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:
browsersandcloud@cma.gov.uk

By email only

Our Ref: TC/ADM838
23 February 2024

Dear Sirs,

Re: Response to CMA's January 2024 Issues Statement on mobile browsers and cloud gaming

This letter is on behalf of the Movement for an Open Web ("MOW"), a not-for-profit organisation that is seeking to secure an open and decentralised web. We write in response to the CMA's Issues Statement dated 13 December 2022 and further to our first response dated 20 January 2023 (attached as Annex 1 to this letter).

Monetisation in the web and data

The consumer's ability to enjoy the web, which is "free", is driven by publishers' ability to monetise their content via digital advertising. The efficiency of digital advertising is based on the volume, frequency, and accuracy of data that is exchanged between the ad buyer and the media owner (ad inventory seller), as well as their ability to assess such data in order to be able to generate a positive return on ad spend by establishing whether such ad has been successful.[1] A common deidentified ID is needed to measure what techniques are driving the most value.

The CMA highlights that "browsers are primarily monetised through search" (para. 13). However, the browser also represents a vital gateway through which consumers access the web, rendering data available via the browser crucial for digital advertising and publishers' ability to monetise. Therefore, when establishing whether Google and Apple have "unilateral market power in the supply of browsers and browser engines" (para. 24), the CMA should include scope to evaluate the role of data (common deidentified IDs) in this market and the ways in which Google and Apple have been restricting third-parties' access to such interoperable data.

---

[1] See paras 286 to 287 at Appendix G of the CMA online platforms and digital advertising market study (1 July 2020) https://assets.publishing.service.gov.uk/media/5fe49554e90e0711ffe07d05/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential_WEB.pdf and paras 64 *et seq.* at Appendix F at https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_-_role_of_data_in_digital_advertising_v.4_WEB.pdf

Other sources of Google's and Apple's market power

In addition to monetisation through digital advertising, there are other sources of market power that we urge the CMA to take into account as part of its investigation. Such sources include Google and Apple's bundling of payments, authentication, fraud prevention, and adjacent services into the web browser. Further detail on this is included in our first response to the Issues Statement, attached as Annex 1 to this letter.

Impact of Google and Apple's interference with web interoperability on mobile browsers

Google and Apple have taken a series of connected steps to restrict web interoperability and discriminate against rivals. These changes in the web are also relevant to mobile browsers: if you do not have an open and interoperable web, then any remedy in the mobile browser is rendered ineffective.

A brief summary of Google's changes in the browser (Chrome) is as follows:
   (a) **Cookie storage** – Google imposed a default requirement on websites to attribute in the website code on 'SameSite' cookies.[2] This has the effect of disabling third-party cookies which do not specify the attribute.[3]
   (b) **Open Web Data and Cookie storage** – In August 2019,[4] Google announced its Privacy Sandbox changes.[5] Privacy Sandbox has offered more than 30 proposals to date (including a plan to eliminate rivals' ability to use cookies, and other Open Web data sources).
   (c) **Open Web Data, User Agent String (a line of code that identifies the browser, version of the browser, model and type of device and operating system it is running on)** – In October 2022,[6] Google started to block access to the User Agent String of data.[7] Google is offering an impaired alternative, 'User Agent Client Hints', which instead offers users a higher latency product and, in time, will remove the web data when "Privacy Budget"[8] or its equivalent is implemented.
   (d) **Open Web Data, URLs** – Since November 2023, Google has begun testing the interference with the practice of browser storage via its Bounce Tracking implementation. Both Google and Apple via the W3C have contemplated changes to URL links. In Google's case, Google refers to this as "link decoration" when *its* Ad Systems rely on this, but "bounce tracking" when *rivals'* ad solutions rely on this real-time communication mechanism.[9]
   (e) **Cookie storage** - Since September 2022, Google has partitioned persistent storage, further degrading open web interoperable data, as websites are unable to practically share data.[10]

---

[2] https://blog.chromium.org/2019/05/improving-privacy-and-security-on-web.html
[3] ███
███████████████████████

[4] https://blog.google/products/chrome/building-a-more-private-web/
[5] https://developers.google.com/privacy-sandbox/overview
[6] https://developers.google.com/privacy-sandbox/blog/user-agent-reduction-oct-2022-updates
[7] https://chrome-developer.pages.dev/en/articles/user-agent-client-hints/#:~:text=User-Agent%20Client%20Hints%20have%20been%20default,enabled%20in%20Chrome%20since%20version%2089. ████████████████

[8] MOW notes that Google has announced that Privacy Budget is no longer an active Privacy Sandbox proposal (see para 104 in the CMA Privacy Sandbox Q4 2023 report at https://assets.publishing.service.gov.uk/media/65ba2a504ec51d000dc9f1f5/CMA_Q4_2023_update_report_on_implementation_of_the_Privacy_Sandbox_commitments_PDFA_1.pdf). However, MOW understands that such proposal stands high chance of being reintroduced by Google.
[9] ██
[10] https://developers.google.com/privacy-sandbox/blog/chips-origin-trial; ███████████████████████████
██████████

Google is intending to fully deprecate the use of third-party cookies from Q3 2024.[11] Apple, via the W3C, have already implemented similar impairments.

(f) **IP Address (akin to a residential address) helps marketers improve the effectiveness of their ad spends** – Google is currently developing a proxy server and has been masking IP addresses. In doing so, it impairs the ability of rivals to understand the address from which an internet-connect device is requesting content from a publishers' server – a critical component used in fraud detection, localization of content, intellectual property protection, and security.[12] Apple has already implemented private relay within its products to similar effect.

(g) **Google's shifting of functionality into the browser** – Google's response to the removal of web data availability and functionality to third parties has been the introduction of its own alternative products in the browser. Google's own website states:

> "*The Privacy Sandbox APIs require web browsers to take on a new role. Rather than working with limited tools and protections, the APIs allow a user's browser to act on the user's behalf—locally, on their device—to protect* **the user's identifying information** *as they navigate the web. This is a shift in direction for browsers. The Privacy Sandbox's vision of the future has browsers providing specific tools to satisfy specific use cases, while preserving user privacy.*"[13]

It is important to note Google has never justified why its collection and processing of Personal Data, such as using specific individual's identity as a match key within its Customer Match, or any other Privacy Sandbox business-facing solution (e.g., its "Topics" cross-site behavioural attributes or cross-site Attribution APIs), is an improvement to "privacy."

Digital ad functionalities: Google moving ad functionality to the browser, such as via Protected Audience API ("PAAPI") (previously known as FLEDGE and TURTLEDOVE) and Topics API. PAAPI enables "on-device auctions by the browser". It has been implemented and is actively being used. What used to take place as server-to-server communication between buyers and sellers of ad inventory will now take place in the browser and in server-side processing controlled by Google. Accordingly, all the risks to individuals identified by Google are not prevented by Google's current designs. The only safeguard to individuals that Google's proposals rely upon is "trust us."

A brief summary of Apple's changes in the browser (Safari) is as follows:
(a) **Cookie storage** – Intelligent Tracking Prevention (ITP) was introduced to Apple's browser, Safari, as a series of features that it claims were to reduce cross-domain data transfers. [14]
(b) **IP Address** – Apple released Private Relay in 2021 as a feature that masks IP addresses.

The CMA should carefully review Google's and Apple's ongoing interference with interoperability and the actions currently being taken which, if not restrained, threaten to prevent any effective remedy from being implemented. For example, Google and Apple's ability to shift functionality between the browser and operating system at their own will.

---

[11] See Google's timeline at https://privacysandbox.com/open-web/#the-privacy-sandbox-timeline versus the CMA's timeline in their Q4 2023 report at para. 113 https://assets.publishing.service.gov.uk/media/65ba2a504ec51d000dc9f1f5/CMA_Q4_2023_update_report_on_implementation_of_the_Privacy_Sandbox_commitments_PDFA_1.pdf
[12] See "In Development" at https://privacysandbox.com/open-web/#the-privacy-sandbox-timeline; ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮
▮▮
[13]https://developers.google.com/privacy-sandbox/overview#:~:text=The%20Privacy%20Sandbox%20APIs%20require,cases%2C%20while%20preserving%20user%20privacy.
[14]See a detailed explanation of each release of ITP at https://www.simoahava.com/analytics/itp-2-1-and-web-analytics/

Changes in the browser are leading businesses to operate in the operating system

The CMA highlights in the Issues Statement (para. 18) that businesses bear the higher costs of native apps due to the inherent bugs in Apple's WebKit. This is further true because of the above-mentioned changes to the browser. With the removal of third party cookies and the ability to effectively monetise across the web, publishers have moved towards developing apps and are being pushed into the mobile operating ecosystem. Google and Apple are the primary mobile browser providers and have benefited substantially from the influx of publishers into the mobile operating ecosystem, with increased access to sign-in data and first party data (see further in our first submission at Annex 1).

We refer also to the Texas-led State Attorneys' General evidence that Google's motive for Privacy Sandbox was to put a wall around the open web, hence enabling Google (and Apple who are working in parallel under the same strategy) to impose app-store rules on all rival media owners and the rival business solution providers that support this competition across digital markets.

The links between the browser and the operating system

The CMA highlights that, as well as holding market power in mobile browsers (para. 24), Google and Apple also have "substantial and entrenched market power in the supply of mobile operating systems" (para. 25). The CMA is thus planning to investigate whether Google and Apple are using their positions to "weaken competition in the 'downstream' supply of mobile browsers and browser engines, and the distribution of cloud gaming services" (para. 25).

Given Google and Apple's market power in these two areas, their entire business model should be examined. As businesses move towards building native apps in the operating system, Google and Apple have also increasingly restricted third-parties from accessing data available within the operating system for third parties to be able to monetise their content. The removal of ID for Advertisers (IDFA) in iOS and Android Advertising ID in Android is akin to the removal of third party cookie storage, but in the mobile browser instead of the open web. Publishers and software or game developers are consequently deprived of cross-app data to effectively monetise their ad inventory.

Native apps also incur a surcharge for in-app purchases, leading to higher revenues for Google and Apple. Google and Apple also benefit from insight into native apps' development and updates via their respective App Stores.

We trust that the above is useful and we are at the CMA's disposal should the CMA have any questions regarding our comments.

Yours faithfully,

Preiskel & Co LLP

Annex 1: MOW's response to Mobile Browsers and Cloud Gaming Issues Statement dated 20 January 2023

PREISKEL & CO

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

For the attention of:
browsersandcloud@cma.gov.uk
██████████████████████████

By email only

20 January 2023

Dear Sirs,

Re: Response to Mobile Browsers and Cloud Gaming Issues Statement

This letter is on behalf of the Movement for an Open Web ("MOW"), a not-for-profit organisation that is seeking to secure an open and decentralised web.

We write in response to the Issues Statement. We aim to highlight ten key points:

1) Consistency with recent CMA precedent and ensuring interoperability.

The CMA found in its Privacy Sandbox case[1] that "transferring key functions" from the Open Web into the browser centralises functions into the hands of the owners of those browsers. Many functions currently exist in decentralised websites that could be centralised into the browser with an attendant loss of competition and local functionality. Key functions that are currently enabled by the HTTP standard and which are at risk of centralisation into the browser include:

-   Sign-in (see further discussion on Sign-in and Authentication below).
-   Access to data sources such as IP addresses, User Agent information, URLs and hyperlinks.
-   Expansion of the definition of the browser to include authentication, password management, digital wallets, payment functions, website blockers (overriding parental or bill-payer agreements with internet service providers over such things such as parental controls), beyond a browser's core functions of page rendering, bookmark management, and download management. An early step on the next stage of the investigation needs to be to define what is, and what is not, the core functionality of a browser absent further abuse and additional bundling.

The investigation will look at browsers and app store bundling but also needs to carefully consider the technical capability of web functions to be re-bundled and centralised in the browser. This is important

---

[1] Para 3.3(b) of the CMA Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals.

with reference to bypassing remedies contemplated for enabling the web apps and app payment unbundling.

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 it exists at all.

2) Web compatibility

We are concerned that the assumption being made as a basis for current remedies is that web interoperability will underpin the functionality of web apps with consumer devices and the browsers therein. Since browser owners can define compatibility and many techniques are available to create incompatibility, the risk is that they will make their browsers incompatible with web apps or limit equivalent quality of experience or quality of service to end users.

If the potential solution is interoperability over the World Wide Web, with compatibility being based on stable and impartial web standards, such as HTTP, then our view is that current web standards are not stable, that web standards making is not impartial, and there is a lack of "unrestricted participation" in their development. Indeed, there is considerable evidence of the dominance of Google and Apple in the development of web standards to and for their own benefit. Any remedy relying on web interoperability is thus at risk of being ineffective.

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[2]).

However, 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 between the browser and the Open Web.

Importantly, Apple may decide not to compete with Google, as it has in relation to search. Instead of competing in search, Apple has demanded that Google pay to place its search engine on Apple's iPhones and other devices. Google is reportedly paying over $1bn a month.[3] A similar commercial solution may appeal to Apple. It could demand that Google's placement of Chromium/Blink browsers on its iPhones and other devices should be accompanied by a similar payment. Competition would suffer and Apple would increase its profits.

Expecting Apple to improve Webkit and its compatibility with websites on the Open Web when faced with competition from Google's Chromium/Blink-based browsers ignores the economic symbiosis between the two companies that currently exists. Given the considerable costs that would otherwise be faced by Apple in upgrading and improving its own browser in ensuring browser/web compatibility,[4] there is an appreciable risk that Apple could instead decide to close its Safari/Webkit engine and use Google's Chromium/Blink, either with a "Chrome UI" or its own new UI.

---

[2] As was found to be the case in *Microsoft Corp v Commission of the European Communities*, Case T-201/04.
[3] See ACCC reports and *USA vs Google*.
[4] And bearing in mind that businesses as technologically sophisticated and 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".

To avoid this poor outcome for competition, it is necessary to ensure that entrants and smaller players can expand, decreasing the incentive for Apple to simply not offer the product.

It is vital when considering remedies to competition cases that existing business models provide indicators of economic interest. Those interests can be amplified with remedies, but no remedy can require supply and the offering of a product when a business decides not to offer one.

3) Simplifying switching between browsers and limiting default/preinstalled browsers

Provided the above risk of Apple not supplying its own browser and switching to Google's browser, we would support the CMA's inclusion of requirements to make switching between browsers more straightforward in the Issues Statement.[5] This was proposed in the Mobile Ecosystems Market Study Final Report ("Final Report") at para 8.139.

A further risk is reduced choice and increased friction.[6] We consider that all preinstallation and defaults identified as creating anticompetitive effects must be subject to neutral user choice architecture and choice screens. We understand the CMA's inclusion of "choice screens to overcome distortive effects of pre-installation"[7] as a remedial action, but one that needs to be tested and trialled for effectiveness before being implemented.

4) Increasing competition between mobile browsers

We agree with the CMA's proposed remedies for increasing competition between mobile browsers.[8]

This runs in parallel with the following remedy proposed by the CMA, namely the requirement of Apple and Google to provide greater access to functionality for rival browsers by exploring the following options:

(a) *"requiring equality of API/functionality access, whereby the controller of the operating system is not allowed to withhold access to device functionality exclusively for their own browser; and*
(b) *requiring Apple and Google to open up access to specific operating system functionality, other than the functionality they make available to their own browser and native apps."*

We consider it to be a necessity to require Apple and Google to allow other competing (i.e., non-Apple or Google) Browser User Interfaces ("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.

5) The definition of browser functionality

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 in the browser may override choices that consumers may wish to make when accessing individual websites. Under GDPR and UK law the issue of compliance is for each business owner and decisions concerning their business, how

---

[5] Issues Statement, paras 69-71.
[6] At para 8.141 of the Final Report, the CMA added that these changes would allow users to make effective choices by reducing friction. Furthermore, the CMA acknowledged that the choice architecture within Apple's and Google's respective ecosystems may lead to self-preferencing. This is particularly true through default browsers/preinstalled browsers.
[7] Issues Statement, paras 72-74.
[8] Issues Statement, para 63.

data is processed and how compliance is ensured. It is not for Google and Apple to act as the world's privacy police, particularly when they have frequently been found to themselves breach privacy law and stand to gain considerable commercial benefit from blocking rivals using privacy as an excuse.

Also, and importantly, privacy does not need to be only a browser function. Privacy can otherwise also be addressed through 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.

Seeing privacy as solely being a browser function risks limiting competition by entrenching the internet gatekeeper Browser UI or the browser engine as the supplier for all. Instead, technical access and interoperability to currently existing browser interfaces should be required, but narrowly defined, so that interoperability is only related to core browser functionality and innovation can then take place in other features, functions and apps, including on privacy compliance by rivals.

Steps need to be taken to prevent an increase in the incentive for the internet gatekeepers to expand the functionality of their browsers to interfere with existing data and functions currently available on the web to consumer's detriment.

For example, enabling access to web apps and unbundling payments from in-App Store apps, would be critically dependent on the open and seamless functioning of web apps. To guarantee such functionality would require the open web apps to have access to current transport level data and depend on standards being developed and applied on an unrestricted basis. The current system for developing web standards is unlikely to be satisfactory, given that it has become captured by the main technology platforms.

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 by browser owners. 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. The recent Web Payments API standard allows them to embed digital wallets into the browser, centralising those functions for their own competitive benefit.

As browser owners, Apple and Google can use their browsers to interfere with existing contracts and functions for sign-in to independent websites.[9] They control important architectural design points in APIs, which should be designed to enable competition and not to foreclose it.

Any browser investigation and any applicable interoperability remedy thus both need to define the boundary of the browser's functions and enable third-party developments and innovation. The obligations covering access and interoperability need to apply to all technical inputs, commercial inputs and financial inputs; not outputs as determined by each of the internet gatekeeper browser owners.[10]

---

[9] 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).
[10] Or gatekeepers as defined in the 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.

6) <u>Unbundling of Authentication (Sign-in)</u>

The function of Sign-in is one of the main sources of market power for Google and Apple. As discussed in Annex Z of the CMA's Online Platforms and Digital Advertising Market Study Report, control over end user data is central to the ability of both platforms to manage their ecosystems effectively. We therefore consider that authentication and sign-in systems need to be available to competing offerings (apps) and competing websites should be included in the MIR.

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 suggest 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 data for hyper-targeted advertising to make more money on its own digital properties.[11]

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). Apple has recently been fined in France for its breach of data protection laws in relation to its ATT product and Google has been fined on multiple occasions for such breach. The disincentive of data protection fines is insignificant and immaterial for Apple and Google limited as it is to fines that are not based on stripping infringers of the profits gained from wrongdoing. As such they are unlikely to change established and very profitable behaviour.

Both Apple and Google also ignore the fact that GDPR applies to all companies and the scheme of the law is to place the obligation for compliance on each in relation to the data that they process. A "One Size Fits All" solution is thus no solution at all.

A competitively neutral remedy would be to allow a competing third party to handle data, provided that it does so responsibly, in accordance with GDPR. This access is crucial if there is to be an ad-funded free web offering at the point of use by consumers. To achieve this, unbundling of authentication for web use from signing into Google or Apple's platforms is thus also likely to be needed. We outline the current position in figure 1 below:


---
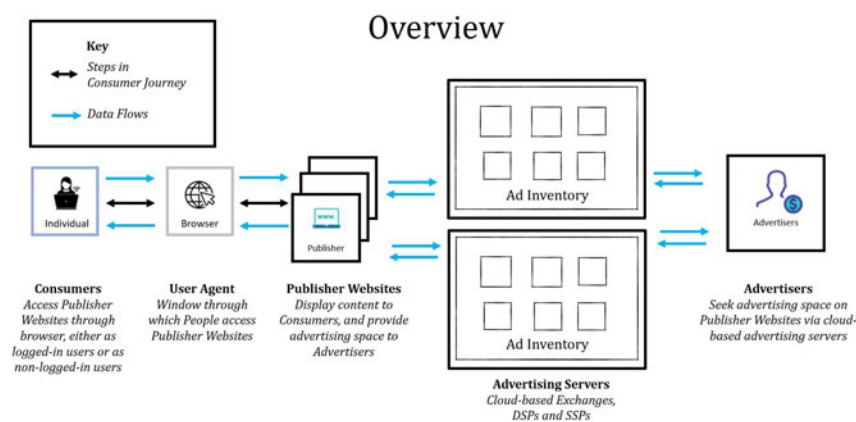
[11] This may be why it exempts all its own properties, as well as other large organisations that operate multiple domains (e.g., via First Party Sets) from its standard interference with interoperable data transfers.
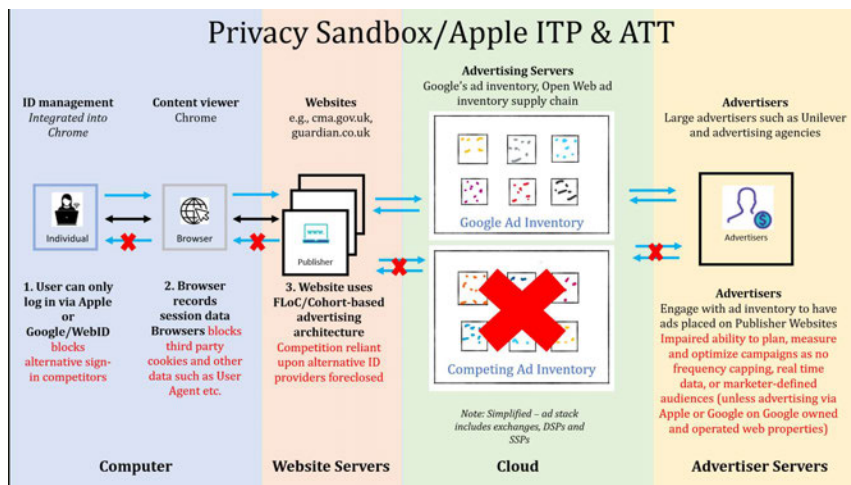
The overview in figure 1 illustrates how Sign-in is used to take end user data, and the data flows that then follow in the advertising supply chains. We outline in figure 2 the current user journey (logged in):
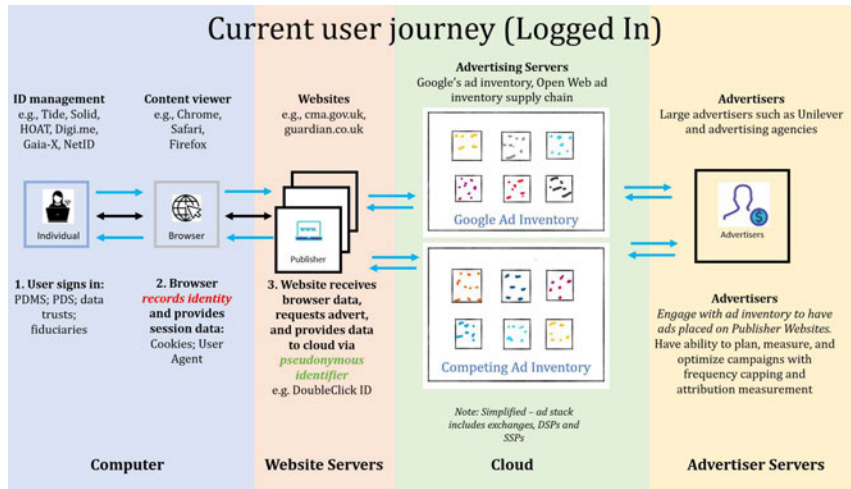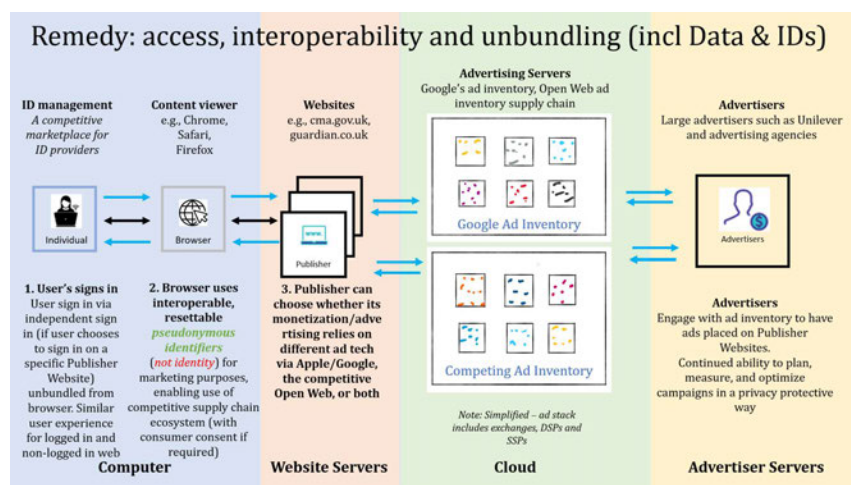

And in figure 3 the user journey (not logged in):
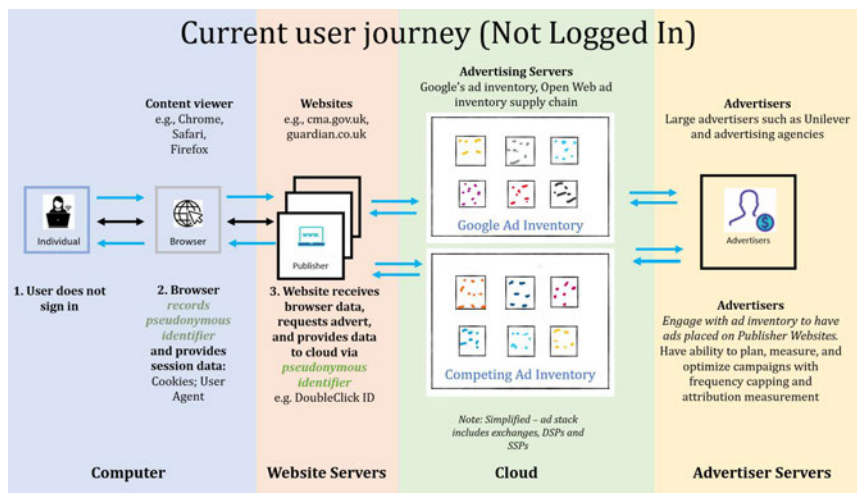
In figure 4 we illustrate the actions being taken by Google and Apple and how they impact third parties:

6

In figure 5 we outline how a remedy to unbundle data from the Sign-in system at the browser level would enable greater competition:

7) Revenue sharing agreements

We welcome the CMA's commitment to address the impact of revenue sharing agreements between Google and Apple:

> "*These remedies would aim to generate competition between mobile browsers on iOS devices by addressing the possible impact of revenue sharing agreements to the extent that these dampen competition between mobile browsers.*"[12]

As described above these agreements affect competitive incentives. We consider managed withdrawal from such arrangements to be necessary if disruption and the provision of free internet services is not also 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.

8) Apple and Google's restrictions on cloud gaming providers

We support the CMA's proposed remedy which requires Apple to remove its App Store restrictions on cloud gaming services.[13] We consider Apple's practices and guidelines to be furthering its commercial interests at the expense of creating a more competitive market.[14] The most restrictive provision which heavily impedes access for cloud gaming providers to the App Store is found at paragraph 4.9 on streaming games. Subsection 4.9.1 states the following:

> "***Each streaming game must be submitted to the App Store as an individual app*** *so that it has an App Store product page, appears in charts and search, has user ratings and review, can be managed with ScreenTime and other parental control apps, appears on the user's device, etc.*"
> (emphasis added)

And subsection 4.9.2 also states the following:

> "*Streaming game services may offer a catalog app on the App Store to help users sign up for the service and find the games on the App Store, provided that the app adheres to all guidelines, including offering users the option to pay for a subscription with in-app purchase and use Sign in with Apple. **All the games included in the catalog app must link to an individual App Store product page.***" (emphasis added)

This provision essentially requires that each game must be individually submitted to the App Store, thus, must be individually downloaded to the user's device which requires storage. This limits the storage as well as the processing capacity benefits which are derived from cloud gaming by making users more hardware dependent than is usually the case with cloud gaming.

Furthermore, paragraph 4.9. states the following:

> "*Streaming games are permitted so long as they adhere to all guidelines – for example, each game must be submitted for review, developers must provide appropriate metadata for search, **games must use in-app purchase to unlock features or functionality**, etc. Of course, there is always the open Internet and web browser apps to reach all users outside of the App Store.*" (emphasis added)

It has been found that this can have a competitive impact by being: "*problematic for cloud gaming services, since it means that games need to be coded separately to be accessible via a native app, whereas the benefit of cloud gaming is the opposite: the game only needs to be coded once and is then available across platforms.*"[15]

Competitive advantages include technical preference. For example, higher latency which was raised by Tim Sweeney, CEO of Epic Games, in Epic Games' lawsuit against Apple,[16] a position which the CMA subsequently agreed with in its Final Report holding that web apps are not functionally equivalent to native apps.[17] The CMA has also raised a number of additional drawbacks to relying on web apps instead of native apps including poorer discoverability and engagement, alongside inferior features and functionality.[18]

It is easy to decipher Apple's rationale for restricting access to cloud gaming services. As was pointed out by Geradin and Huijts, cloud gaming apps contain a catalogue of games akin to that of the App Store, which could lessen users' reliance on the App Store if cloud gaming continues to grow in prominence. If the growth of cloud gaming is sustained, it could introduce greater price competition and potentially erode Apple's 30 percent commission on in-app purchases.

The CMA finds that Apple has a growing advertising business and has sought to interfere with and limit apps from providing competing advertising services. This both helps to boost its own ads business and

---

[15] Geradin, Damien and Huijts, Stijn, Dark Clouds Gather – An Analysis of Apple and Google's Restrictions on Cloud Gaming (September 15, 2022), https://ssrn.com/abstract=4219715 at p. 12.
[16] Testimony given at trial in Epic v. Apple, N.D. Cal., 3 May 2021, p. 138.
[17] Final Report, paras 4.129-4.132.
[18] Final Report, Appendix I, para 22.

"encourages" apps to switch to subscription-based offerings where possible.[19]

If the current restrictions are eradicated carefully, it may have the impact of incentivising Apple to invest and innovate on the merits of its products and services rather than as a result of restrictive and anti-competitive practices.

9) Google Play Store's restrictions

At present, the Issues Document excludes any mention to the Google Play Store. While native cloud gaming apps have been able to launch on Google Android, users on Google Play Store are not able to complete in-game purchases in the app which effectively eliminates a significant source of revenue for cloud gaming providers. We therefore ask the CMA to more closely scrutinise Google's policies for cloud gaming as part of this investigation.

10) Apple's strategic 'privacy fixing'

In 2018, Apple released SKAdNetwork (SKAN), a tool to replace mobile measurement platforms (MNP), designed to enable apps to measure the effectiveness of their advertising. The reports offered by SKAN, however, are far less useful than those offered by MNP and have undermined advertisers' ability to determine the most effective allocation of advertising spend.

Apple's SKAN attribution tracks events across apps controlled by different developers (i.e., third parties to Apple, but first-parties to a consumer). So, if the user sees an ad on the Facebook app and on Apple's News+ app on an iPhone, Apple collects this user information, whilst preventing Meta from doing the same, despite the fact that in this case Apple is a third-party to the Facebook app.

SKAN restricts multi-touch attribution, which previously allowed an advertiser who spent, for instance, 25% of their budget buying ad space on Facebook and Google and 50% on the Open Web, to see that 75% of their clicks and attribution came from the Open Web and the rest from Facebook and Google. This disincentivises advertisers from attributing their advertising spend to 'third-party' advertising and to use, instead, Apple Search Ads.

Furthermore, as was highlighted in a recent webinar on 'Mobile Game Marketing with SKAN 4.0',[20] the marketing measurement mechanism employed by SKAN 4.0 has stark consequences for smaller advertisers. SKAN 4.0 returns two types of conversion values - coarse-grained and fine-grained. The fine-grained conversion value is returned when the privacy threshold is met. Apple basically argues that to ensure anonymity, they limit trackable information being sent back to the advertiser when the install count is low. When the install count increases, more data is returned to the advertisers. From tests, large campaigns using SKAN 4.0 are much more effective. This gives larger advertisers an advantage and encourages smaller ones to spend more money on their campaigns.

App Tracking Transparency (ATT), likewise, undermines the potential advertising revenue of third-party apps. ATT requires app developers to secure user permission to track data across other apps or

---

[19] See Harming Competition and Consumers under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates by D. Daniel Sokol, Feng Zhu :: SSRN.
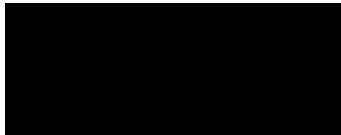[20] See Mobile Game Marketing with SKAN 4.0: How to boost your iOS campaigns - Splash (splashthat.com).

services, whilst Apple collects cross-site data for the purpose of personalised advertising by default. This is both clearly anticompetitive and violates consent requirements under GDPR.

In short, Apple has reduced the capacity of app developers to advertise on iOS devices, increasing its own access to multi-site data for attribution and interest-based advertising. MOW suggests that this forms part of a deliberate strategy to not only increase Apple's revenue from ads but to force more developers into subscription models, where Apple can also extract their excessive rent. We would similarly contend that Apple's cuts to Safari's budget, which has led to a sharp downgrade in the browser's quality, represents a concerted effort to substitute web applications for mobile applications as the de facto user choice. By increasing user dependence on mobile apps, Apple increases the volume of activity which carries its 30 percent tax.

We trust that the above is useful and we are at the CMA's disposal should the CMA have any questions regarding our comments.

Yours faithfully,

Preiskel & Co LLP