PREISKEL & CO

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

t [redacted]
e [redacted]
www.preiskel.com

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

By email only
mobilesms@cma.gov.uk

Our Ref: TC/ADM838
12 February 2025

Dear Sirs,

Re: Movement for an Open Web submission on the CMA's SMS investigation into Google's and Apple's mobile ecosystems

We write on behalf of the Movement for an Open Web ("**MOW**"). We are writing in response to the CMA's Invitation to Comment dated 23 January 2025[1] ("**ITC**") regarding its investigation into Google's strategic market status ("**SMS**") in Google's[2] and Apple's[3] mobile ecosystems ("**Investigation**).

We welcome the CMA's investigation and provide specific comments below. However, as the CMA notes in the ITC, the Investigation is subsequent to previous CMA investigations conducted under the Enterprise Act 2002 ("**EA02**") and thus, much of Google's and Apple's conduct as part of the Investigation will be a repetition of the previous findings.

The evidence gathered through the substantial efforts of the CMA in the mobile ecosystems market study and the mobile browsers investigation should be taken into account in the Investigation (as per para 2.65 of the CMA Guidance on the DMCCA) and in particular, any findings of fact need not be re-established as part of the new Investigation.

The CMA is due to reach a final decision as part of the mobile browsers investigation by 16 March 2025. Under the EA02, the CMA is under a duty to remedy adverse effects and take such action that it considers to be "reasonable and practicable" (s.138 EA02) within 6 months of the report (s.238A EA02) (by September 2025). We note that the DMCCA provides more powers for the CMA but any remedies contemplated now under the DMCCA would not come into force until 2026 or 2027.

We therefore urge that the CMA needs to take swift action and demonstrate its effectiveness in supporting competition and growth by addressing competitive restrictions with remedies now. Specifically:

1) Illegal revenue sharing deals. The CMA provisionally found that the Information Services Agreement between Google and Apple reduced competition.[4] These can be declared to be illegal so that Google's anti-competitive revenue sharing and default setting agreements with

[1] https://assets.publishing.service.gov.uk/media/679115f1cf977e4bf9a2f1a0/Invitation_to_comment.pdf
[2] https://www.gov.uk/cma-cases/sms-investigation-into-googles-mobile-ecosystem
[3] https://www.gov.uk/cma-cases/sms-investigation-into-apples-mobile-ecosystem
[4] See CMA Provisional Decision Report, para 9.73 onwards and Remedy 4 in the Provisional Decision findings

Apple and others would be invalid and unenforceable, enabling the parties to them to operate without competitive constraint. Overnight change to the market is unlikely, but it can be expected that the considerable financial rewards Google has been paying out to prevent competition would cease and innovation and competition would emerge rapidly.

Remedies also need to be considered while investigating harms so that evidence can be gathered that support remedies that are suitable to address the issues identified.

CMA Specific Questions

Q1: Do you have any views on the scope of our investigations and descriptions of Google and Apple's mobile ecosystem digital activities?

1. MOW welcomes the CMA's grouping of the digital activities under section 3(3) of the DMCCA. Google and Apple's mobile ecosystems as a single digital activity are well defined as the activity that Google and Apple respectively controls and have SMS status within – the provision of a mobile ecosystem to users. Through the operating system (Google's Android or Apple's iOS) and the browser (Google's Chrome and Apple's Safari), they are able to operate the mobile browser and native apps via the Google Play store like the owner of a shopping or sports centre. The shopping centre owns the building and hosts the different shops (the mobile ecosystem), whereas the different shops (publisher websites and/or native apps) exist within their own distinct markets (food, retail, travel, etc.).

2. As part of the ecosystem, Google and Apple regularly urge users to sign in, and thus to accept their terms and conditions. These terms and conditions allow Google and Apple to collect information regarding the activity across all the services provided by Google and Apple and by Google and Apple as distributors of competitors products and services. In effect user interactions with the platform owners are controlled by the platform owners and content or apps accessed via the platforms do not control or get access to user interaction data. Where the economy generally is data dependent, the digital economy is more so, which has become channelled through end use of devices. Mobile browsers and mobile devices are the province of Google and Apple. Consumer interactions with rival services access via OS/browser software products and physical devices provide what Google calls "the Magic of Google"[5] from which customer needs and their purchasing intent can be understood. The information about those needs is vital for all online businesses (for example to understand consumer preferences and hence innovate) but is presently being controlled by Apple and Google. Google and Apple's access to such data within the mobile operating system reinforces the fact that this is one single ecosystem.

3. Google and Apple's data dominance is reinforced by the Information Services Agreement (as mentioned above):

   (a) It is a horizontal agreement between two competitors (both are browser and other mobile ecosystem owners).
   (b) It includes an exclusive arrangement of Apple supplying data only to Google and no Google publishing competitors in exchange for a percentage share of ads revenue.

[5] See USA v Google (Search) [2020] Trial Exhibit "Google is magical" at https://www.justice.gov/d9/2023-09/416665.pdf

(c) Under the Information Services Agreement Google restricts Apple's ability to innovate in its browser. The browser is the window on the web, so by limiting what users can see through the browser the agreement limits the ability for developers to put ads on Apple devices that Apple users can see. This restriction on the function of Apple is explicit in the Agreement as a browser is a search access point.

(d) Apple gets a revenue share from Google Search meaning it has an incentive to help Apple undermine Display advertising in favour of Search advertising. Apple is also disincentivised (effectively, restricted) from building its own search engine, and thus, excludes Apple's ability to compete with Google in search text ads (market, as found by Judge Mehta). Apple also has no incentive to compete with Google in Display ads or allow its App developers to use Display ads to compete with Search. This reinforces Google's Display ad empire, shifts advertising from Display to Search and steers companies to increasingly use apps to reach consumers (whose install relies on paid acquisition via Search)[6].

(e) Apple restricts third party access to interoperable data through ITP and ATT (see further on this below). Moreover, Apple exempts Google's apps for displaying the anticompetitive ATT screens, which contain dark patterns, and such conduct further steers consumers to the better install process for Google apps over those of rivals.

(f) For example, see Google's negotiation of a new term in the 2016 agreement, where Apple's implementation of the Safari default must "remain substantially similar" to prior implementations (para 305 of Judge Mehta's opinion). This reinforces Google's dominance in its browser distribution and access to search volumes. More importantly it harms those who would use Display ads in iOS or Safari, which then steers businesses into Apple's apps store to fund their businesses.

Q2: Do you have any submissions or evidence related to the avenues of investigation set out in paragraph 70-72? Are there other issues we should take into account, and if so why?

4. As mentioned in our prior filings to the CMA's other investigations into Google and Apple[7] and related to the above, Google and Apple's coordination operates in a way that interferes with other competitors' freedom to operate on the web. This adds to the competitive restraint faced by rivals in sustaining their business through ad revenue.

   (a) The State Attorneys General vs Google (Texas) Ad Tech case discloses evidence that the CMA should see about how Google and Apple coordinated to use privacy as a misleading shield and pretext for their anti-competitive actions. Their lack of support for local storage, such as cookies, means that rival publishers' ability to monetize the ad inventory across their properties has been and is being impaired.

   (b) At the same time, Google and Apple initially provided to the open web and then more recently withdrew a common match key via the operating system (i.e. the Mobile Advertising ID or MAID). This is anticompetitive conduct of a type that was found to be an abuse of dominance in the EU case against Microsoft. This conduct had the effect of shifting rival publishers from interacting with visitors to their property on mobile browsers (which as the CMA has found

[6] If Apple gets a rev share for distributing Chrome (say X%), but gets a higher rev share from Google Search (say Y%) conducted via Siri and Safari (which we believe to be true), then there is no disincentive to build Safari at that time, but there may be a disincentive over time and AND there is a disincentive to allow advertisers access to Display advertising (powered by cookies) as to reach iOS / Safari consumers, they must shift advertising spend to Search (+app stores).

[7] For example, correspondence dated 18 July 2024, 23 July 2024 to the CMA Mobile Browsers and Cloud investigation team, which outline a list of events that took place in the World Wide Web Consortium ("W3C"), which work in Google and Apple's favour (including the standard of payment via digital wallets in the browser)

monetize at less than 50% without access to a common match key) to prompt visitors to interact with the identical B2C service via an app (which Google and Apple each provided a MAID).

(c) Once the migration from open web standards to proprietary APIs via apps was sufficiently large, both Apple and Google began to interfere with rival B2B supply chain partners' ability to monetize these publishers' ad inventory with MAIDs (e.g., Apple's ATT and Google's Sandbox (see further under para. 6 below)). This joint conduct has restricted innovation and competition in mobile ecosystems.

5. Relating to the forward-looking remedies, we suggest the following:

(a) Labelling[8] of local storage by data controllers as to whether it will or will not contain Personal Data. When the interoperable match keys in the local storage have the appropriate protections to prohibit reidentification by recipients, then the contents are deidentified which as the ICO has stated in their guidance is a desirable data protection measure.

(b) Labelling of media owners' content as to whether it contains sensitive category information. Such labelling can support user-controlled alerts and warnings that individuals wish to flag as they navigate across web properties.

(c) Google and Apple must not use consumer interactions with rival publisher properties content to train their AI models, or if such information is collected it must be made available to rival AI software organizations on an equivalent basis (see under para. 9 below).

Q4: Which potential interventions should the CMA focus on in mobile ecosystems? Please identify any concerns relating to Apple's or Google's mobile ecosystems, together with evidence of the scale and/or likelihood of the harms to your business; or to consumers.

6. Both Google and Apple have restricted third-party use of cookies in the browser. The CMA should ensure to investigate these actions, as they foreclose third parties' ability to generate ad revenue.

(a) Third Party Cookies are small storage files. They are a widely deployed and vital part of online publishing. They enable ads to be matched with publishers' available inventory. As accepted by the CMA in its seminal 2020 Report, they are essential to programmatic exchanges which match demand and supply through cookie syncing[9] via ad exchanges. This brings higher revenue for publishers, by allowing programmatic exchanges to source the highest value possible for them based on the data available within milliseconds.

(b) Apple released Intelligent Tracking Prevention (ITP) in Safari from 2017. There have been numerous versions of ITP, which limits services providers from reading cookies from a website (limits "first-party" cookies and blocks "third-party" cookies altogether). Third-party cookies do not need to rely on identifiers that are associated with an individual's identity. However, through ITP, Apple has blocked all third-party cookies regardless of the anonymity of the data that they provide. It is important to note that Apple indirectly benefitted from Google's Search revenue that was miraculously "*immune*" from Apple's ITP changes (as noted by the CMA[10]).

---

[8] MOW has provided details of the labelling solution to the CMA in its other investigations. MOW welcomes the opportunity to outline details to the CMA as part of this investigation in due course.

[9] See CMA Digital advertising market study, appendix H and in particular, para. 97 at https://assets.publishing.service.gov.uk/media/5dfa172240f0b6217b108351/Appendix_H2.pdf

[10] 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

(c) Google subsequently released its Privacy Sandbox changes to its Chrome browser from its announcement in 2019, which is subject to a separate CMA investigation procedure. However, these changes should also be included within scope of the possible interventions under the DMCCA. This added to the cascade of previous steps made by Google, which restricted rivals (see Appendix 1).

(d) Digital advertising revenues for publishers using the Safari browser fell by approximately 60%.[11]

(e) Google research showed that by disabling access to third-party cookies, average revenue for the top 500 global publishers would decrease by 52% and for the median publisher by 64%.[12] It states that some publishers lost over 75% of their revenue. This was supported by the CMA in its online platforms market study final report, which stated "*that UK publishers earned around 70% less revenue overall when they were unable to use third party cookies to sell personalised advertising but competed against others who could.*"[13] This will be used as a benchmark to estimate the harm from ITP.

7. Similarly, Google and Apple have restricted third-party use of the mobile operating system ID (Android Advertising ID in Android (AAID) and ID For Advertisers in iOS (IDFA)).

(a) Apple released the App Tracking Transparency (ATT) prompt in 2021. It required rival apps only (excluding Google[14]), which implement "*tracking*" (as defined by Apple)[15], to use a 'pop-up' consent request, ATT. If the user reacts to the pop up and opts out, app publishers are restricted from the IDFA and are unable to effectively target or attribute ads. This reduces an app's ability to attribute a sale to prior ad impressions and will have reduced the value of ads that can be sold by publishers.

(b) Apple does not subject itself or even Google's apps to the same restrictions. The ATT prompt only appears for third parties' apps and Apple's definition of "*tracking*" purposefully does not capture Apple's combining of data across its own group's apps or its collection of consumer interactions across rival publihers' apps (see SKAN), but only if such combination of data is done between two rival entities' apps.[16]

(c) It is estimated that following the introduction of ATT, there is now a 65% opt-out rate[17] meaning an estimated drop of 65% of data supplied for app publishers.[18]As a result, platforms must revert to group-level advertising ("*which almost by definition is less precise and efficient than user-level targeting*"[19]), with less effective results given impaired attribution reporting, and further pushes publishers to a subscription revenue model by which monetization model, Apple and Google each tax rival publishers' revenues.

[11] https://www.theinformation.com/articles/apples-ad-targeting-crackdown-shakes-up-ad-market
[12] https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf (27 August 2019)
[13] See para 6.41 of the CMA Online platforms and digital advertising final report (July 2020) at https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf; further supported in para 3.38 of the CMA's Decision to accept commitments from Google at Decision to accept commitments (publishing.service.gov.uk)
[14] See under section "How we're complying with ATT" at https://www.blog.google/products/ads-commerce/preparing-developers-and-advertisers-for-policy-updates/ where it states that Google will not be showing the ATT prompt
[15] "*Tracking refers to the act of linking user or device data collected from your app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also refers to sharing user or device data with data brokers.*" https://developer.apple.com/app-store/user-privacy-and-data-use/
[16] See CNIL's 8 million euro fine against Apple for collecting cross-site data for the purpose of personalised advertising by default at https://www.cnil.fr/en/advertising-id-apple-distribution-international-fined-8-million-euros
[17] See at page 237 of the CMA's Mobile ecosystems Market study final report: Final report (publishing.service.gov.uk). See further at https://www.lotame.com/idfa-and-big-tech-impact-one-year-later/
[18] Even Google reported to app developers that Apple's new ATT framework is likely to "see a significant decrease in reach https://support.google.com/google-ads/answer/10307993?hl=en
[19] https://mobiledevmemo.com/the-att-recession/

(d) Google similarly disabled access to its mobile advertising ID, the AAID, from Android 12 starting in late 2021.[20]

8. The above restriction in data should be considered in the light of the ISA between Google and Apple, and the data sharing that the agreement provides to each of them, in discrimination to rivals.

9. Browser owners that act as the user's agent and disregard the interests of other parties, Google and Apple are able to use this control to scrape third party content (publisher content) to train and feed into their AI models. The CMA should ensure that the operating system and browser are not used to circumvent publisher rights.

10. The CMA should bear in mind Section 29 of the DMCCA, which provides for an exemption to the undertaking in the event of a conduct investigation. The CMA should anticipate that Google would use privacy and security as the benefits that is provided to users as a result of the current "walled garden" approach to their mobile ecosystems.

(a) **Privacy.** The CMA notes both Apple[21] and Google's[22] claims that their anticompetitive conduct is somehow justified by reference to their ill-defined reference to protecting "*privacy*." The CMA found in the mobile ecosystems report in 2020 and in the mobile browsers investigation, that there was no basis to Google's use of privacy as an argument.

(b) 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.[23]

(c) **Security.** There should be an operations analysis regarding the type of data that needs to be kept secure. If it does not regard personal data, the foreclosure of rivals becomes disproportionate on these grounds.

(d) Security can be defined as preventing unauthorised access.[24] 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

[20] https://support.google.com/googleplay/android-developer/answer/6048248?hl=en-GB#:~:text=Any%20attempts%20to%20access%20the,Play%20starting%201%20April%202022.
[21] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraphs 4.20ff, 7.102ff, 11.112ff.
[22] 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
[23] 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
[24] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 4.130.

reasonable to have greater safeguards in place, such as deidentifying the data or rendering it non-sensitive.[25]

(e) 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.

Q5: Are the potential interventions set out above likely to be effective, proportionate and/or have benefits for businesses and consumers?

11. As the CMA notes, so that remedies are effective under the DMCCA, they should be designed in a way that withstands technological change. 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.

12. 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.[26] This can be reinforced with relation to the obligations on Apple and Google with relation to browsers as defined with relation to W3C standards.

13. 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.[27]

14. 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.

Q6: What key lessons should the CMA draw from interventions being considered, imposed and/or implemented in relation to mobile ecosystems in other jurisdictions?

15. The CMA should draw findings from the DOJ complaint against Apple filed on 21 March 2024[28] and in particular, the ones that support Apple's strategy to make its mobile ecosystem "sticky" and thus, restrict third parties' interoperability.

[25] The California data protection law allows for transient processing to render sensitive information non sensitive. See 1798.140(e)(4).
[26] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 2.118.
[27] CMA, Mobile Browsers and Cloud Gaming, Provisional decision report (22 November 2024), paragraph 2.120
[28] https://www.justice.gov/archives/opa/media/1344546/dl?inline

If you have any questions about this response, or would like to speak further, please let us know.

Yours faithfully,

[redacted]

Preiskel & Co LLP

Appendix 1
Evidence of Google's Exploitative Conduct

Google's privacy sandbox is a modification to Google's Chrome browser, which transforms how online data is collected by Google, and the terms on which it is available to third parties[29]. Google announced the Privacy Sandbox in 2019[30]. The below table provides a chronologic sequence around Google's impact on data availability:

Source of data	Google's changes under Google Privacy Sandbox
2008-2009 **Double Click IDs** (advertising IDs)	Google acquired DoubleClick in early 2008. From 2009, Google encrypted the Double Click ID match keys that were previously used widely in the industry, thereby reserving to itself the quality-of--service benefit arising from their use.
2015 **Header Bidding** (used by publishers to allow non-Google ad exchanges to bid for ad inventory)	Google blocked the underlying functionality and disabled rivals' ability to compete via Last Look. Then, from 2015, Accelerated Mobile Pages ("AMP")[31] Unified Pricing rules.
2017 **Open Bidding**	The DOJ noted that the effect of driving rival systems to rely on cookie files for match key synchronisation[32]. Google began to prevent rivals access via JavaScript to the cookie files containing common match keys when used in a third-party context.[33]
2019 **Open Web Data and Cookies**	In August 2019[34], Google announced its Privacy Sandbox changes[35]. 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)
2022 **Google Advertising IDs (in Android)**	In 2022[36], Google announced its further withdrawal of match keys across its Android OS, which are called Mobile Advertising IDs or MAIDs (Privacy Sandbox in Android)[37].
2023 **Open Web Data and User Agent String ("UAS")**	UAS is a line of code that identifies the browser, version of the browser, model and type of device and operating system it is running on.

[29] https://blog.google/products/chrome/building-a-more-private-web/ Google's announcement of GPS in August 2019.
[30] https://www.chromium.org/Home/chromium-privacy/privacy-sandbox/ Chromium project blog in August 2019 stating that GPS will replace functionality.
[31] Google introduced "Accelerated Mobile Pages" (AMP). The effect of this extra step gave Google's Ad Systems two advantages: greater scale and faster matching for any new browsers visiting publishers' properties - given its systems could continue to rely on real-time transport with access to a locally stored match key. The network effect of scale here cannot be isolated from the scale analysis in the **US Search** case.
[32] Instead of using the open web data available for Header Bidding, publishers were faced with a much more limited technical solution, where Google imposed additional fees for integration, with restricted data and limited interoperable information. Google portrayed Open Bidding as an improvement to Header Bidding that created a real-time bidding auction with multiple ad exchanges, like Header Bidding, but on Google's servers to reduce latency: thereby placing rival exchanges at a technical and economic disadvantage. Once more, the barrier to entry this caused cannot be ignored in the context of network effects in **Search**.
[33] See https://developers.google.com/search/blog/2020/01/get-ready-for-new-samesitenone-secure
[34] https://blog.google/products/chrome/building-a-more-private-web/
[35] https://developers.google.com/privacy-sandbox/overview
[36] https://trackiercom/blog/everything-you-need-to-know-about-gaid "Google announced in March that GAID, their user identification for marketers, will be deprecated by Android, the most popular operating system in the world, by 2024."
[37] https://developer.android.com/design-for-safety/privacy-sandbox

	In October 2023[38], Google started to block access to the UAS of data[39]. Google is offering an impaired alternative, 'User Agent Client Hints', which instead offers users a higher latency product and, in time, will in practice remove the web data when "Privacy Budget" is implemented.
November 2023 **Open Web Data URLs**	Since November 2023, Google has begun testing the interference with the practice of decorating URL links (which Google refers to as "link decoration" when its Ad Systems rely on this, but "bounce tracking" when rivals' ad solutions rely on this real-time communication mechanism).[40]
2024 **Cookies**	Google imposed a default requirement on websites to attribute in the website code on 'SameSite' cookies[41]. This has the effect of disabling third-party cookies which do not specify the attribute[42]. Google had announced a change of direction with GPS and Cookies in July of this year[43], however, the blog updates detail makes clear that Google will still make irreversible change to third party cookies[44]. Framed as a choice, the decision to not turn to Chrome's data will restrict the choice of functionality and interoperability available in Search and Search Advertising.
November 2024 **Search Rankings**	Google promised the UK CMA that it will not directly use participation in the GPS to adjust a site's rankings in organic Search. However, Google has worded its promise to allow for indirect use of participation to achieve the same anticompetitive effect.[45]

[38] https://developers.google.com/privacy-sandbox/blog/user-agent-reduction-oct-2022-updates

[39] 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.,

[40] We can provide you with MOW's submission to the CMA on this matter (provided on request).

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

[42] MOW had also engaged the CMA in this matter, and filed a formal complaint dated 23 November 2020 and to the W3C on 25 January 2023.

[43] https://privacysandbox.com/news/privacy-sandbox-update/

[44] Per the blog, Anthony Chavez, the VP of the Privacy Sandbox - "*Instead of deprecating third-party cookies, we would introduce a new experience in Chrome that lets people make an informed choice that applies across their web browsing, and they'd be able to adjust that choice at any time.".* In practice, the terms on which this choice is made amounts to a leveraging of Google's monopoly in Search and Search Advertising.

[45] CMA, CMA update report on implementation of the Privacy Sandbox commitments (11 November 2024): "*Google has confirmed to us that Google* ***Search will not use a site's decision*** *to opt-out of the Topics API* ***as a ranking signal.***" (emphasis added) https://assets.publishing.service.gov.uk/media/6731ffb00d90eee304badaff/CMA_s_Q2_to_Q3_2024_report.pdf