PREISKEL & CO

**MOW Response to CMA Mobile Ecosystems Market Investigation Reference ("MIR") Consultation**

Below we provide an executive summary, a summary of issues and remedies identified in the CMA's Final Report, and a discussion of what is needed to achieve "**Browser Neutrality**". We then provide our responses to the CMA's questions.

**Executive Summary: the danger of platform and browser bundling and importance of Browser Neutrality for effective competition in Mobile Ecosystems**

1. The scope of the proposed MIR[1] recognises Browsers as "a key gateway" … "for users and online content providers to access and distribute content and services over the internet." We agree with the CMA's observation at para 1.21 that, absent intervention, Apple and Google are highly likely to retain their market power in the supply of mobile browsers and browser engines for the foreseeable future and that an adverse effect on competition arises.[2]

2. Browsers can be divided into Browser Engine and User Interfaces ("Browser UI") and competition issues identified accordingly:
    a. **Browser (rendering) Engines** appear to be driven by web compatibility. The scale of technological developments worldwide suggests a significant economy of scale, but tactics of browser manufacturers in providing repeated and successive upgrades, also acts as a barrier to entry for rivals and should be further investigated.
    b. **Browser UI** competition.[3] The presentation of website information rendered by the browser engine and information to navigate to websites is a functionality that was, originally, limited to such display and navigation and has recently become a vehicle for other functionality. Where choice exists, it is emerging. Edge, Brave, Samsung, Opera and many others offer different interfaces and experiences to consumers using identical Browser (rendering) Engines.

[1] As set out in Section 1 of the CMA consultation document (para 1.15 et seq.). Paras 1.16-1.21 identify limited competitive constraints on browsers and significant barriers to competition. The Final Report identifies issues with browser engine restrictions in iOS (bundling of Safari and Webkit Browser Engine within Apple's platform), which is mirrored by the anti-competitive bundling of Chrome and Blink Browser Engine in Android.
[2] As detailed in Chapters 5 & 8 of the CMA's Final Report.
[3] Like the issue that arises for service providers, aggregators and resellers at retail level in high fixed costs network industries with high externalities and economies of scale (and high concentration levels) of businesses in other markets e.g., telecoms, electricity, energy or water

3. Other application software can be added into the browser that are not core to the browser engine's role in facilitating navigation and interaction between consumers and digital properties they visit. These additional application software features are sometimes hidden from the user (e.g., Topics, Fledge, Gnatcatcher, Attribution API, etc.). Sometimes this application software is enabled via a plug-in or extension, such as ad blockers. Bundling these additional software applications into the browser (e.g., ad blocker software in the case of Brave) does not change the core function of the Browser Engine, nor the User Interface to facilitate user interactions across digital properties. However, it may restrict competition, if that browser manufacturer prevents rivals' software solutions from operating, providing similar functionality, or via default, preferences their own services. These additional software applications meet different needs in the same way that Microsoft's Operating System was designed for a different purpose than the Windows Media Player, which was found to be an anticompetitive when bundled.[4] In the same way that apps in app stores can be restricted by platform owners, apps in browsers can be restricted by internet gatekeeper manufacturers.

    a. **Wallets**. By way of example, the Open Web enables multiple payment systems and a range of choice. The integration of only one wallet into a platform, ***at any point in that platform***, involves foreclosure of other wallet suppliers. It may be accompanied by self-preferencing and anti-competitive discrimination in the supply of payment services and systems.[5] This can raise barriers to entry in payments markets. The CMA has identified the issue of App Store payment systems. We agree that bundling of separate and independent functionality, such as technical limits on payment systems used by apps in apps stores, limits competition and choice.[6] Similarly, the issue arises where the platforms owners add wallet functionality into their browsers. We have raised and submitted separately the issue of the anti-competitive integration of payments into the browser, as currently attempted at the W3C, as a matter for further investigation.

    b. **Authentication, security and privacy**. We also suggest that websites that exist on the Open Web normally provide for themselves authentication, security and privacy. Entry to each website is usually accompanied by a user being asked to share data with that site, on terms that are specific to that site, and for that site's own purposes. Competition and privacy can better be assured where choices are exercised freely and with regard to the purpose for which consent is requested. Similarly, website owners in B2B

[4] *Microsoft Corp v Commission of the European Communities,* Case T-201/04.
[5] There is a need to avoid market distortion in the integration process, and to ensure that it works in the consumer interest. Similar notions are expressed in relation to Apple Wallet at paras 6.24 et seq., 7.35, and 8.170.
[6] We note that the CMA has highlighted instances of decreased competition arising from the Apple Wallet at paras 6.32 and 6.39-6.41.

relationships may be better able to determine what data is needed to enable legal transactions to be efficiently conducted.

4. **Objective justification or integration benefits**. There is no clear inherent need (or obvious objective justification) for such functionality as described above to reside bundled into the browser or OS solutions, and no reasonable requirement that such manufacturers have exclusive control over these adjacent applications. Alternative solutions should always have a pathway to market, and care is needed not to allow product integration decisions to close off alternative designs that should continue to exist on the Open Web.

5. **Definition of a browser and assumptions of browser functionality**. The Final Report does not dwell on the issue of the browser's functionality and the way that it can be misused to embed functions that otherwise reside on competing websites. That issue was considered in the Privacy Sandbox case. Consistency of analysis by the CMA suggests that where a browser manufacturer seeks to misuse control over the browser to block existing functionality (such as User Agent String data or cross-site data for a platform's exclusive use) or substitute in-browser functionality for Open Web functionality, that should be investigated and assessed on a consistent basis. We consider this is a critically important issue to consider in the next stage of the investigation. Features that may be bundled into the browser, ***or may already have been so bundled***, as a means to limit competition and restrict user choice, include authentication, privacy and security settings that otherwise reside on each website. There is a need to assess what is, or could be offered separately and not to make any assumption as to the starting point of the inquiry, before examining any of the benefits of any current integration, if they exist at all.

6. The nature of the browser, what is defined to be within the browser and its boundaries should thus not simply be "taken as found". The CMA has picked up on the fact that the current position of the markets represents the outcomes from years of dominance and abuse. The current markets are thus already distorted by the commercial activities of dominant entities. An early step on the next stage of the investigation needs to be to define what is, and what is not, the functionality of a browser absent further abuse and additional bundling.

7. **Consistency of assessment and absence of objective justification.** We have raised with the CMA the issue of browser bundling and consider that since Open Web alternatives can and often do include authentication, security and privacy settings, the assumption should not be that such elements are part and parcel of the Browser UI or Browser Engine. There is no reason to assume that monopoly provision of this functionality is required for consumers to benefit from

innovations, and there is history of open design (notably, the integration of DOH DNS changes into Google Chrome, which were structured to remain open to several providers).

8. We draw to your attention to the fact that the Daily Mail and General Trust is currently raising this issue in litigation in the USA. That litigation notes that browser changes carry a serious risk of decreasing competition in advertising systems, e.g., in header bidding.[7]

9. The MIR consultation scope covers the relevant issues, but we have concerns about both the internal consistency between the CMA's Mobile Ecosystems Final Report with its statements concerning Apple's ITP and ATT therein and its Privacy Sandbox Decision.

10. The CMA refers to the way in which Apple's ATT will reduce revenues for apps who employ an ad-funded business model.[8] The Final Report also acknowledges that some developers have already turned to subscription-based business models as a result of Apple's ATT changes on apps hosted on iOS devices. Although MOW represents a variety of members from different areas of the supply chain, the advertising technology industry that supports news publishing is significantly affected by this, which may in fact constitute an adverse effect on competition on both industries as a result of Google and Apple's anti-competitive browser or OS restrictions. With this in mind, and with the CMA admitting that "ATT is likely to result in harm to competition, make it harder for app developers to find customers and to monetise their apps, and ultimately harm consumers by increasing the prices or reducing the quality and variety of apps available to them", we trust that its concerns in relation to ATT will be fully addressed in the scope of the CMA's MIR.

11. As the CMA recognises, many apps are made available to end users for free at the point of use by virtue of ad-funding. Apple's ATT framework blocks third-party advertisers' access to the IDFA, meaning that it gives its competitors a limited opportunity to offer personalised advertising. However, ATT does this without blocking Apple's own access to critical information and data needed to produce effective advertising solutions. As such, Apple is able to continue offering advertising solutions that will remain free for the end user (and therefore more desirable in the current socio-economic climate), whilst other developers are forced to (partial) subscription-based models. Apple has an added incentive to push for these

[7] *Associated Newspapers Ltd. and Mail Media, Inc. v. Google LLC and Alphabet, Inc*. Case 1:21-cv-03446 (S.D.N.Y., Apr. 20, 2021) at para 41.

[8] *See* Final Report at para 6.216-6.219: "*ATT reduces the revenues that developers can earn from in-app advertising. This means that the ad-funded business model for apps will likely generate less revenue for app developers compared to pre-ATT. As a result, developers might turn to alternative ways to monetise apps, charging users for content instead of providing it for free. Given that Apple charges a 30% commission on most in-app purchases of digital content through IAP, Apple has an incentive to encourage such a shift by developers.*"

subscription-based models, given that it takes 30% from any purchase of an app made on its App Store, or 30% of any in-app purchases made through its Apple Pay system (the only system permitted on apps on iOS devices).

12. To reiterate the point made in relation to consumers above, costs borne by consumers should be an especially important factor for the CMA in its upcoming analysis when considering harm to consumer welfare in light of the current rising costs of living. The CMA makes clear that it aims to prioritise those who are disadvantaged;[9] a point which at present is not considered in the CMA's MIR consultation. At a time when inflation is rising, and the cost of living is increasing, those who are most vulnerable should be prioritised. Should the CMA leave functionalities in the browser to be dictated by Apple and Google, it risks neglecting the most vulnerable, who will be unable to access free apps or content therein, but who will also be unable to pay the cost of a subscription for these services. As such, it is important for the CMA to consider the harm passed onto consumers.

13. Below we briefly cover the CMA's identified barriers to competition and suggest remedies that may address them. We then address the CMA's consultation questions.

**Barriers to competition**

The main barriers have been identified in the CMA's Final Report include:

a. Apple's restriction that requires other browsers to use Webkit;
b. web compatibility;[10]
c. native apps' use of in-app browsers;
d. pre-installation and defaults;
e. restrictions on access to functionality;
f. revenue sharing agreements in search;[11]
g. control over information shared with advertisers;
h. user controls over data access "privacy" settings; and
i. restrictions that reinforce Google's position in search and display advertising.[12]

**Browser Neutrality Remedies**

[9] CMA, Prioritisation Principles for the CMA (CMA 16), April 2014. *See* para 4.3 at page 7. "*[The CMA] may sometime favour projects that would benefit disadvantaged consumers, in order to build overall consumer confidence in markets.*"
[10] Web compatibility is the browser's ability to properly access and display the content on a particular web page. *See* Chapter 5 of the Mobile ecosystems market study final report for further details.
[11] Competition and Markets Authority (2020), Online platforms and digital advertising market study, Appendix H.
[12] *See* Final Report, Appendix J. We note that the browser controls labelled "privacy" neither align to appropriate data protection regulation definitions, nor prevent large organisations or even their own parent organisation from accessing the same personal data related to digital activity linked to consumer identity.

14. **Apple's restriction that requires other browsers to use Webkit.** Remedy: A requirement on Apple and Google to allow other competing (i.e., non-Apple or Google) Browser UIs and Browser Engines to be used on each of Apple and Google's platforms to increase competition on privacy and security settings when browsing the web. This would mean increasing competition between systems that increase authentication, privacy and security settings on websites or systems for Open Web sites and functions in Browser UIs.

15. We agree with the CMA's view that "the main implementation costs associated with additional API access for browsers are likely to be the technical costs of supporting interoperability between the operating system and third-party browsers. Apple's submissions do not suggest that these implementation costs are likely in themselves to be disproportionate".[13] We disagree with Apple and Google where they have stated that restricting access to APIs is justified where these APIs govern access to privacy and security: those functions can be addressed through improved end user interfaces in both Browser UIs and elsewhere using independent systems or via authentication and personal identity management systems such as referred to in the CMA's July 2020 Online market Final Report in Annex Z.

16. "**One company knows best**": **Unbundling of Sign-in**. There is also a major, unstated assumption that somehow an integrated privacy system is likely to be more secure when operated by each platform supplier, whereas their incentives may lead to precisely the opposite. In Google's case it has strong incentives to gather large-scale data in order to sell more advertising and other services. Google benefits from infringing consumer privacy to use for hyper-targeted advertising to make more money on its own digital properties. This may be why it exempts all its own properties, all well as other large organisations that operate multiple domains (e.g., via First Party Sets) from its standard interference with interoperable data transfers. It is telling that the large browser manufacturers mention only the risks associated with other companies, without specifying what these are, and do not mention the significant risks from large first-party data handling (e.g., the incentive to adopt incomplete or misleading consent mechanisms as part of an integrated solution). A neutral approach would always allow a competing third party to handle data, provided that it does so responsibly, and this access is crucial if there is to be a fee offering of websites at the point of use by consumers. As part of this, unbundling of authentication for web use from signing into Google or Apple's Browser UIs is also likely to be needed.

[13] Final Report, para 8.133.

17. **Web compatibility**: Remedy: we see scope for Gecko engine and Webkit engine competition to improve functionality in competition with the Blink engine (and others such as Goanna which are occasionally referred to, but which may provide an important source of fringe competition[14]). Technical oversight may be needed to prevent compatibility being used as a club with which to beat rivals and to ensure that updates improve interoperability and non-discriminatory compatibility between the browser and the Open Web. Expecting Apple to improve Webkit and its compatibility with websites on the Open Web when faced with competition from Blink-based browsers is not the only commercial solution available to Apple. Given the considerable cost and risk in ensuring web compatibility,[15] **there is an appreciable risk that Apple could instead decide to close its Webkit engine and use Blink**, either with a "Chrome UI" or its own new UI. To avoid this poor outcome for competition, it is necessary to ensure that entrants and smaller players are able to expand, decreasing the incentive for Apple to simply not offer the product.

18. **Native apps' ability to use in-app browsers**. Technical interoperability is needed so that functionality that could operate independently over the Open Web is unbundled. There is a strong case for a prohibition on in-app browser availability. Open interfaces and the access thereto should apply to both Apple and Google for the benefit of third parties, including to provide progressive web apps and other browsers. This reflects the important point, as developed in the *Microsoft* Media Player case cited above, that products running on a platform compete in a different market from those in the upstream platform market.

19. There is much to gain from a ***subtractive*** remedy whereby platforms must remain open but can integrate their own apps if this is truly the consumer preference. So, for example, the CMA should enable Progressive Web Apps and sign-in to Open Web systems and prohibit the exclusive bundling of such authentication functionality into platform or the Browser UI by the manufacturer of this other software. Any functionality that can be provided over the Open Web should not be foreclosed, restricted or bundled on an exclusive basis into the Google or Apple platform, either in the internet gatekeeper Browser UI or Browser Engine or elsewhere.

20. **Pre-installation and defaults**: all such preinstallation and defaults identified as creating anticompetitive effects must be subject to neutral user choice architectures and choice screens. We note that the CMA is proposing to consider further the issue of consumers' ease of switching and "*mandate certain forms of choice screens to be displayed to users, or other*

[14] As was found to be the case in *Microsoft Corp v Commission of the European Communities,* Case T-201/04.
[15] And bearing in mind that businesses at technologically sophisticated as well-funded as Microsoft have given up on Trident. *See* Microsoft Support, "Download the new Microsoft Edge based on Chromium"; Venture Beat, "Microsoft is embracing Chromium, bringing Edge to Windows 7, Windows 8, and macOS"

*requirements relating to the way choices are displayed*".[16] We consider that authentication and sign-in systems to competing offerings and websites should be included in that further review for consistency and to avoid workarounds to other remedies.

21. **Restrictions on access to functionality**: here, access to existing functionality risks limiting competition by entrenching the existing supplier of existing functionality of the internet gatekeeper Browser UI or the Browser Engine as the supplier for all such functionality to others. Technical access and interoperability to currently existing interfaces should be required but narrowly defined so that interoperability as to core browser functionality and innovation can then take place in other features, functions and apps. Steps need to be taken to prevent an increase in the incentive for the internet gatekeepers to expand the functionality of their internet gatekeeper browsers to the individual consumer's detriment. For example, browser bloat is likely already contributing to adverse end user experiences available memory and battery usage. Technical access and interoperability to something considered to be within the internet gatekeeper Browser UI needs to be very carefully ***defined*** to avoid misuse by the internet gatekeepers. Put another way, functionality that does not relate to rendering of web pages and input data used by the Browser UI or Browser Engine which can, and should, be available for use by business solutions to web properties (i.e., third parties) can inadvertently or deliberately be bundled into the browser. For example, Apple's ITP and Google's Privacy Sandbox browser changes both embed, or propose to embed, functionality into the browser that otherwise exists and is used by businesses on the Open Web. They also limit data gathering by competitors to each of Apple and Google, and allow Apple and Google to interfere with existing contracts and functions for sign-in to independent websites.[17] They amount to a data exclusivity requirement embedded in the browser by each internet gatekeeper platform, including important architectural design points in APIs, which should be competitively designed, and in some cases, prevent data from ever being collected in the first place. This is already limiting competition to Apple and Google in fraud and security products and services, and is reinforcing their position in advertising, its measurement, assessment and attribution. Any browser investigation and any applicable remedy both need to define the boundary of the browser for rendering web pages and disaggregate access to underlying data to enable third-party developments and innovation over the Open Web. The obligations covering access and interoperability need to apply to all

[16] Final Report, para 8.147.
[17] See the *DGMT vs Google* litigation in the USA: *Assoc. Newspapers Ltd. and Mail Media, Inc. v. Google LLC and Alphabet, Inc.* Case 1:21-cv-03446 (S.D.N.Y., Apr. 20, 2021).

technical inputs, commercial inputs and financial inputs; not outputs as determined by each of the gatekeepers.[18]

22. Access interfaces can also be mandated to Apple's Safari for use by other Browser Engines[19] and to Google Chrome for other Browser Engines, as well as vice versa, and measured against outputs to both interoperating businesses, as well as individuals (i.e., in terms of use and functionality).

23. Contractual discrimination also needs to be guarded against (trading terms have an effect on quality of experience and quality of service (e.g., latency, round trip delay and speed of overall functionality)), and financial discrimination (e.g., payments that may otherwise occur between functions of Apple and Google as internet gatekeeper browser manufacturers and those in relation to third parties – referenced further below).

24. **Revenue sharing agreements in search (and the revenue sharing agreement between Apple and Google)**: managed withdrawal from such arrangements appears necessary if disruption and the provision of free internet services is not to be undermined. Non-discrimination and prohibition of self-preference obligations can address some of the issues identified if applied to Google as the search provider and policed carefully.

25. **Control over information shared with advertisers**: we welcome the statements made by the CMA that:

> "***Self-preferencing through the approach to privacy***
>
> *8.187 Both Apple and Google continue to evolve the way in which users make choices about privacy, and what data they share with app developers.*
>
> *8.188 As discussed in Chapter 6,694 Apple has introduced privacy initiatives (ITP and ATT) which are intended to enhance users' privacy through providing greater control over the use of their personal data, which we recognise bring privacy benefits. However, we have concerns that there are differences between the approach to privacy in respect of Apple's own apps such that it is not applying the same standards to itself as to third parties, and that consumers may not be making fully informed choices.695 […].*

[18] European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)). *See, in particular,* Articles 5 and 6 for obligations relating to access and interoperability.

[19] To remedy the fact noted by CMA that extensive information on features used by Safari including access to audio features and webcams which are not available to other browsers on iOS.

...

*8.191 We would also encourage Apple to engage with a broad set of industry participants in advance of introducing any changes to the ATT framework – or before implementing similar policies in future – given the potential impact it can have on their businesses.*

*8.192 Finally, we would expect Apple to support and engage with industry efforts to develop new standards for privacy preserving functionalities that support a thriving ad ecosystem. This is consistent with what we expect from Google as part of the commitments accepted on Privacy Sandbox.*

*8.193 We intend to continue to engage with Apple on these issues, in partnership with the ICO, now that this market study has concluded.*"

26. These statements suggest that Google (in its Privacy Sandbox) and Apple in its ITP and ATT actions overstate their "privacy" claims for their own commercial benefit. We agree. What is to be done is then less than clear.

27. Advertising promotes products to users, informing them of things they might want and is the cornerstone of competitive markets. Control of advertising messages, and the ability to develop marketing insights based on a rich stream of (GDPR-compliant) data is essential to bring products to market and to promote them successfully. Understanding user needs is thus the business of every business and brings major consumer benefits (some obvious – knowledge of discounts; some less so – for example, the promotion of a new green product to a keenly green consumer on a targeted basis).

28. Google and Apple are increasingly restricting data required for advertising, as well as payments made via app stores, whether generally across the web or specifically, for products sold via apps in apps stores. The CMA should seek to check that competition is working well, and where it is not (e.g., 30% platform fees; arbitrary data collection and handling restrictions), then a targeted approach should be taken to ensure that innovative competitors are not prevented from competition through arbitrary restrictions.

29. We applaud the CMA's wise scepticism of Apple and Google's claims concerning individuals' privacy. It is highly questionable that Google and Apple's promotion of first-party relationships improves consumer privacy at all. First, there is the issue of whether the consents applied by these large networks align with the consumer interest, and there is considerable current experience to suggest that this is an area open to serious anti-competitive bias (e.g., iOS 14.5's

prompting initially not applying to Apple). Google collects individuals' personal data and marries up large data files using data provided by large customers. This enables significant data profiling to take place, and although Google has doubtless undertaken GDPR compliance reviews, and presumably uses safeguards like pseudonymisation, there is a critical weakness in such a large data file emerging which could well link relatively invasive data (e.g., geotargeting; automated email scanning). Smaller rivals pose lesser risks since they handle smaller data sets and do not have the same network reach (e.g., two cookies rather than 24/7 geolocation data). There is a serious risk that competition without clear disclosures encourages the most invasive data handling, which may well exceed what consumers would agree to with more transparent disclosures. It is essential for rivals to be able to compete on the basis of the quality of their data handling practices (akin to Fairtrade certification for groceries). If this is integrated into the browser, however, it will prove practically impossible to do so. We note that previous investigations by the CMA into Online Markets and Digital Advertising and Google's Privacy Sandbox acknowledge the discrepancy as far as is possible for a competition authority.

30. The CMA and ICO have accepted in their Joint Statement of May 2021[20] that there is no necessary correlation between privacy risks and first or third-party domains: the sensible position that *what* is done with the data is more important than *who* does it. Google and Apple nevertheless both claim that logging into their browser would work to limit the number of entities "tracking" a user on their browser. The identifiable personal information belonging to a user is then only available to Google or Apple when a user signs in through their platform. This seriously limits the scope for GDPR-compliant independent providers of advertising services, which are currently offered by a range of manufacturers.

31. By definition, pseudonymous identifiers keep an individual's offline identity entirely separate from a culmination of their online activity. The sole privacy concern is only and always the connection of someone's online identity to what is otherwise simply a file about "User123" going to X site and Y site. Personal details relating to an individual are neither needed nor desired by advertisers and developers to sell products and operate their businesses. Pseudonymous identifiers provide enough information to know what might be of interest to a certain user for the sole purpose of tailoring advertising of products that may then be relevant to that user. By limiting the scope for this decentralised data handling and the permissionless innovation it implies, Google and Apple are thus foreclosing pseudonymous solutions, so

[20] CMA and ICO, "Competition and data protection in digital markets: a joint statement between the CMA and the ICO", 19 May 2021.

advertisers are facing an abrupt decline in the data available for no specified reason, nor a basis for compliance following specification of a legitimate and non-discriminatory concern.

32. For example, if there are concerns about the creation of unwelcome advertising categories (e.g., health, solvency) as frequently referenced in data privacy complaints (e.g., Johnny Ryan's complaints against TCF[21]), then these could be addressed through rivals adopting (further) network rules and enforcement initiatives in the handling of their identifier-based systems. There is no rational basis on which to assume that large first-party systems will somehow solve the problem, since they face similar incentives, and in any event, there is a less competitively restrictive approach to addressing concerns about data accumulation from pseudonymous identifiers, in the form of network rules.

33. Apple has introduced its own version of single sign-on which moves to sign in away from the individual publisher or website, and towards the browser manufacturer. This shifts functionality into the browser itself posing the product integration concerns noted above: especially, the conflict of interest in data handling by the federated log in provider (Apple).

34. Apple's Intelligent Tracking Prevention ('ITP') framework introduced on Apple's browser, Safari, has a similar anticompetitive effect. The ITP framework is a series of features that reduce cross-domain data transfers, i.e., it allows Apple to do what others are prevented from doing, which has a significant effect on competitors who rely on reaching users through Safari. This substitution effect for the internet gatekeepers' own B2B advertising solutions for that of even a large rival is illustrated with the well-publicised decline in Facebook's mobile revenues, as Apple's solutions, which were not subject to the same data input restrictions, offered to advertisers.

[21] *See,* for example, Decision of the Dutch Data Protection Authority of 2 February 2022 in response to Johnny Ryan's complaint; Privacy International, "Regulatory complaint against Google and other "ad tech" companies under Europe's GDPR by Johnny Ryan, Jim Killock and Michael Velae", 12 September 2018.

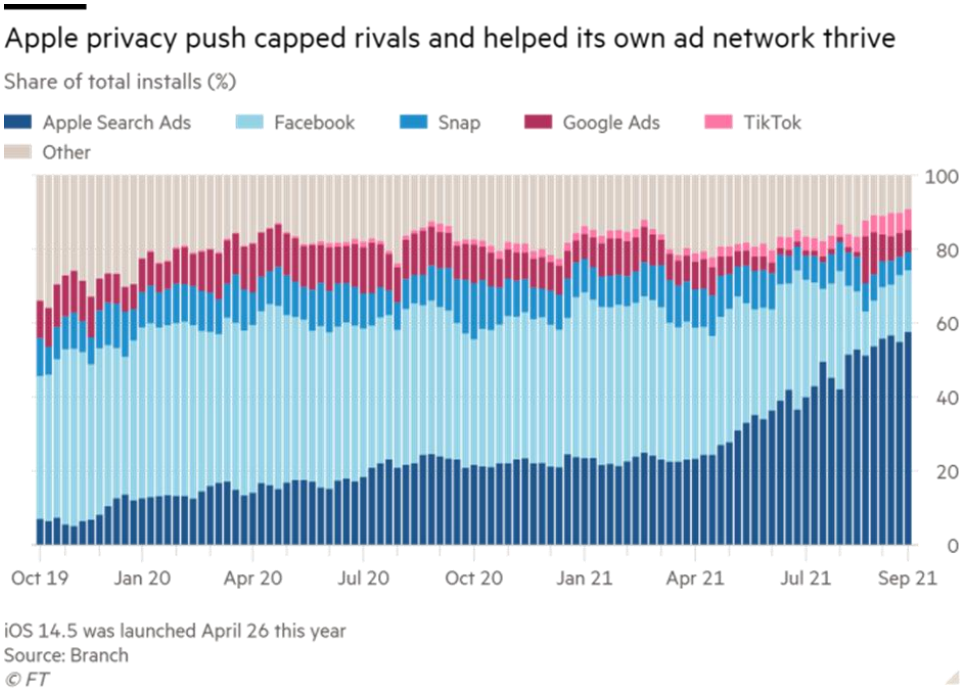


*Figure 1. Source: Financial Times*

35. With the introduction of the ITP framework, Apple released a list of "unintended consequences" to competitors' business practices. In doing so, it accepted that its actions had significant anti-competitive potential. Apple failed to justify this behaviour of "protection of consumer privacy" and in any event, could have specified less restrictive means to achieve "privacy" (which was not defined in any but the broadest terms, and certainly not in any specification which third party businesses could comply with).

36. Similarly, Apple also operates a 'Sign in with Apple' functionality, which allows a user to sign into a third-party app, website or most importantly a web browser using their Apple ID (usually made up of the user's email address). Apple is therefore able to view the user's activity and combine this information with the personal information given to Apple when the user has signed up for an Apple ID (e.g., their email address, date of birth, and payment method). This explains why Apple is not concerned by the loss of *other* data sources. Third parties are left without access to any or a critical amount of data needed to improve their own online advertising model's accuracy. This seriously harms competition from them.

37. The ultimate consequence of a Federated ID login on either Chrome of Safari would be disastrous for any third-party organisation whose business model relies on receiving and analysing the data proposed to be restricted. If the CMA allows Web ID and ITP to continue operating and concede their functionality to be in browser functionality, Google and Apple will continue to enjoy uninterrupted access to users' data, while restricting downstream data flows.

38. At the very least, dominant platforms, including browsers, should be required to specify reasonable and non-discriminatory specifications of concerns if seeking to restrict data flows, so that rivals can check that any restrictions are narrowly tailored and based on evidence, and to push back if this is not the case. This would simply be the well-known adage that "sunlight is the best of disinfectants; electric light the best policeman."

39. At the moment, data handling restriction decisions are, on the contrary, taking place in the dark. As the CMA notes, these organisations are purporting to act like regulators, but without the due process safeguards which public regulation would apply.

**CMA questions**

a) **Do you consider that our analysis is correct with respect to the suspected features of concern in the supply of mobile browsers and cloud gaming in the UK?**

40. In short, we see Browser and Web functionality that is currently being impeded by Google and Apple. The CMA appears to agree, but we are concerned that the position could be inconsistent unless altered as set out above.

41. The Open Web was developed through, amongst other factors, fierce competition between browser manufacturers, with each striving to enable their respective user base to view the Web. Commonality started to emerge between the browsers being created. This included, for example, the use of the "HTTP" communications layer protocol, which enables a user to retrieve a hypertext link but is made up of a number of different functionalities that render such a link visible to the user. HTTP, along with the other 'building blocks' of the Web, including the IP address and User Agent String, have essentially become de facto standards of interoperability on the Web that enable the Browser to effectively render web pages to individuals.

42. Google and Apple have replaced the fundamental building blocks that traditionally make up the browser as a rendering engine or web viewer and have designed integrated functionalities. There are good aspects of some integration, but a risk emerges of limitations to information that passes in and out of the browsers. This is possible because platform dynamics – especially, high barriers to entry – mean that integration decisions could be anti-competitive and depart from the consumer interest.

43. These features have impacted competition immensely. Yet several of the features do not relate to webpage functionality, or webpage rendering, but instead limit data flows and thereby undermine competition. Since these functionalities compete with functionality on the Open Web, by introducing changes to their browsers, Google and Apple are limiting the ability for web-based functionality to continue.

44. For example, the use of progressive web apps is promoted by the CMA, but such apps are often provided by websites that depend for their incomes on independent sign-in and independent agreements between users and individual websites for use of data by those websites. Google and Apple's changes to their browsers seek to restrict information from the browser well beyond what is needed for any stated rationale (which has, in any event, not been forthcoming in any of its details). This reduces or eliminates competition from websites that currently exist.

45. The changes to the functionality of the browser necessarily affect all operations that pass over the browser. We therefore commend the CMA's decision to investigate browsers and include in-app web browsers in the scope of its market investigation.

46. We note that the CMA has indicated it does not intend to include desktop browsers within the scope of its investigation but would urge the CMA to reconsider this position. Given that the CMA admits that Apple's Safari and Google's Chrome browsers are the largest on both mobile devices and on desktops with a combined market share of 90%, the changes to Google's and Apple's browsers will have a similar detrimental effect on competition in the same way that they are currently having on competition on smartphones and tablets.

47. There is acute scope for workarounds unless browsers are addressed. This can be seen in the Apple iOS 14.5 ATT incident: the same question was asked in apps ('Ask App Not To Track') that appears in a cookie dialogue ('Accept/Decline Cookies'). There are equivalent practices affecting the same services depending only on whether they are presented in an app- or web-based format (reflecting the fact that many apps are essentially reskinned browsers). It would be inconsistent, and potentially ineffective, to turn a blind eye to the browser while investing time and effort on the app side.

48. It is, however, less than clear in the remainder of the Final Report or consultation how these issues, which are accepted to be within scope of the MIR, will be addressed. Given that they are interrelated with the other issues listed by the CMA concerning browsers, we are concerned that they don't meet with the CMA's duties and reasonable decision making; in short, we

consider it would be unreasonable for these issues not to be reviewed in detail in the CMA's MIR.

49. Overall, we are concerned that the CMA has identified the key issues but, so far, potentially understated the dynamics of the web and that web functionality and platform functionality are often interchangeable and can provide competitive constraints on one another if allowed to operate unimpeded by internet gatekeeper platform manufacturers.

50. It is clear that the internet is primarily funded by advertising, as are much of the business of both Google and Apple. There are serious concerns that Big Tech uses data handling restrictions to undermine competitive constraints on it. There is no good reason to restrict GDPR-compliant data flows unless there is a specific and articulated basis. If there is a privacy concern, it can be stated clearly and addressed on a narrowly tailored basis, avoiding competitive harm. Competition should only be restrained where it is objectively justified, and proportionality requires the tailoring of a restraint to the specific issue that needs to be addressed. The overly broad implementation of a restriction of competition will not be the least restrictive alternative if proportionality is not respected. Competition over privacy and other consumer benefits should be promoted between Browser UIs and third-party website authentication systems. The CMA should not concede that management of authentication is uniquely a browser function.

**b) Do you consider that our analysis is correct with respect to the reference test being met in relation to the supply of mobile browsers and cloud gaming in the UK?**

**Browser definition: Risk of inconsistency and self-preferencing**

51. The CMA should not concede as a starting point in its MIR the definition of the functionalities of a Browser Engine or Browser UI as they currently exist. The CMA Final Report identifies significant indications of anticompetitive activity which is likely to have continued for some time. Among the issues identified is bundling. We submit that bundling of functionality within the browser as well as bundling of functionality into platforms is part of the problem to be investigated.

52. To define the scope of the MIR as including the current functionality of the browsers may logically concede that no such bundling has taken place and is internally contradictory of the inclusion of in app web browsers and undermine the ability of the CMA's investigation of the

facts. For example, past anticompetitive acts (such as ITP changes some of which date back to 2019) might not be covered.

53. Unless carefully defined, there is a high risk that browser manufacturers will give undue preference to their own systems, processes and apps, and use sign in to obtain "user consent" in circumstances where there is increasingly limited choice, as well as affirmative restrictions on handling the data necessary to create competitive constraint on legacy "Big Tech" players. Anticompetitive behaviour from bundling of non-browser functions within the browser manifests itself in a number of different ways, and all should be investigated including through Google and Apple's authentication systems using Web ID login and Federated Login, which essentially ringfence the user's data from being exploited by anyone apart from Google or Apple. This effectively forces advertisers to use Google's and Apple's advertising services (e.g., Google Ads and SKAN measurement tools). The introduction of a Privacy Budget and Trust Tokens, which eliminate independent trusted intermediaries for multiple activities related to fraud prevention and online security, reinforce Google's position in advertising technology and growing Apple's role in measurement.

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

54. Yes, provided the above issues are included within the activities investigated.

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

55. Yes, provided the above issues are included within the activities investigated.

**e) Do you have any views on our current thinking on the types of remedies that a MIR could consider (see above and Chapter 8 of the market study Final Report)? Are there other measures we should consider?**

56. We are not sure that the remedies that are considered fully include the remedies that may be needed to prevent in browser bundling and foreclosure of innovation by of third parties and have set out our views in that regard above.

**f) Do you have any views on areas where we should undertake further analysis or gather further evidence as part of an MIR in relation to the supply of mobile browsers and cloud gaming? We would particularly welcome any specific evidence from respondents in support of their views.**

57. We have outlined our view on in-browser bundling and the competition issues arising and what would be needed for Browser neutrality in our comments above.