no consideration is made of the full range of risks that are required to be considered by law under the comprehensiveness test.[15] For example:
    - the fact that the DMCCA is new, and a range of its provisions have not been applied before, raising opportunities for defendants including Apple to raise legal issues via the courts.
    - Both Apple and other potential designates may delay the process through legal challenge as is usual with new laws that have not been applied before.

[14] As is required by Section 138 of the Enterprise Act 2002under the title "Duty to remedy adverse effects". The language of the provision is imperative not discretionary- the CMA being required to remedy
[15] Section 134(6) & Section 138(4) EA02

- The CMA cannot rule out that it might not properly designate Apple in accordance with the provisions of the DMCCA and,
- Apple may seek to claim that the Provisional Reports' conclusions are a determination that is seeking to prejudice the discretion that should be exercised by the CMA when making its determinations under the DMCCA – a set of determinations that should be made by different people under a different law based on future facts. By tying the hands of the CMA in the exercise of its discretion under the DMCCA the risk is that the CMA's Browsers investigation can be claimed to be prejudging the outcome of a determination under the DMCCA. That type of claim may or may not be successful, but if it were, it would leave the CMA with the inability to make any effective assessment under the DMCCA on facts and matters that it finds to breach the Enterprise Act 2002, in its Provisional Findings.
- Even if the CMA's designation is perfect, and its independent assessment of the application of s29 robust, that does not change the overriding incentive for Apple to seek to avoid the application of the act and delay its implementation for as long as possible, maximising its income from Google by seeking appeals through the courts to the highest level on every conceivable point that can be raised, [redacted]

One controversial feature of the DMCCA which has been overlooked by the CMA in its Provisional Report is the inclusion, at the behest of the technology platforms between the Bill leaving the Commons and entering the House of Lords, of the countervailing benefits exemption (S29). In our view Apple is highly likely to seek to rely upon S29. While we agree that the CMA is correct to reject Apple's privacy and security claims, how those claims would fall to be assessed under S29 is both unknown and unknowable at this point.

What we can say now with total certainty is that the assessment required by law is different under the DMCCA's S29 from the assessment that the CMA is required to make under the EA02. The matter thus has to be addressed now – and if that is not done the CMA will inevitably be in breach of its obligations under S138 EA02 and may be in some difficulty in addressing these matters under the DMCCA. This is because S138A EA02 also requires remedies to be in place within a six-month timeframe and that timeframe will start to run from the date that the CMA publishes the Final Report under S136 EA02.

Risking the certain outcome of remedies applicable now for potential remedies that might apply in the future is thus quite unreasonable.

Here, we consider that the obligation in the law is to remedy the effect of the harm, from the date of the CMA decision as a Market Report under the EA02, not at some undetermined future point under a law that is yet to be implemented.

It should be born in mind that Apple appealed the Mobile Ecosystems Market Study ("**MEMs Report**") and is Appealing the application of the DMA[16]. It is likely that it will appeal any future remedy or decision whether under the DMCCA concerning designation, applicability of S29 DMCCA, or otherwise. Since the DMCCA requires a series of steps to be correctly followed before it is in place, Apple is being provided with more opportunity to appeal and the CMA is facing greater risk of delay.

[16] Competition and Markets Authority Appellant v Apple Inc; Apple Distribution International Ltd; Apple Europe Ltd; Apple (UK) Ltd [2023] EWCA Civ 1445

Given the ongoing harm to both consumers and rival businesses, action to address this harm prior to new risks of appeal and litigation under the DMCCA is warranted.

(d) Remedies that may apply now and those that may reasonably be assessed later under the DMCCA

The CMA has assessed six remedies that can apply now: we believe that Remedy 4, which would prohibit the Chrome revenue share and the agreement of which it forms part, should be implemented as soon as possible. The CMA describes the issue to be remedied in Remedy 4 as:

"*A potential remedy to address AEC 2 would be to prohibit the contractual provisions in the ISA pursuant to which Google shares revenue derived from Chrome on iOS with Apple (Chrome Revenue Share). Further, Apple and Google would be prohibited from entering into any agreement of equivalent effect pursuant to which Google shares its search advertising revenue with Apple derived from Chrome on iOS (including agreements in relation to any other future product that performs the equivalent functions of a dedicated mobile browser)*"

We agree with the CMA finding in para 11.259 that "*If the Chrome Revenue Share were to be terminated, Apple's incentives to encourage its users to make and/or keep Safari as a default would likely increase*"[17]. If nothing else is achieved from the outcome of the MEMs and the Mobile Browser investigations, a remedy that achieves that outcome would be applauded. Apple might seek to obtain other search and browser solutions from other search and browser suppliers and address any reduction in income that Google might threaten from the changes to the provisions – again to the benefit of consumers and competition.

We note that Apple has highlighted the issue that the Chrome agreement is part of a wider agreement between the parties that affects other products and has effects on other markets and geographies can be expected. In effect it claims that the UK Competition Authority striking down an [redacted] agreement that applies to other products and other places would be disproportionate because, presumably, the wider agreement that applies to non-browser-related products (such as search) is potentially valid. However, this is based on a false premise since the agreement as a whole is likely to be invalid and the claim falls to the ground.

For example, Google's ISA with Apple has been found by the US Court to have been an illegal breach of US law. This is a finding that is applicable now. It may, of course, be appealed in the future but at this point in time it represents the finding of a foreign court of competent jurisdiction on a matter of foreign law, and likely, one that is highly relevant to the ISA whose parties are subject to the application of US Antitrust laws. Any argument by Apple that it should be allowed to [redacted] based on equitable relief from enforcement, under the agreement being valid elsewhere is groundless and should be roundly rejected.

Furthermore, Apple's position lacks substance as it rests on an assumption of validity that is plainly unsustainable. There are 4 main reasons:

[17] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.259

1) The CMA should consider further that the US Court has recently found the ISA to be illegal under US law in the Google Search Judgment. That judgment does not find the agreement to be partially valid. It is invalid and unenforceable in its entirety because of the application of US law.
2) The CMA can determine in its discretion that in its view it is likely that the agreement as a whole may be illegal and unjustifiable under parallel European Union's (EU) and US laws, without overstepping the mark of proportionality. If Apple were to challenge this issue the CMA should feel confident of its ability to successfully defend its position in court. Moreover, it would be best to address the issue now as the issue would not change under the DMCCA. Indeed, if Apple were to be correct in its assertion now, it would be no less correct in relation to the application of the DMCCA to these provisions.
3) The CMA seems to take the view that "*The prohibition of the Chrome Revenue Share would not preclude either party from continuing to fulfil the remaining ISA obligations which are not part of the potential remedy, including the arrangements relating to Google's search engine being the default on the Safari browser*."[18] This is likely to be mistaken and depends on the severability or otherwise of the provisions of the contract under the law of the jurisdiction of the contract. We would expect that to be a matter of contract and antitrust law under the relevant UK, EU and US laws, and as suggested above, it is more likely that the finding of illegality by the CMA and the US judgment strikes at the heart of the bargain made between the two parties such that the contract as a whole is invalid and unenforceable.
4) Apple has also raised the fact that a finding of illegality would have effects beyond the UK. Given the [redacted] this is similar to a claim that a cartel affecting the UK might not be illegal or could be justifiable in another place, under another law, and hence the CMA should not interfere: which is not a matter that the CMA should entertain.
5) The CMA only identifies what it describes as "*Distortion*" and "*Circumvention*" risks with relation to Remedy 4. We have seen no account taken of the duty under S138 which is an obligation on the CMA. Nor have we seen any assessment of the major risks identified in this letter toward the use of the DMCCA alone – which far outweigh the points laid out in the CMA report.

We accept that there are specification, circumvention and monitoring risks, but those risks arise with relation to any intervention under any obligation or order in technology markets that are necessarily written in the language of today and against findings of fact in an investigation which, by the time the remedy is determined, are historic in the sense of being facts found before the remedy can apply to them. No legitimate remedy of the type contemplated can be truly forward looking and define the illegality of future conduct on future facts against a future market context. If it is not possible to address this issue now it will be no easier under the DMCCA. We are aware that the same issue has troubled those dealing with remedies in technology markets for many years. See the following on the issue of technology change.[19]

[18] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph11.261
[19] T. Cowen Oxford Journal of Antitrust enforcement, "European regulatory transformation—A case study: competition, remedies, and Google" (July 20224) available at https://academic.oup.com/antitrust/article-abstract/12/2/213/7649334. Please confirm if the CMA would like a PDF copy. See also Per Hellstrom and others following Microsoft we also consider that future proofing will be possible through a type of structural change such as that which applied under previous US Consent Decrees. Those are likely to be taken into account in the current US Proceedings

(e) Web Standards as part of Remedy Design

The concerns about future proofing can potentially be overcome with reference to standards, and standards making such that the definition of browser functionality is tied to W3C standards and an oversight and monitoring committee- similar to the one that was implemented in the Microsoft remedy, could be put in place, funded by Apple. In effect the definition of browser software functionality can be cross-referred to the standard and any variation then subject to notification oversight and control of the CMA on an ongoing basis and a periodic review of the remedy and market effects overseen by a monitoring trustee.

The CMA accepts web standards bodies are important in ensuring compatibility and hence interoperability – which is only true if they are defined as being competitively neutral.[20] This can be reinforced with relation to the obligations on Apple and Google with relation to browsers as defined with relation to W3C standards.

We reiterate our concerns that Apple and Google slow innovation and investment in web businesses, by dominating committees that set standards to restrict competition. We appreciate that these concerns were noted by the CMA but not yet considered as part of remedy design.[21]

The undue influence on standards committees and undermining of open standard interoperability has resulted in a large shift in the market from websites and web apps to native apps, against the interests of content owners, publishers, advertisers and the consumers who access this online content and services.

(f) Conclusions

MOW also agrees with the CMA that the indirect network effects of interfering with interoperability shifts online consumer behaviour further under the control of Apple and Google to the detriment of choice, competition and innovation.[22]

The findings of this case bear an important precedent for remedying Google's anticompetitive conduct in the Privacy Sandbox case, such as its exclusive bundling of B2B Ad Systems into both its mobile Android OS and Chrome browser. The discriminatory access to OS and browser functionality and consumer choice signals is an abuse of Google's dominant position, and without modification will distort competition in the adjacent business-facing solution markets that depend on continued access using open interoperable web standards.

Other conduct, including the Privacy Sandbox changes to the Chrome browser can be addressed in time and with a parallel application of the DMCCA when it is fully in force.
Conclusions

[20] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 2.118.
[21] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 2.120
[22] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 2.122-3.

For the reasons set out above we believe that the CMA should act now. Indeed, it is recorded in the Court of Appeal[23] that the CMA accepted the need for speed in its decision to proceed with the enquiry which Apple appealed. That urgency has only increased.[24]

We also appreciate the CMA is keen to address the issues where browsers are part of the wider ecosystem being linked to B2B distribution and B2C access via dominant apps stores and search engines.

However, that does not mean browsers cannot be addressed now and the wider set of issues addressed under the DMCCA at a suitable point down the road.[25]

(g) Further comments and considerations

Our further comments and considerations on the CMA's analysis are provided below.

1. Apple and Google's Revenue Sharing Agreements

MOW agrees with the CMA that "*Apple and Google hold a de facto duopoly in relation to the supply of mobile operating systems*."[26] MOW also agrees with the CMA and the prior European Android decision "*that the supply of mobile browsers on iOS and the supply of mobile browsers on Android should be considered as two separate product markets*."[27] The CMA found that the browsers of Apple and Google have dominant shares in both iOS and Android, at greater than 90%.[28]

Remedy 1a – Apple to remove OS restrictions via policies for rival browser engines

MOW agrees with the important inclusion of "*any guidelines with similar effect in the future*" to prevent circumvention.[29]

Remedy 1b – Apple to grant "*equivalent access*" to OS features for rival browser engines[30]

MOW agrees with the FRAND approach to iOS functionality access for rival browser vendors to select browser alternative engines to Apple's WebKit. However, to avoid perfunctory appeals to "*security and privacy*" unsubstantiated justifications, it is important ensure what "*privacy*" definition is objective and reasonable. Given the CMA provides Apple a provision to restrict rivals access to features or

[23] Competition and Markets Authority Appellant v Apple Inc; Apple Distribution International Ltd; Apple Europe Ltd; Apple (UK) Ltd [2023] EWCA Civ 1445

[24] The CMA stated that they had, independently, undertaken additional analysis which gave it "increased confidence that interventions to remove certain restrictions – in particular those relating to mobile browsers and cloud gaming services – could be implemented without compromising safety, security, or privacy over people's data". Para 31. In view of the lack of imminence of new legislative powers, the CMA concluded that now was the right time to take targeted action by way of a MIR." One of the relevant criteria for making the MIR was that:"(b)There is a reasonable chance that appropriate remedies would be available.

[25] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 2.122-3.

[26] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 2.80, 3.12, 3.136, 9.102.

[27] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 3.49.

[28] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 3.155(c)-(d): "*The available data shows that the combined share of these two browsers on mobile devices across iOS and Android in the UK amounts to 90% in 2024, with Safari having a share of supply of 44% and Chrome a share of 46%. When considering Android and iOS devices separately, as of March 2024, Safari was the main browser on iOS in the UK, with a share of supply of 88% and Chrome was the second largest, with a share of supply of 11%; on Android, Chrome was the main browser, with a share of supply of 78%.* ***Apple and Google also have the largest browser engines, with a combined***
share of almost 100% on mobile devices across iOS and Android in the UK."

[29] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.83(a).

[30] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.83(b).

functionality via its dominant OS on the grounds of "*security and privacy*",[31] it is critical to avoid circumvention that these terms be limited to clear definitions.

MOW agrees with the CMA's earlier recommendations on remedies that "*[s]imilar to security requirements, privacy requirements should not be overly prescriptive or vague*."[32] MOW suggests using analogous language as in the Google Privacy Sandbox Commitments, where privacy risks are defined by reference Applicable Data Protection Legislation, which should also include recent court cases that clarify any ambiguities, rather than Apple's consistent misinterpretation of "*privacy*" to restrict rivals.

We agree with the CMA that the risk of Apple's attempt at circumvention is high, given Apple's continuous self-preferencing definitions of these terms in the past (e.g., referring to "*first party*" vs "*third party*," imaginary distinctions of running software it controls on consumers local devices rather than on Apple servers, or treating all rivals' interoperable data as Personal Data, despite its own use of deidentified random identifiers).

Unfortunately, Apple and Google's long-time dominance of standard setting bodies means many of the definitions and proposals in those forums do not represent the interests of most publishers, consumers and competitors to these big tech giants. To avoid circumvention by setting new standards on mobile browsers, Apple and Google should be required to publish a competition impact assessment associated with any proposal they submit or contribute within these bodies. The publication of any Apple assessment of privacy concerns[33] associated with functionality must go further than merely repeating its unsubstantiated positions of the past (such as those called out in the prior paragraph and in this submission). The CMA must require Apple to apply the same evaluation criteria as the courts have relied upon to evaluate Applicable Data Protection Legislation in address privacy concerns.[34]

To address this circumvention concern, MOW recommends that appeals to "*privacy*" require:

- Apple to "*demonstrate*"[35] the necessity of restricting functionality or withholding self-preferencing access to features via a reasonable and "*appropriate*"[36] policy or architectural design "*for privacy reasons*" using "o*bjective criteria"*[37] about specifically identified harms, including the likelihood and severity of such harms.
    - This in turn requires
        - Distinguishing Personal Data from de-identified data,
        - Distinguishing Sensitive information from non-sensitive information, and
        - Ensuring any restrictions on data use for rivals should apply on an equivalent basis for own Apple's business-facing services.
    - Per our prior filings to the CMA, labeling of local storage, such as cookie files, based on their contents by the data controller of those cookies as well as of online content can ensure the data is appropriately distinguished so that consumer-facing software does not use overbroad restrictions on interoperable communication that distorts

[31] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.100, 11.111, 11.123, 11.192 (Remedy 1), 11.166, 11.174, 11.175(b) (Remedy 2).
[32] CMA, Mobile Browsers and Cloud Gaming, Working Paper 7 (2024), paragraph 5.52.
[33] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.174, 11.188 (such a publication is mentioned in reference to Remedy 3).
[34] For example, reference to the court's reasonableness approach, rather than the rejected ever possible risk criterion. Breyer, C 582/14, EU:C:2016:779 (19 October 2016).
[35] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.174.
[36] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.11, 11.192.
[37] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.220.

competition among "*multiple adjacent markets and may therefore require interventions that are wider than a single market or a limited number of markets*."[38]

- Apple is prohibited from using any choice architecture that incorporates dark patterns (e.g., ATT or "*consent sludge*" in Google Privacy Sandbox dialog windows),[39]
- Apple to distinguish individuals' personalisation preferences from preexisting data protection obligations on all recipients.

Remedy 2a – Apple to grant "*equivalent access*" to OS features used by Safari for rival browser vendors using Safari's browser engine

MOW agrees with the FRAND approach to functionality used by Safari to any rival browser vendor who chooses to use Safari's browser engine.[40]

MOW believes the same recommendations to avoid circumvention in Remedy 1 should be applied to Remedy 2.

Remedy 2b – Google to grant "*equivalent access*" to OS features used by Chrome for rival browser vendors

MOW notes that in the provisional remedies, the CMA stated under Option A4 the "*Requirement for Google to grant equivalent access to APIs used by Chrome.*"[41]

This remedy is still required, particularly around the outcomes of choice screen architecture that may be prompted by Android in relation to Privacy Sandbox. Just as the restrictions imposed by Apple iOS prevented rival browsers and service providers "*from offering users additional privacy features when browsing the web*" so too is Google's design of its Privacy Sandbox in Android and Chrome restricting the consumer choice signals and necessary interoperability for a range of competitive solutions to offer their services to the set of concerned consumers whose devices run on the Android OS.

MOW does not believe this concern is yet addressed in the current remedies outlined in Potential Remedy 6.

Remedy 3 – Apple to grant interoperability for cross-app functionality to provide in-app browsing

MOW agrees with requiring Apple to make such cross-app interoperability available.[42] Interoperability technically requires a common match key across systems to maintain state. MOW suggests that Apple's de-identified "*random identifier*" be made available to rivals to support such interoperability, with the inclusion of new prohibitions on reidentification by any recipient of this common match key.

Remedy 4 – Prohibitions on Apple and Google against revenue sharing from Chrome or from search advertising

---

[38] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.41.

[39] See CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 8.26ff (unnecessary friction imposed on user journeys), 8.12ff (repetitive and annoying popups for rivals' solutions and prompts reset to default settings).
Apple and Google both employ dark patterns, such as "consent sludge" to steer user choices by increasing friction to choose other services than those of their OS and browser manufacturer. CMA, Mobile Ecosystem Market Study, Appendix J, (10 June 2022) paragraph 78: "A*pple is not applying the same standards to itself as to third parties forced to show the ATT prompt when it comes to seeking opt in from consumers for personalised advertising.*"[39]

[40] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.130-132.

[41] CMA, Mobile Browsers and Cloud Gaming, Working Paper 7 potential remedies (2024), table 4.1.
https://assets.publishing.service.gov.uk/media/66b484020808eaf43b50dea8/Working_paper_7_Potential_Remedies_8.8.24.pdf

[42] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.163.

MOW agrees with restrictions on the revenue sharing agreements that Apple and Google have used to act as one company.[43]

However, given browsers need a funding model, which traditionally has been based on revenue sharing from search advertising, MOW agrees it is important for any rivals to Safari or WebKit be allowed to earn search revenues from search engine providers, including Google.

To ensure Google does not shift its single payment to Apple to merely a multi-payment model, the total payments to any browser ought to be capped as a percentage of revenue from Google to match what such browser vendors receive from rival search providers to Google, in line with the US DOJ Search remedies.

Remedy 5 – Address Apple's abuse of its iOS dominance in mobile OS's to distribute Safari via unfair choice architecture prompts

MOW agrees with obligations the CMA seeks to impose on Apple to ensure it does not abuse its dominant iOS OS to distribute its Safari browser via unfair choice architecture prompts.[44] This same concern applies to Apple using its dominant iOS OS to restrict interoperable functionality required by rivals to compete with Apple's business-facing solutions supported available to app developers. For example, Apple SKAN (ad network and attribution reporting) relies on interoperability in its aim to provide necessary feedback signals to advertisers regarding their cross-app media spend so that they can optimise their media buying to achieve more effective results.

To validate this is not the case, MOW suggests that the CMA conduct independent survey research (as it did with the Verian research) of any proposed choice screens to ensure consumers will not be misled by Apple's language or UX designs (e.g., Apple used large fonts in warning consumers with ATT, but small fonts for the reasons app owners were requesting the use of the interoperable IDFA token).

Remedy 6 – Address Google's abuse of its Android dominance in mobile OS's to distribute Chrome via unfair choice architecture prompts

MOW agrees with obligations the CMA seeks to impose on Google to ensure it does not abuse its dominant Android OS to distribute its Chrome browser via unfair choice architecture prompts.[45]

MOW suggests that the CMA go further in requiring Google not use its Android dominance to retain for itself a consumer choice signal regarding personalisation preferences or advertising choices, but instead as with the CMA's findings regarding Apple's iOS restrictions, ensure competition exists across Android devices for rivals to Google's consumer-facing and business-facing software services to meet the needs of the minority of concerned consumers.

Yours faithfully,

Preiskel & Co LLP

[43] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.228.
[44] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.270ff.
[45] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 11.271ff.

Appendix A – Rebutting pretextual claims to "*improving privacy*"

This appendix aims to clarify why Apple and Google's proposed justifications to their [redacted] conduct have no basis under Applicable Data Protection Legislation. The CMA notes both Apple[46] and Google's[47] claims that their anticompetitive conduct is somehow justified by reference to their ill-defined reference to protecting "*privacy*."

This lack of evidence-based risk assessments has led to a disproportionate restriction of functionality that has distorted competition, by shifting online consumer behaviour away from free access to online websites to accessing the identical content and services via Google and Apple's proprietary app stores. The harm to consumers is the extortion of fees associated with any online payment that would not exist when that same individual were to interact with that same online business via a browser. Businesses must both pass these costs along to consumers in terms of higher prices, but also increasingly prompt consumers to pay to access their property or increase the ad load in their websites to make up for the reduced monetisation ability given Apple's interference with cookie storage.[48]

Apple and Google frequently rely on vague statements of potential risks, without the necessary evidence associated with the likelihood or severity of the risk as required by a proper privacy-by-design evaluation.[49]

In its earlier MEMS report, the CMA noted that unlike Google, Apple had less of a financial incentive to distort competition in relation to digital advertising.[50] Given the recent disclosures about the degree of financial incentives from preferencing Search advertising by undermining rivals Display advertising, we believe Apple has a strong financial incentive to architect ITP in an overbroad rather than narrowly tailored fashion. The CMA did note that Apple indirectly benefitted from Google's Search revenue that was miraculously "*immune*" from Apple's ITP changes.[51]

Tracking requires business data to be linked to specific individuals, rather than deidentified

[46] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraphs 4.20ff, 7.102ff, 11.112ff.
[47] Google, The path forward with the Privacy Sandbox (11 February 2022): "***Google's aim with the Privacy Sandbox is to improve web privacy for people*** *around the world, while also giving publishers, creators and other developers the tools they need to build thriving businesses*." (emphasis added)
https://blog.google/around-the-globe/google-europe/path-forward-privacy-sandbox
[48] Online Platforms and Digital Advertising Final Report (1 July 2020), paragraph 5.326: In research conducted by the CMA it found UK publishers earn "*around 70% less revenue overall*" when unable to sell advertising using third party cookies.
https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf
[49] See GDPR, Art. 25 "Data protection by design and by default," which requires data controllers to balance the "*cost of implementation" and other balance of interests tests associated with the "risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing….*"
https://gdpr-info.eu/art-25-gdpr
[50] CMA, Mobile Ecosystem Market Study, Appendix J, (10 June 2022) paragraph 210: "*Another important difference between Apple's ITP and Google's Privacy Sandbox Proposals is the extent to which they directly impact Apple's and Google's other activities online and ultimately their impact on competition. In particular,* ***Google directly benefits from a distortion in competition in the supply of ad inventory and ad tech services, given its strong presence in both display and search advertising****. Apple, on the other hand, does not have as significant a presence in display advertising, such that* ***there is less of a concern of Apple self-preferencing its own display advertising***."
https://assets.publishing.service.gov.uk/media/62a229c2d3bf7f036750b0d7/Appendix_J_-_Apple_s_and_Google_s_privacy_changes__eg_ATT__ITP_etc__-_FINAL_.pdf
[51] CMA, Mobile Ecosystem Market Study, Appendix J, (10 June 2022) paragraph 212: "***Apple benefits from higher Google Search revenues through its Revenue Share Agreement with Google****, through which it receives a high share of Google Search revenues generated through Safari. For consumers, a loss of competition in advertising can cause harm, for example, by increasing advertisers' costs and causing these to be passed through to consumers*."
https://assets.publishing.service.gov.uk/media/62a229c2d3bf7f036750b0d7/Appendix_J_-_Apple_s_and_Google_s_privacy_changes__eg_ATT__ITP_etc__-_FINAL_.pdf

When referring to protecting and improving "*privacy*," some stakeholders focus on limiting "*tracking*," while others emphasise user control over Personal data, including the possibility of compensation for the use of their Personal Data.[52]

The CMA notes the W3C's definition of "*tracking*" in its MEMS report.

> "*The W3C defined tracking as 'the* ***collection of data regarding a particular user's activity across multiple distinct contexts*** *and the retention, use, or sharing of data derived from that activity outside the context in which it occurred. A context is a set of resources that are controlled by the same party or jointly controlled by a set of parties*."[53]

Per our prior filings, given the undue influence of Apple and Google in the W3C and other standards bodies, MOW suggests scrutinising their outputs carefully. In this particular instance, MOW agrees with W3C's definition of "*tracking*" as referring to the collection of activity data "*regarding*" a particular individual. The second part of the definition defines this individual consumer's activity across different "*contexts*." We would submit that the "*context*" is not determined by ownership or control, but instead by consumer expectations, such that Apple News would be considered a separate context from Apple Weather app, despite common control. Indeed, the CMA concluded that Apple's collection and processing is no better than rivals, who implement the same safeguards.

> "*Our assessment is that* ***Apple's own processing of its users' personal data is no less consistent with the description of tracking (as set out by the UK's data protection authority and the W3C) than what third-party developers do****. More specifically, Apple's cross-app processing activities are similar to those of third-party developers aside from the fact that the latter are conducted under separate corporate ownership.* ***As such, we do not consider there to be a justification for the differences*** *between, on the one hand, how the two activities are described to users in terms of language used respectively in Apple's own prompt and in the ATT prompt to characterise such activities – Apple claims explicitly on its personalised advertising prompt that 'Apple does not track you' – and, on the other hand, the design of the ATT prompt and Apple's personalised ad prompt.*"[54]

Some browser vendors suggest that privacy should be equated with seeing fewer ads.[55] The CMA quotes Brave and Apple among this group that believe "*some privacy features (e.g. option to block ads)*" are associated with "*privacy*" rather than "*user experience*."

Seeing ads has nothing to do with privacy

Yet seeing ads has nothing to do with privacy or data protection.[56] Only the illegal collection or use of Personal Data would trigger a privacy risk. The majority of ads displayed across the open web and in mobile apps rely on people consenting to the use of cookies and it needs to be remembered that for

[52] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 4.130(a): "We have seen evidence (see paragraph 4.195) that privacy may be interpreted differently by different stakeholders….some stakeholders focus on limits to 'tracking' while others focus on giving users control over their data (which may entail getting compensated for allowing tracking)."
[53] CMA, CMA, Mobile Ecosystem Market Study, Appendix J, (2022), footnote 48.
[54] CMA, CMA, Mobile Ecosystem Market Study, Appendix J, (2022), paragraph 73.
[55] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraphs 4.39.
[56] The District Court of Mosbach issued an important decision on August 27, 2024, in case 2 O 89/23, related to Article 82 of the GDPR. The key statement of the judgment is: "*Personalized advertising in the context of using a free service does not cause damage within the meaning of Article 82 GDPR…. According to common sense, it is obvious that* ***the defendant can only make its offer available free of charge because it sells advertising****. This is neither defamatory nor prohibited. If the plaintiff feels uncomfortable as a result, it is completely free not to use the defendant's offers or to pay for an offer without advertising.*" (machined translated) LG Mosbach, decision of 27 August 2024 – 2 O 89/23, GRUR-RS 2024, 25749.

these uses, such cookies do not contain personal data but rather only deidentified match keys, like the ones Apple suggests improve privacy in its own consumer-facing marketing.[57]

MOW suggests that the CMA not refer to "*privacy*" concerns as including features "*to block ads.*"[58] Bronner rejected the ever-possible criterion for evaluating risk, even for the concerned minority of consumers. Any risk from the use of Personal Data applies equally to any data collection and subsequent processing, regardless of whether the data is collected for advertising or otherwise. Accordingly, we suggest true privacy features focus on the more accurate privacy concern related to prohibiting the use of Personal Data for advertising.

Rejecting Apple and Google's attempts to resurrect the rejected "*first party*" exemption under security concerns

Security can be defined as preventing unauthorised access.[59] However, this definition raises who is empowered to provide appropriate authorisation. When the business data in question is neither Personal Data nor sensitive information, then it seems reasonable that the business controlling that data ought to determine which partners can access it. Having Apple and Google indiscriminately block such interoperable exchanges and sharing causes grave competition concerns, which is at the heart of concerns regarding Apple's ATT and Google's Privacy Sandbox. When the data in question is Personal Data or sensitive information, it seems reasonable to have greater safeguards in place, such as deidentifying the data or rendering it non-sensitive.[60]

MOW supports Apple and Google's innovations that truly protect against the unauthorized use of sensitive data and Personal Data. However, Apple and Google should cease confusing "*tracking*" and "*first party*" and "*site isolation*," where realistic concerns relate to Personal Data and Sensitive Data, with the necessary interoperability required by rivals to compete against the business-facing services these OS and browser vendors bundle into their consumer-facing software. Apple and Google's overbroad definitions disguise their interference with necessary interoperability that is distorting digital markets through the abuse of their respective dominant positions in consumer OS and browser software. In short, tracking must not be confused with interoperability.

[57] See for example the screenshot to Apple's privacy policy in this submission.
[58] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraphs 4.40.
[59] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 4.130.
[60] The California data protection law allows for transient processing to render sensitive information non sensitive. See 1798.140(e)(4).