PREISKEL & CO

MOVEMENT FOR AN OPEN WEB

Analysis of CMA Decision on Privacy Sandbox

Background and context

1. The CMA has now issued its formal Decision[1] in its enforcement action taken against Google for breach of competition law with respect to Google's proposed browser changes known as the "Privacy Sandbox". The "Decision to Accept Commitments Offered by Google in Relation to its Privacy Sandbox Proposals" addresses the prospective breaches of the law and the Commitments put the CMA and ICO in an oversight role to review further changes and secure compliance.

2. This analysis is provided by Preiskel & Co who are legal advisors to the Movement for an Open Web ("MOW"); a not for profit organisation created to campaign for the Open Web and which filed the original complaint with the CMA, as well as a parallel complaint with the EU Commission. It is derived from the 198-page CMA Decision which is referred to throughout and is not a substitute for reading the full Decision but aims to provide an accessible summary and guide. Reference is made to Decision's paragraph numbers so industry participants and commentators can understand Google's obligations and how future proposals will be reviewed. Please do not hesitate to contact Preiskel & Co if you need further guidance or are looking to join MOW.

3. Google's Privacy Sandbox[2] Proposals (the "Proposals") are a set of proposed changes on Chrome that the CMA has identified[3] as aiming to:

   3.1 remove the cross-site tracking of Chrome users through third party cookies ("TPCs") and other methods of tracking such as fingerprinting; and

   3.2 create a set of alternative tools to provide the functionalities that are currently dependent on cross-site tracking.

4. Absent CMA intervention, Google's proposed browser changes would be likely to amount to an abuse of its dominant position by leveraging its position in the supply of web browsers to foreclose competition in the markets for digital advertising and exploit web users.

CMA has identified functionalities currently dependent on or associated with cross-site tracking

5. Currently, TPCs and other forms of cross-site tracking serve a range of purposes. CMA sees[4] these as including:

   5.1 Ad targeting, in particular interest-based targeting and retargeting […]

   5.2 Measurement, attribution, frequency capping, and reporting: i.e., use to determine how (many) ads have been served successfully to users (measurement), to determine views and clicks on ads which led to conversions (attribution), and to limit how often a specific user is shown an ad (frequency capping). It also supports the reporting of the

[1] https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/100222_Privacy_Sandbox_Decision_edit.pdf
[2] The following is taken mainly from Chapter 3 of the CMA's Decision: https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/100222_Privacy_Sandbox_Decision_edit.pdf
[3] Para 3.9 CMA Decision
[4] Para 3.10 et seq CMA Decision

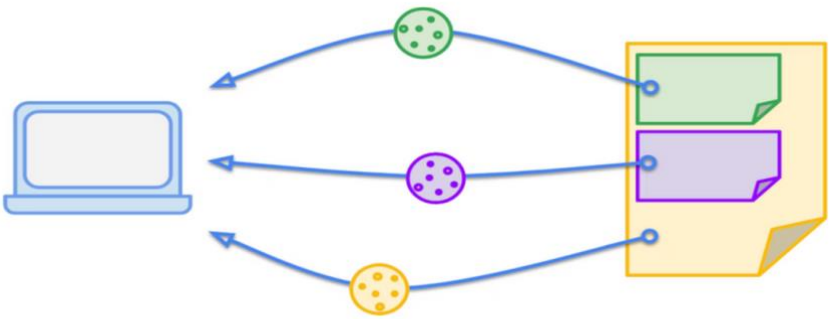
outcomes of ad auctions to advertisers and publishers to facilitate payment and show performance of contracts.

5.3 Spam and fraud detection: Tracking a user's browsing activity across the web is a way to establish whether that user can be trusted or should be considered as conducting fraudulent or spam activities.

5.4 Federated log-in: Allows the user to use a single method of authentication (e.g., username and password) to access different websites rather than creating a new username and password for each website, or to use one login to be signed in on many sites.

What are first-party and third-party cookies? [5]

6. As a helpful posting from Google explains: "*Cookies that match the domain of the current site, i.e., what's displayed in the browser's address bar, are referred to as first-party cookies. Similarly, cookies from domains other than the current site are referred to as third-party cookies. This isn't an absolute label but is relative to the user's context; the same cookie can be either first-party or third-party depending on which site the user is on at the time*."[6] This can be illustrated as:



Cookies may come from a variety of different domains on one page.

First-Party Sets

7. First-Party Sets are a mechanism by which a set of domains can be declared as belonging to the same entity and thus be considered first-party to each other rather than third-party. Consequently, cookies on these domains will not be categorised as third-party cookies and will not be blocked. Functions such as cross site measurement within the set will be possible. Corporate ownership is used to determine the boundary of First-Party Sets. The consequence is that vertically integrated entities, and big companies with a lot of websites (which will be designated as first party domains) will be advantaged over more decentralised businesses and networks of companies and websites of businesses such as newspapers or those like ETSI that use a lot of TPCs.

The CMA's competition concerns

8. Chapter 3 of the CMA Decision in its Privacy Sandbox case sets out the four key issues, three of which are identified as "concerns" aka prospective breaches of competition law that would

[5] https://web.dev/samesite-cookies-explained/
[6] SameSite cookies explained (web.dev)

be breaches, absent Google's Undertakings that enable CMA to oversee what is happening, and prevent the anticipated action and harm being caused from taking place. The first concern is about announcements and differs from others since the announcements have already taken place and harm has already been caused and is ongoing.

Concern 1. Google's Privacy Sandbox Announcements: Existing Publication and Republication

9. Caselaw under the Competition Act has established that anti-competitive announcement may breach the law.[7] To address this issue, the CMA has taken a two-part approach in its Decision. First, it sets out its view that the announced conduct would be likely to amount to an abuse of a dominant position. Second, it sets out that the announcements themselves, and steps taken before the June Notice, are likely to constitute an abuse.

10. This means that the CMA has found Google's announcements prior to June 2019 to be anticompetitive. The CMA lists Google's key announcements.[8] The CMA's view is that Google is likely to have been aware that these announcements, including the setting of a two-year deadline for deprecating TPCs, would adversely affect market participants and reduce competition. For example, studies cited by Google in the announcement of 22 August 2019 suggested that when advertising is made less relevant by removing TPCs, funding for publishers falls by 52% on average.[9] In view of this awareness that the announcements would reduce competition, the CMA's preliminary view is that these announcements were not competitive on the merits.

11. Given Google's position on the relevant and related markets, its status as an unavoidable trading partner and its commercial incentives, the CMA found that a rational market participant would understand that the announcements and/or implementing steps have adverse implications for them. The expectation of a reduction in competition is reflected, for example, in actions that have already been taken by advertisers, publishers and ad tech providers to adjust to the likely future removal of TPCs.

12. It is also likely that any more recent or future announcement that republishes or reinforces the anti-competitive messages contained in previous Privacy Sandbox announcements would also contribute a further breach of the law, if not an identical breach on another occasion to the same or a new audience, and further harm.

13. We note that as at 08 March 2022, Google's Privacy Sandbox statements, its marketing material, and published announcements identified in the CMA Decision have yet to be changed. Many of its publications to date also either directly or indirectly refer out or link back to previous statements, which also serves to republish them.

14. Under English law, the announcements the CMA has identified, as breaches of competition law, fall into the category of a civil wrongs or 'tort'. Damages are available in the civil courts for publication torts and can be quantified with reference to the effects on others which may be evidenced in a number of different ways. There are ways that this can be done while protecting the identity of those harmed. Damages actions and other forms of redress (on an individual or class action basis) may thus now be available to those harmed by Google's anticompetitive announcements.

Three anticompetitive outcomes identified by the CMA

[7] *Royal Mail plc v Office of Communications* [2019] CAT 27.
[8] See para 2.28-2.29 CMA Decision for references and weblinks.
[9] https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf

15. The CMA identifies that the Proposals will illegally allow Google to:

15.1 **Create unequal access**[10] to functionality associated with user tracking, and hence distort ad tech markets and those buying online ad inventory by restricting the functionality associated with user tracking for third parties while retaining this functionality for Google;

15.2 **Self-preference** its own ad inventory and ad tech services by transferring key functionalities to Chrome, which cannot be overseen by others;

15.3 **Exploit** its dominant position by denying Chrome web users substantial choice over how personal data is used for targeting and delivering adverts.

Concern 2: Unequal access to existing functionality

16. This concern relates to the risk that Google's proposals will limit the functionality available to its rivals in the open display market,[11] while leaving Google's ability to offer these functionalities relatively unaffected, thereby having a harmful impact on the ability of:

16.1 publishers to sell ad inventory to advertisers in competition with Google; and

16.2 ad tech providers to sell services to publishers and advertisers in the open display market in competition with Google's ad tech services.

17. The Proposals aim to replace existing functionality including TPCs with alternative solutions, while leaving first-party cookies unaffected.[12] TPCs enable the common identification of web users on web pages. They are a fundamental building block of the advertising used by publishers and ad tech providers that funds many websites. Publishers and ad tech providers depend on TPCs to collect information about web users and provide it to advertisers to target advertising and measure conversions, and the effectiveness of ads. Google can use first-party cookies to perform these functionalities in competition with publishers and ad tech providers. By blocking TPCs, Google is blocking its rivals from being able to compete.[13] Google has a significant data advantage over others.[14]

18. As the CMA describes it: "*the Proposals would therefore be likely to significantly tilt the playing field in display advertising in favour of Google. Google's marketing material shows the potential costs for advertisers of deprecating TPCs, including through the actions of various parties including browsers, and highlights potential solutions including greater use of Google products. For example, it states that there are 'more limitations on the sources of data that can be used to select audiences and personalise ads', that 'restrictions on cookies have made it harder to manage how many times people see ads', and that this risks 'irritating users and damaging your [marketer's] brand' and 'cookies and other identifiers are used to attribute conversions to digital media. So when these measurement tools are constrained, it becomes harder to accurately report on and evaluate how your [marketer's] ads are performing'*."[15]

19. Google's own marketing material suggests that its customers: '*Invest in a comprehensive first-*

[10] Para 1.7.CMA Decision
[11] For example, in terms of the amount of information about a web user that can be associated with an adrequest, which facilitates targeting, frequency capping, verification, and attribution, or the other forms of functionality discussed above.
[12] What will be regarded as a first-party cookie depends on the definition given to first-party under the First-PartySet proposal.
[13] Google has told the CMA that Google's current use of its data in measuring conversions or targeting on third- party inventory necessarily involves the use of TPCs and would become unavailable after TPC removal. Google told the CMA that other publishers can use their own first-party cookies in competition with Google.
[14] Market Study, Appendix F, paragraphs 52–63 and Appendix M, paragraphs 307–314.
[15] Google, Think with Google: The marketer's playbook for navigating today's privacy environment, July 2020,page 5. The document is available on the Internet Archive here (accessed on 3 February 2022).

party measurement solution, where cookies are set only when someone has contact with your [marketer] site. Google's global site tag and Google Tag Manager offer this capability, and support all of Google's advertising and measurement products, including Google Ads, Google Analytics, Campaign Manager, Display & Video 360, and Search Ads 360'.[16] Further, on a Google web page entitled 'Why conversion modelling will be crucial in a world without cookies', Google states: '*What's more, richness and reach of data remain must-haves for reliable modelling. This means leveraging high quality data with a comprehensive view across platforms, devices, browsers, and operating systems. Scale should be your top priority when evaluating the right measurement provider for modelling accuracy'.*[17]

20. The CMA sees these Google statements as suggesting to its customers that removing TPCs, taken by itself, would likely reduce the effectiveness of open display advertising compared to that of advertising provided by Google.

21. This is further supported by the CMA's analysis of UK data from a Randomised Control Trial conducted by Google, which found that, in the short run, unequal access to TPCs and the detailed user information associated with them has a significant negative impact on the revenue of those publishers who cannot sell personalised advertising when competing with those who can.[18]

22. The CMA expressly notes that competition in the "Quality of advertising" (including targeting, frequency capping, verification and attribution) which rivals can offer compared to that offered by Google is a its concern. Two elements then arise- first the usefulness of Google's suggested alternatives (for its rivals) and second, that Google will not be as affected by this as third parties, because of its access to first-party and other user data.

The CMA's issues with Google's 'tools'

FLoC/Topics

23. The Topics API is intended to enable interest-based targeting by ad tech players after Google has blocked cookies from third party domains. This is a subset of the functionality that is currently available using cookies. The initial taxonomy includes 350 topics, which are publicly listed with relation to website names. Topics are assigned to users based on their browsing history of websites that are using the Topics API. Every week, Chrome will calculate the top five topics from the user's browsing history that week. On request Google will supply rivals with one of the top five topics for each of the last three weeks (up to three topics in total). Google will continue to have access to all the information available to calculate topics including from cookies, while its rivals will have only a subset of the available information.

24. Google's Proposals "*would allow publishers to offer advertisers the ability to provide some degree of personalised advertising on their ad inventory, this will be less granular and less personalised. Moreover, while publishers and ad tech providers can at present compete to offer different definitions and delineations of relevant audiences, and this is likely to be a factor underpinning the attractiveness of the open display market, such competition might no longer be feasible under the Privacy Sandbox Proposals as the audience would be determined by Google*.[19] This could reduce the ability of rivals to provide a value proposition. This concern was raised about Google's initial interest-based advertising API proposal, FLoC, and remains

[16] Google, Think with Google: The marketer's playbook for navigating today's privacy environment, July 2020,page 7. The document is available on the Internet Archive here (accessed on 3 February 2022).
[17] Why conversion measurement will be crucial - Think with Google (accessed on 3 February 2022).
[18] The results showed that the removal of TPCs led to a 70% reduction in publisher revenue per page view in the short term. For further reference, see Market Study, Appendix F, paragraphs 115–119.
[19] Although Google has suggested that the topics taxonomy and the classifier itself may be open sourced ormaintained externally, the browsing history itself that the topic assignment depends on will require Google Chrome.

relevant for Topics.

25. CMA notes that "*Google could advantage itself in several ways. If Google were to use Chrome browsing history data in its ads products, for example, then it would have a further advantage against competitors because browsing history is a key input to the Topics API, so Google would be able to make better use of the topics for a user it receives from the Topics API, as it has the training data of the Topics API to cross-reference its targeting model against, and thus may more easily segment users into richer interest groups (giving an ability similar to cross-site tracking with identifiers).*" [20]

26. The CMA understands that the number of topics a site may be able to learn about users is proportional to its reach. For Google, with a large 'reach' (e.g., in the form of Google Analytics but also other products), it may gain an undue advantage. Sections G and H in the Final Commitments are intended to help the CMA ensure that Google is unable to engage in such behaviour.

Two Uncorrelated Requests, Then Locally-Executed Decision On Victory (TURTLEDOVE), First 'Locally-Executed Decision over Groups' Experiment (FLEDGE) and related proposals

27. Retargeting is the practice of serving targeted ads to specific individuals following a visit to an advertiser's website. Google proposed the following to enable retargeting to continue without using TPCs. The TURTLEDOVE/FLEDGE proposals aim to allow an advertiser to calculate and store custom interest groups in the browser based on the user's activity on that advertiser's website. The winning interest group ad is shown in a 'Fenced Frame'. The purported aim of Fenced Frames is to prevent the webpage on which the ad is shown from learning about the contents of the frame, to ensure that no information about the browser's ad interest is leaked. Google will continue to have access to all data and is not obliged to use this system, which will affect its rivals' ability to retarget users.

28. The CMA notes that "*Google's retargeting proposal would give Chrome full and unique visibility on- device of the retargeting groups to which users belong and the responsibility for joining these groups. Retargeting of individual users is based on groups of users created by advertisers. Google would determine the minimum size of these groups and, in so doing, rival publishers and ad tech providers would not be able to compete with a different minimum group size. This could restrict their ability to compete with Google in retargeting, which would be further exacerbated, according to concerns the CMA has heard from market participants, by their limited ability to optimise advertisers' campaigns in real time."* The concern is that Google could have access to more granular user interest data and therefore have a competitive advantage over rivals in the provision of retargeting services to advertisers.

Reporting and Measurement APIs

29. This proposal is currently aimed at allowing click-through and view-through attribution. Attribution is important for advertisers to measure the effectiveness of advertising via one route rather than another. The proposal allows advertisers to attach data (including intended conversion destination) to their ads. This data is stored by the user's browser when the ad is clicked or viewed. If the user visits the intended destination and converts, the browser records the conversion event and, with a delay, sends a report to the publisher and advertiser that a

[20] The concerns set out in this paragraph are specific to Topics and supersede those raised about FLoC. Specifically, with FLoC Google's DSPs would have been better able to interpret and form relevant inferences from users' FLoC cohort IDs than rival DSPs by associating users' FLoC cohort IDs on its owned and operated properties with other extensive (first-party) data that it has about those web users. Chrome could also give Google's DSPs insights about the FLoC cohorts of web users identified by the browser to advantage itself when bidding on open display ad inventory. See the June Notice, paragraph 5.41.

conversion occurred, without the inclusion of any information about the user. Google will limit the information available about the conversion event and add "noise" to the conversion. The browser would report random instead of actual conversion data some of the time, making the measurement of advertising effectiveness and attribution more challenging for Google's rivals.

30. The CMA found that the measurement and reporting data available to third parties is more limited than under the current framework using TPCs. Google's proposal would mean advertisers and the ad tech providers which act on their behalf would receive noised, circumscribed event-level data in real-time, or aggregated data at various intervals with delay, rather than individual-level data in real time. ***This would limit rival ad tech providers' ability to demonstrate the effectiveness of their services to advertisers and optimise their campaign spend.*** The CMA notes that none of the Proposals currently developed allows for measurement and attribution across publishers such that advertisers, after the removal of TPCs, would not be able to understand which publishers provide better value.

User-Agent Client Hints, Privacy Budget and Gnatcatcher

31. One example the CMA identify of functionality that is potentially being interfered with by Google in a way that adversely affects its rivals is the information provided through the user-agent string. The user agent string of data provides information about the user's browser and device to the website that the user is visiting, and which is used for optimising the user's viewing experience (for instance, to select the most suitable version of a website for the user's browser and device).

32. A further example of functionality used by Google's rivals is the Internet Protocol ('IP') address, which is useful for detecting fraud and the geographical tailoring of content. This proposal aims at reducing the information websites see when looking at IP addresses. Google's browser may forward its hypertext transfer protocol ('HTTP') traffic through an IP privatising server using end-to-end encryption, masking the user's IP address. Certain anti-fraud use cases are to be protected. The cloaking or masking of IP addresses will affect competitor ad companies and independent sources of data used in fraud detection and affect telecoms traffic management and is the subject of a separate complaint to the EU Commission by a group of telecommunications companies.

33. Google's proposals aim to reduce the amount of identifying information, which is passed on to websites, in addition to the limit that will be applied when its Privacy Budget is enforced. ***However, much of the information is also currently used by publishers to optimise the presentation of their website and ads and ensure a high quality user experience as well as fraud detection and prevention***.

34. Specifically, the CMA notes concerns that the User-Agent Client Hints and Gnatcatcher proposals could lead to Google's rival publishers offering a worse service to both users and advertisers when competing with Google to attract advertiser spend to their ad inventory. The CMA understands that both these proposals would hamper Google's rivals' abilities to detect fraud and limit their ability to optimize their online content to, for example, a user's device (because of the User-Agent Client Hints proposal) or a user's geographic location (because of the Gnatcatcher proposal).

Federated Credential Management ('FedCM')

35. The Federated Credential Management ('FedCM'- successor to Web ID) proposal aims to prevent independent decentralised log-in as is common on the Open Web. Google is exploring three variations. Each could add more friction (e.g., in the form of permission prompts) or take control of choice architecture, or delegate a log-in to the browser, cutting across current sign in processes and the contractual relationship between the website owner and its customers. The

CMA found that one variant involves the browser providing warnings and consent notices to the user when a tracking risk appears,[21] which could add friction to the user experience reducing user visits. It also found that some variations could lead to the disintermediation of publishers with harmful consequences for their ability to engage with their customers on their properties.

First Party Sets discretion and data advantages

36. The CMA found that Google retains functionality by using first-party data and first party cookies that would be denied to its rivals on withdrawal of TPCs. One issue is how third-party domains and first-party domains are distinguished. The "First-Party Sets" proposal is a mechanism by which a set of domains can be declared by Google as being first-party to each other, rather than third-party. Consequently, cookies on these domains will not be categorised as TPCs and tracking across the domains within a First-Party Set will continue to be unrestricted. Google owns a very wide range of domains and user- facing services, with the ability to remain able to track users extensively for the purposes of digital advertising.[22] Google's ability to block third parties from equivalent use could distort competition in digital advertising markets.

37. The CMA further noted evidence from its Market Study, and inferred that, for a material portion of traffic handled by Google's ad tech services, Google could use its first-party and signed in data. Google told the CMA that it makes 'extremely limited' use of first-party data, the CMA nevertheless found it had the ability to do so through its privacy policies.

38. In addition, data uploaded via Google's **Customer Match** could continue to allow advertisers to upload their own first-party customer data and match this with other data third-party to Google for the purposes of providing ad targeting and related functionalities on both its owned and operated ad inventory as well as third-party non-Google ad inventory.

Use of Chrome browsing history data for advertising

39. The CMA concern is that third parties would be unable to track individual web users on Chrome while, after the proposals are implemented, Google would retain that ability. For example, Google could use synced Chrome browsing history data to target ads and provide related functionalities linked to web users who have signed into their Google Account on Chrome and allowed their browsing history to be included in their 'Web & App Activity' associated with their Google Account. When users allow this functionality, Google can combine any declared age and gender information from a web user's account with his/her Chrome data and offer personalised advertising to advertisers and publishers.

40. On its Safety Centre web page, Google states that: "*partner websites and apps use your online activity to create ads that are more useful to you […] When we show ads on these partners' sites and apps, they are based on… data that we collect about your online activities… We might also show you ads based on sites that you've visited or your Chrome browsing activity when logged into your Google Account'*.[23]

41. This, and Google's current approach to signed-in users, shows that Google can track users in a way that is not contingent on TPCs, and that it could continue to do so. This is likely to give Google a significant advantage over rival ad tech providers and publishers.

[21] Further information on this 'permission-oriented' variation can be found on the WebID GitHub pages here andhere (accessed on 3 February 2022).
[22] Competition and data protection in digital markets: a joint statement between the CMA and the ICO, May 2021,paragraphs 76–82.
[23] Google Safety Centre, Your Privacy: Ads and Data (accessed on 4 February 2021).

Use of third-party data uploaded via Google Analytics tools for businesses for advertising

42. Google Analytics tracks site activity, such as session duration, pages per session and bounce rates of visitors, and the source of traffic to the site. Google argued that it only uses data from Google Analytics for its own purposes if the customer has enabled data sharing with Google.[24] The CMA found that it could nevertheless use its analytics tools to collect first-party data and use it for advertising purposes.

Concern 3: Self-preferencing Google's own ad tech and ad inventory

43. The CMA's next concern relates to power over Chrome's decisions. Google owns Chrome and operates as a publisher and ad tech provider. This creates a conflict of interest. Google has an incentive not to act in its customers' best interests, for example by self-preferencing its own ad inventory and ad tech services via Chrome's decisions on which ads to display to a given web user. This also affects Google's incentives in engaging with industry and taking on board any suggested alternative solutions to the Proposals, which might reduce Google's ability to self-preference. The CMA's preliminary view is that Google using its control over Chrome to affect competition in related markets in this way would not represent competition on the merits.

44. The Proposals aim to move some of the functions currently performed by ad tech providers (DSPs, SSPs and/or the publisher ad server) to Chrome. This gives Google an opportunity to leverage its position in the market for the supply of web browsers to reinforce its position in open display advertising. For example, Google's ad tech services could benefit from increased interoperability when interacting with the Privacy Sandbox solutions when compared to rivals (e.g., via reduced latency). It can also use its control over the device on which the auction will take place (e.g., Android devices) to grant its own services a technical advantage in the form, for example, of additional processing power.

45. The CMA is also noted that new tools being developed by Google could be used by Google for further self-preference and discrimination.

46. Google acknowledged in its commitments that the Chrome browser is part of Google's Ads System.[25] However, browsers are designed to be B2C consumer software that help people navigate across the open web and interact with web properties (e.g., entertainment, information, communication, commerce), while the B2B processing of "Ad Systems" can be done on servers on people's local devices, but where this happens does not change WHAT processing is occurring.

Topics API

47. Currently, market participants analyse and draw their own inferences from users' browsing histories using TPCs and other identifiers. The Proposals would change this as advertisers, publishers and ad tech providers would face restrictions on using frequently used identifiers. Topics gives Google control over determining the topics that users are associated with and providing them to users of the Topics API. Google could then be in a gatekeeper position for the ad tech ecosystem.[26]

TURTLEDOVE and FLEDGE

48. Currently, DSPs apply their own bidding logic to determine what bid to return (if any) to a bid

[24] Market Study, Appendix F, footnote 17.
[25] See paragraphs 4.66 and 4.67 of CMA introduction.
[26] Google suggested that the Topics taxonomy could be externally maintained and the classifier that maps sites to topics would be open source and could also eventually be externally maintained to limit the amount of self-preferencing Google would be able to do.

request. For retargeting, an early version of the Proposals would have changed this. DSPs would have shared part of their bidding logic with the browser. This would have introduced new opportunities for conflicts of interest, as Google (which operates the browser) would have known how rival DSPs would bid on retargeting opportunities. The FLEDGE proposal, by contrast, seeks to avoid this issue,[27] but the CMA will monitor the position.

Reporting and Measurement APIs

49. The important activity of reporting to advertisers and media agencies on ad campaign performance, including measurement and attribution is mainly currently carried out by the advertiser's ad server.

50. Under the Proposals, Chrome would replace the advertiser ad server, Chrome would be responsible for tracking the impression events (when a web user views but does not necessarily click on an ad). Chrome would deal with matching such events with conversions, based on the event registration calls the advertiser's ad server is making, and then sending back reports which would be delayed and include less granular data. The browser would essentially become the 'source of truth' for marketers. When advertisers also use Google DSPs, Google would be in a position of 'marking its own homework' and moving this functionality to the web browser increase its conflicts of interest.

Gnatcatcher, Federated Credential Management ('FedCM') and X-Client Data

51. Since Chrome will have access to IP addresses, rivals would have access to more limited data under the Gnatcatcher proposals. Similarly, under FedCM, Chrome would have access to all the user's log in data,[28] which could be shared with Google's advertising services. After the deprecation of the User-Agent string, Chrome will still receive similar but more granular information in the form of X-Client Data, which Google could also use to optimise the performance of its services – and, in principle, track users across the web.[29]

52. Overall, absent its oversight, the CMA is concerned that the shift of functionalities currently performed by ad tech providers to Chrome would give Google discretion that cannot be scrutinised or challenged by third parties. This could lead to the emergence of conflicts of interest and a lack of confidence about Google's intentions. Google's commitments were then needed to put the CMA in an oversight role and provide an impartial review and confidence to the market. This commitment breaks new ground legally as Google's undertaking creates a new role for the CMA in advance of Google's browser changes hitting the market.

Concern 4: Imposition of unfair terms on Chrome web users

53. The CMA considers that different web users will have different attitudes and preferences about the collection and processing of their personal data. Some users may prefer not to have their personal data collected and processed by their browser and/or third parties, while others may agree to such data usage in return for seeing more relevant ads, avoiding repeated ads, or other rewards. As such, the CMA sees "***the degree of control and optionality enabled by browsers with respect to the collection and processing of Personal Data is likely to be a parameter of competition between browsers*".**

54. A browser developer operating under normal and sufficiently effective competition would be expected to face an incentive to give its users significant control over whether and how their

[27] Deciding what counts as misuse would still be at Google's discretion.

[28] The delegation-oriented variant of WebID can be found on the WebID GitHub pages here and here (bothaccessed on 4 February 2022)

[29] Google told the CMA that X-Client Data header is used to help Chrome test new features before rolling themout, not to identify or track individual users.

personal data is used, subject to suitable defaults and an adequate choice architecture. The CMA notes that Firefox and Safari each provide a degree of control to their users in this respect: while TPCs are blocked by default in these two browsers, users have the option of disabling TPC blocking, either in general or for specific sites.

55. In contrast, under the Proposals, the CMA has been informed by Google that Google has not decided whether Chrome web users will have the option of enabling TPCs in Chrome after Google's removal of TPCs. Chrome web users could have little or no control with respect to whether and how their personal data is used by the browser/ Google for cohort advertising retargeting or otherwise.[30] The CMA is concerned that this may amount to an abuse in the form of the imposition of unfair terms on consumers, and that such unfair terms would likely harm consumers by preventing them from adjusting the level of privacy and targeting in line with their preferences.

Asymmetry of information and lack of confidence on the part of market participants

56. Google has encouraged market participants to engage and provide feedback, including through the World Wide Web Consortium ('**W3C**'), on the Privacy Sandbox Proposals.[31] The CMA notes that in this and other fora, some market participants have suggested amendments to the Proposals, these appear to have influenced FLEDGE, FloC and Topics. However, issues have been raised that:

    56.1 W3C engagement has been limited, very technical, ad hoc for feedback rather than using a process for discussing and agreeing new standards.

    56.2 There is a lack of transparency over how Google intends to test the effectiveness of the Proposals, including the criteria it will use in evaluating their effectiveness and how feedback from market participants will be taken into account.

    56.3 Google's claims lack evidence. For example, Google's test of the effectiveness of FLoC, as a replacement signal for TPCs, was seen to reflect Google's use cases only and,[32] insufficient underlying evidence has been provided to enable such claims to be assessed and some Proposals are a 'black box', in that the workings of Google's algorithms in Chrome cannot be observed, and their impartiality and effectiveness cannot be assessed.

57. The CMA considers that these issues reflect the strong asymmetry of information between Google and market participants as well as the commercial incentives that Google faces in developing its Proposals given its likely dominant position in the browser market and its significant presence in open display advertising, where it competes with publishers and ad tech providers which could be significantly impacted by the Privacy Sandbox Proposals.

58. For these reasons, the CMA considers that it is important to ensure greater transparency in relation to the process for developing the Privacy Sandbox Proposals and regarding the effectiveness of the Privacy Sandbox Proposals themselves to ensure that Google does not gain

[30] Google has added user controls regarding the Privacy Sandbox trials in Chrome settings.

[31] For example, in Google's announcements dated 14 January 2020 and 25 January 2021.

[32] For example, in January 2021 Google stated publicly that 'FLoC can provide an effective replacement signal for third-party cookies. Our tests of FLoC to reach in-market and affinity Google Audiences show that advertiserscan expect to see at least 95% of the conversions per dollar spent when compared to cookie-based advertising'.See Google Ads, 'Building a privacy-first future for web advertising' (accessed on 4 February 2022). Note that, inJanuary 2022, Google replaced FLoC with Topics. See Appendix 3 for further details.

a competitive advantage from its likely dominant position in browsers.

Summary of concerns

59. The CMA is concerned that, without sufficient regulatory scrutiny and oversight, the Privacy Sandbox Proposals would:

    59.1 distort competition in the market for the supply of ad inventory and in the market for the supply of ad tech services, by restricting the functionality associated with user tracking for third parties while retaining this functionality for Google;

    59.2 distort competition by the self-preferencing of Google's own advertising products and services and owned and operated ad inventory; and

    59.3 allow Google to exploit its likely dominant position by denying Chrome web users substantial choice in terms of whether and how their personal data is used for the purpose of targeting and delivering advertising to them.

60. In addition, the CMA is concerned that the announcements have caused uncertainty in the market as to the specific alternative solutions which will be available to publishers and ad tech providers once TPCs are deprecated. The announcements and actions prior to issue of the June 2021 Notice showed (and created the expectation) that Google was determined to proceed with changes in the relevant areas, including by deprecating TPCs within two years of the announcements, in ways which advantage its own businesses and limit competition from its rivals.

61. In this regard, the CMA considers that the concerns that third parties have expressed to it regarding the impact that the Privacy Sandbox Proposals are likely to have in the future, reflect, in part:

    61.1 the asymmetry of information between Google and third parties regarding the development of the Privacy Sandbox Proposals, including the criteria that Google will use to assess different design options and evidence relating to their effectiveness against these criteria; and

    61.2 a lack of confidence on the part of third parties regarding Google's intentions in developing and implementing the Privacy Sandbox Proposals, given the commercial incentives that Google faces in developing Google's Proposals and the lack of independent scrutiny of Google's Proposals.

62. The above provide the basis for the CMA's position and the concerns addressed by the Undertakings.

What is next?

63. Google has committed to training and independent monitoring and compliance. The compliance statements require Google to put in place a series of actions including "A description of training Google has carried out to ensure that all relevant Chrome staff and agents are aware of the requirements of paragraphs 25-27 and 30-31 of these Commitments and the attendees of such training.." and "A description of training material Google makes available to all relevant publisher-and advertiser-facing staff and agents to make them aware about how to communicate around the Removal of Third-Party Cookies and the Privacy Sandbox (at least with respect to paragraphs 25-27 and 30-31 of the Commitments)".

64. Solutions like Topics, FLEDGE and FLOC are inadequate in their ability to replicate the functionality of products such as third-party cookies and hence cannot be use as a substitute. This needs to be made clear in communications so that industry knows to rely on the current system rather than waste time and resources on addressing inadequate alternatives.

65. Google probably needs to modify its public communications including the privacysandbox.com website.

66. GDPR applies. This indicates that standards bodies such as IAB, W3C and IETF that are working on solutions where Google is putting forward alternatives, need to re-assess and seek to progress solutions that do not either ignore GDPR or restrict lawful data sharing if they wish Google to be able to participate in such solutions.