Notice of intention to accept commitments offered by Google in relation to its Privacy Sandbox Proposals

Case number 50972

11 June 2021

Contents

Page

1. Executive Summary

1.1 On 7 January 2021, the Competition and Markets Authority ('**CMA**') opened an investigation into suspected breaches of competition law by Google. The investigation concerns Google's proposals to replace third-partycookies ('**TPCs**') and other functionalities with a range of changes known as the 'Privacy Sandbox' Proposals. It follows complaints of anticompetitive behaviour and requests for the CMA to ensure that Google develops its proposals in a way that does not distort competition.

1.2 The Privacy Sandbox Proposals are a set of proposed changes on Chrome that aim to address privacy concerns by removing the cross-site tracking of Chrome users through TPCs and other methods of tracking; and create a set of alternative tools to provide the functionalities that are currently dependent on cross-site tracking.

1.3 The CMA has been working closely with the Information Commissioner's Office ('**ICO**') who is also assessing the Privacy Sandbox Proposals for compliance with data protection and ePrivacy law. The CMA and the ICO are working collaboratively in their engagement with Google and other market participants to build a common understanding of Google's proposals, and to ensure that both privacy and competition concerns can be addressed as the proposals are developed in more detail.

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

(a) 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;

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

(c) allow Google to exploit its apparent 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.

1.5 The CMA is also concerned that the announcements of the Privacy Sandbox Proposals 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 to date have shown (and created the expectation) that Google is 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.

1.6 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:

(a) 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

(b) 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.

1.7 Google has offered commitments ('**Proposed Commitments**') which seek to address these concerns. The CMA has reached the provisional view that the Proposed Commitments, once implemented, would address its competition concerns as they:

(a) **Establish a clear purpose of the Proposed Commitments** that will ensure that Google's Proposals are developed in a way that addresses the above competition concerns, by avoiding distortions to competition, whether through restrictions on functionality or self-preferencing, and avoiding the imposition of unfair terms on Chrome's web users.

(b) **Establish the criteria that must be taken into account in designing, implementing and evaluating Google's Proposals**. These include the impact of the Privacy Sandbox Proposals on: privacy outcomes and compliance with data protection principles; competition in digital advertising and in particular the risk of distortion to competition between Google and other market participants; the ability of publishers to generate revenue from ad inventory; and user experience and control over the use of their data.

(c) **Provide for greater transparency and consultation with third parties over the development of Google's Proposals**, including a commitment publicly to disclose the results of tests of the effectiveness of alternative technologies. This would help to overcome the asymmetry of information between Google and third parties regarding the development of the Privacy Sandbox Proposals;

(d) **Provide for the close involvement of the CMA in the development of Google's Proposals** to ensure that the purpose of the Proposed Commitments is met, including through regular meetings and reports, working with the CMA without delay to identify and resolve any competition concerns before the removal of TPCs, involving the CMA in the evaluation and design of tests of Google's Proposals. This would ensure that the above concerns about the potential impacts of the Privacy Sandbox Proposals are addressed and contribute to addressing the lack of confidence on the part of third parties regarding Google's intentions in developing and implementing Google's Proposals;

(e) **Provide for a standstill period** of at least 60 days before Google proceeds with the removal of TPCs ('**Standstill Period**'), giving the CMA the option, if any outstanding concerns cannot be resolved with Google, to reopen its Investigation and, if necessary, impose any interim measures necessary to avoid harm to competition. This provision would strengthen the ability of the CMA to ensure its competition concerns are in fact resolved;

(f) Include specific **commitments by Google not to combine user data** from certain specified sources for targeting or measuring digital advertising on third-party and first-party ad inventory. This would contribute to addressing the competition concerns arising from Google's greater ability to track users after the introduction of Google's Proposals; and

(g) Include **specific commitments by Google not to design any of the Privacy Sandbox Proposals in a way which could self-preference Google**, not to engage in any form of self-preferencing practices when using the Privacy Sandbox technologies and not to share information between Chrome and other parts of Google which could give Google a competitive advantage over third parties. This would address the above concerns relating to the potential for discrimination against Google's rivals.

1.8 Overall, the CMA's provisional view is that, in combination, the Proposed Commitments would address the competition concerns that the CMA has identified in relation to the Privacy Sandbox Proposals, and provide a robust basis for the CMA, ICO and third parties to influence the future development of Google's Proposals to ensure that the Purpose of the Commitments is achieved.

1.9 The CMA has not reached a final view and invites all interested parties to submit observations and evidence in order to assist the CMA in its final assessment of the Proposed Commitments. **How to respond** is set out in section 7 with deadline for comments by **8 July 2021 at 5pm**.

2. Introduction

2.1 On 7 January 2021, the CMA opened an investigation into suspected breaches of the prohibition in Chapter II of the Competition Act 1998 (the '**Act**') by the undertaking comprising Google UK Limited and Google LLC and any other member of their corporate group[1] ('**Google**'), in relation to Google's proposals to withdraw support for TPCs on Chrome and Chromium and replace TPCs and other functionalities with a range of Privacy Sandbox tools, while transferring key functionality to Chrome (the '**Investigation**').[2]

2.2 On 28 May 2021, Google offered commitments to the CMA aimed at addressing the CMA's competition concerns in this Investigation. The Proposed Commitments are described in section 6 of this notice and the text of the Proposed Commitments is set out at Appendix 1.

2.3 The CMA gives notice[3] that it intends to accept the Proposed Commitments and invites representations from interested third parties on this proposed course of action. The CMA will consider representations made by third parties on the Proposed Commitments before making a final decision on whether to accept them. Details on how to comment are provided at section 7 of this notice. The closing date for comment is **8 July 2021 at 5pm.**

2.4 Formal acceptance of the Proposed Commitments by the CMA would result in the termination of the Investigation, with no decision made as to whether or not the Act has been infringed by Google. Such acceptance of the Proposed Commitments would not prevent the CMA from taking any action in relation to competition concerns which are not addressed by the Proposed Commitments. Moreover, acceptance of the Proposed Commitments would not prevent the CMA from continuing the Investigation, making an infringement decision, or giving a direction in circumstances where the CMA had reasonable grounds for:

- believing that there had been a material change of circumstances since the commitments were accepted;

[1] For these purposes, 'group' is to be interpreted as including those companies with which any of Google UK Limited, Google LLC and Alphabet Inc. has the links described in Article 5(4) of the EU Merger Regulation, which is available on eurlex.europa.eu. Please refer to paragraphs 175 et seq of the Commission Consolidated Jurisdictional Notice, which is available on eurlex.europa.eu.

[2] These proposals are interchangeably referred to as '**Google's Proposals**' or '**Privacy Sandbox Proposals**'. They are described in detail in Appendix 2.

[3] Pursuant to paragraph 2 of Schedule 6A to the Act.

- suspecting that a person had failed to adhere to one or more of the terms of the commitments; or

- suspecting that information which led the CMA to accept the commitments was incomplete, false or misleading in a material particular.[4]

2.5 Where a person from whom the CMA has accepted commitments fails without reasonable excuse to adhere to the commitments, the CMA may apply to the court for an order requiring the default to be made good.[5]

2.6 To assist third parties in responding to this consultation, this notice provides information on the Investigation, the market context and the CMA's competition concerns. The notice then summarises the commitments offered by Google and sets out why the CMA provisionally considers that the Proposed Commitments address its competition concerns.

[4] Pursuant to section 31B(4) of the Act.
[5] Pursuant to section 31E of the Act.

3. The CMA's Investigation

The Investigation

3.1 In its market study into online platforms and digital advertising (the '**Market Study**'),[6] the CMA highlighted a number of concerns about the potential impact of Google's Proposals, including that they could undermine the ability of publishers to generate revenue and undermine competition in digital advertising, entrenching Google's market power. Before launching the Investigation, the CMA had been discussing Google's Proposals with the ICO through the Digital Regulation Cooperation Forum ('**DRCF**').[7] As part of this work, the CMA had also been engaging with Google to better understand its Privacy Sandbox Proposals.

3.2 In autumn 2020, the CMA received complaints, including from Marketers for an Open Web Limited ('**MOW**'), alleging that, through its Privacy Sandbox Proposals, Google was abusing its dominant position. The CMA also received applications, including from MOW, requesting that the CMA give interim measures directions to Google under section 35 of the Act for the purpose of preventing significant damage to 'parties in the Open Web' and to protect the public interest.[8]

3.3 On 7 January 2021, the CMA launched the Investigation, having established that it had reasonable grounds for suspecting that Google had infringed Chapter II of the Act in relation to its Privacy Sandbox Proposals and having determined that a formal investigation would be consistent with the CMA's Prioritisation Principles.[9]

3.4 During the course of its Investigation, the CMA has undertaken a number of investigative steps to gather evidence from Google and third parties,[10] including sending formal notices under section 26 of the Act requiring the provision of documents and/or information. Some third parties submitted information voluntarily to the CMA. The CMA has also continued its

[6] Online platforms and digital advertising market study, final report, July 2020.
[7] For more information see DRCF. Indeed, the Investigation informs the joint work in relation to data protection and competition regulation between the CMA and the ICO, as set out in 'Section B: Joined up regulatory approaches' of the DRCF: Plan of work for 2021 to 2022, March 2021.
[8] The application from MOW was submitted on 23 November 2020. Under section 35 of the Act, the CMA can require a business to comply with temporary directions (interim measures) where: (i) the investigation has been started but not yet concluded; and (ii) the CMA considers it necessary to act urgently either to prevent significant damage to a person or category of persons, or to protect the public interest. In giving interim measures directions, the CMA can act on its own initiative or in response to a request to do so.
[9] Prioritisation principles for the CMA (CMA16), April 2014.
[10] The CMA gathered evidence from a variety of market participants including publishers, industry bodies and businesses active in the digital advertising supply chain.

engagement with the ICO and both authorities have jointly held meetings with Google and third parties.

3.5 Following discussions with the CMA, Google indicated an intention in principle to offer commitments. On 12 February 2021, the CMA sent a summary of its competition concerns to Google. In line with its Procedural Guidance,[11] the CMA proceeded to discuss with Google the scope of commitments which the CMA considered would be necessary to address the concerns it had identified.

3.6 Section 31A of the Act provides that, for the purposes of addressing the competition concerns it has identified, the CMA may accept, from such person (or persons) concerned as it considers appropriate commitments to take such action (or refrain from such action) as it considers appropriate. The Procedural Guidance describes the circumstances in which it may be appropriate to accept commitments and the process by which parties to an investigation may offer commitments to the CMA.

3.7 In accordance with paragraph 10.21 of the Procedural Guidance, a business under investigation can offer commitments at any time during the course of an investigation until a decision on infringement is made. In this case, no decision on infringement has been made.

3.8 On 31 March 2021, Google submitted a draft commitments proposal to the CMA. It did so without prejudice to Google's position in this Investigation or any other. Following discussions with the CMA, Google revised its proposal and formally offered commitments to the CMA on 24 May 2021. These are referred to in this notice as the Proposed Commitments, and are set out in Appendix 1. The offering of commitments does not constitute an admission of an infringement of the Chapter II prohibition of the Act by Google.

3.9 Having considered the Proposed Commitments and for the reasons set out in this notice, the CMA is currently of the view that the Proposed Commitments address the CMA's competition concerns and, as a result, it is appropriate for the CMA to exercise its discretion to close the Investigation by way of a formal decision accepting the Proposed Commitments. Formal acceptance of commitments would result in the CMA terminating the Investigation and not proceeding to a decision on whether or not the Chapter II of the Act has been infringed. This does not prevent the CMA from re-opening its Investigation in certain circumstances.

[11] Guidance on the CMA's investigation procedures in Competition Act 1998 cases (CMA8), November 2020 ('**Procedural Guidance**'), paragraph 10.22.

3.10 The CMA has received requests that it use its interim measure powers under section 35 of the Act to give directions to Google, pending the outcome of the Investigation. The CMA is currently minded to accept commitments from Google to address its competition concerns. Accordingly, the CMA has not reached a view on whether the conditions of section 35 of the Act are met. If, following the current consultation, the CMA maintains its view that the Proposed Commitments address its competition concerns and the CMA decides to accept commitments, the CMA will not adopt interim measures in relation to the conduct which was the subject of the Investigation. Interim measures could be considered in the future if one of the statutory exemptions applies.[12]

The party and conduct under investigation

3.11 Google LLC is a limited liability company incorporated in the US. It is the immediate parent and controlling shareholder of Google UK Limited, a limited liability company incorporated in the UK. Google LLC is a wholly owned subsidiary of Alphabet Inc, a US-incorporated multinational technology company listed on the NASDAQ stock exchange and Frankfurt stock exchange. Alphabet Inc's turnover for the financial year ending 31 December 2020 was USD 182,527 million.[13]

Google's activities

3.12 Google is active in a wide range of internet-related services and products. These include a search engine (Google Search), a video-sharing platform (YouTube), an email service (Gmail), a web browser (Chrome) as well as a browser engine (Chromium), a mobile and tablet operating system (Android), and hardware devices (such as Google Home). Google is also involved in the supply of search and display advertising and offers online advertising technologies (such as AdSense and AdWords).

3.13 Chromium is an open-source project created by Google which includes Blink, the browser engine. Chromium, including Blink, is the basis of Google's browser Chrome. Browser engines are a core software

[12] Section 31B(2)(c) of the Act makes provision that the CMA shall not give a direction under section 35 of the Act (interim measures) in relation to the conduct which was the subject of its investigation unless one of the statutory exceptions applies. Under section 31B(4) of the Act, the CMA is not prevented from (among other things) giving a direction where it has reasonable grounds for: (a) believing that there has been a material change of circumstances since the commitments were accepted; (b) suspecting that a person has failed to adhere to one or more of the terms of the commitments; or (c) suspecting that information which led it to accept the commitments was incomplete, false or misleading in a material particular.

[13] Alphabet Inc., Form 10-K, Annual Report pursuant to section 13 or 15 (d) of the Securities and Exchange Act 1943 for the fiscal year ended December 31, 2020.

component which produces web pages. Several other browsers rely on Chromium, including Microsoft Edge.

Browsers

3.14 Browsers are used both on desktop computers and mobile devices. Browsers provide services to web users, publishers, and advertisers (and, by extension, the ad tech intermediaries operating on behalf of publishers and advertisers). In particular:

- Web users use browsers to access and interact with online content.
- Publishers build and optimise web pages that load in browsers to make content available to web users. Where publishers use an ad-funded business model (ie monetise their content using ads), publishers and their ad tech providers may also collect and use data about users' browsing behaviour, in order to display targeted ads to them.
- Advertisers pay for ads to be displayed on publishers' web pages. These ads may direct users to the advertisers' own web pages selling goods and services. Like publishers, advertisers and their ad tech providers may collect and use data about users to devise, execute, and evaluate advertising strategies. This includes determining whether and how much to bid for an opportunity to show an ad to a given user, where display advertising is sold programmatically. It also includes determining the extent to which users that have been exposed to an ad go on to convert (eg make a purchase), and hence the return on advertising spend.

3.15 Each browser sits on top of a browser engine, which transforms web page source code into web pages that people can see and engage with.

3.16 Many of the methods that publishers, advertisers and ad tech providers employ to collect and use data which are specific to web users depend on features of browsers, including TPCs and other functionalities affected by changes proposed in the Privacy Sandbox as set out in Appendix 2.

The digital advertising supply chain

3.17 In digital advertising, publishers sell **ad inventory** to advertisers. This is space on a publisher's property (eg on a web page or mobile app), which can be filled with an advertiser's ads. Ads that are shown in response to search queries are referred to as **search advertising**. In the Market Study the CMA estimated that Google's share of the search market is more than

90%.[14] **Display advertising** refers to ads displayed alongside the content displayed on a web page or mobile app.

3.18 Display advertising comprises two channels: (i) the '**owned and operated**' channel, which is primarily made up of large vertically integrated platforms which sell their own ad inventory directly to advertisers or media agencies through self-service interfaces; and (ii) the '**open display**' channel, which comprises a wide range of publishers who sell their ad inventory through a complex chain of ad tech intermediaries that run auctions on behalf of the publishers (including online newspapers) and advertisers.

3.19 On the advertiser (demand) side, ad tech intermediaries include demand side platforms ('**DSPs**'). DSPs allow advertisers to buy ad inventory from many sources. In the Market Study the CMA estimated that Google's two DSPs, DV360 and Google Ads, account for [50-60]% of the value of ads purchased through DSPs.[15]

3.20 On the publisher (supply) side, supply side platforms ('**SSPs**') provide the technology to automate the sale of digital ad inventory. They allow real-time auctions by connecting to multiple DSPs, collecting bids from them, and performing the function of exchanges. They can also facilitate more direct deals between publishers and advertisers. In the Market Study the CMA estimated that Google accounts for [50-60]% of the value of ads sold in the UK across SSPs.[16]

3.21 **Publisher ad servers** manage publishers' ad inventory and are responsible for the decision logic underlying the final choice of which ad to serve. They base this decision on the bids received from different SSPs and the direct deals agreed between the publisher and advertisers. Google also provides publisher ad server services accounting for [90-100]% of the display ads served in the UK, according to the CMA's Market Study findings.[17]

Conduct under investigation

3.22 Currently, open display advertising relies on the ability to identify individual web users and 'track' them across web pages by means of TPCs and other forms of cross-site tracking. In 2019, Google announced its plans to

[14] Market Study, Appendix C, paragraph 97.
[15] Market Study, Appendix C, paragraph 254.
[16] Market Study, Appendix C, paragraph 248.
[17] Note that this finding relates to Google's position amongst specialist publisher ad servers. When considering all of the intermediaries who served ads to UK users from whom the CMA received data in the course of the Market Study, Google had a share of [70-80]% of impressions served. Market Study, Appendix C, paragraph 244.

remove support for TPCs in its Chrome browser and replace the functionality of TPCs and other forms of cross-site tracking with a number of changes through its Privacy Sandbox Proposals. Google made the following key announcements in relation to its planned changes to Chrome:

(a) 7 May 2019: Google announced its intention to update Chrome to provide users with more transparency about how sites use cookies, as well as simpler controls for cross-site cookies.[18]

(b) 22 August 2019: Google announced the Privacy Sandbox initiative, comprising 'a set of open standards to … enhance privacy on the web'.[19]

(c) 14 January 2020: Google first announced its intent to remove TPCs from Chrome.[20]

(d) 25 January 2021: Google provided a progress update and set out early results and new proposals ready for testing.[21]

(e) 3 March 2021: Google provided further detail on its use of user-level identifiers to track users across the web once TPCs are phased out.[22]

(f) 9 April 2021: Google provided an update on its proposal to replace use cases for conversion measurement at aggregate and event level once TPCs are phased out.[23]

(g) 19 May 2021: Google provided an update on its proposal to reduce the granularity of information available from user-agent strings, indicating that their proposed replacement, eg the User-Agent Client Hints application programming interface ('**API**'), was available by default in Chrome (since M89).[24]

3.23 The stated aim of Google's Proposals is to remove cross-site tracking of Chrome users through TPCs and alternative methods such as fingerprinting, and replace it with tools to provide selected functionalities

[18] Chromium Blog, Improving privacy and security on the web, May 2019.
[19] Google, Chrome: Building a more private web, August 2019; and Chromium Blog, Potential uses for the Privacy Sandbox, August 2019.
[20] Chromium Blog, Building a more private web: A path towards making third-party cookies obsolete, January 2020.
[21] Chromium Blog, Privacy Sandbox in 2021: Testing a more private web, January 2021; and Google Ads, Building a privacy-first future for web advertising, January 2021.
[22] Google Ads & Commerce Blog, Charting a course towards a more privacy-first web, March 2021.
[23] Google Ads & Commerce Blog, Privacy-first web advertising: a measurement update, April 2021.
[24] Chromium Blog, Update on User-Agent String Reduction in Chrome, May 2021.

currently dependent on cross-site tracking. These proposals are described in more detail in Appendix 2.

3.24 The Investigation focuses on the following areas of potential harm that could arise from Google's conduct:

(a) potential harm to rival publishers and ad tech providers through Google restricting the functionality associated with user tracking for third parties, while retaining this functionality for Google;

(b) potential harm through Google preferencing its own ad tech services and owned and operated ad inventory; and

(c) potential harm to Chrome web users through the imposition of unfair terms.

3.25 The CMA's competition concerns in relation to these areas are set out in section 5 below.

4. Background

4.1 This section sets out the CMA's preliminary view of:

(a) the most plausible definitions of the relevant markets; and

(b) Google's position in the relevant markets.

4.2 The purpose of this section is to provide context to section 5 of this notice which describes the CMA's competition concerns.

Relevant markets

4.3 The CMA has considered the most plausible definitions of the relevant markets that Google is engaged in which relate to the conduct under investigation. The CMA's preliminary view is that the main relevant product markets for the purposes of this Investigation are: (i) the supply of web browsers to web users and publishers; (ii) the supply of display ad inventory to advertisers; (iii) the supply of search ad inventory to advertisers; and (iv) the supply of ad tech services to publishers and advertisers.

The supply of web browsers

4.4 Web users use web browsers to access and interact with online content and make purchases. In the context of its concerns about the potential imposition of unfair terms on Chrome web users, the CMA has considered whether users could use alternatives. Although users can access some online content through different channels (eg apps), for which there might be a degree of substitutability with web browsers (particularly on mobile devices), users cannot access the vast majority of online content through these other channels.

4.5 The CMA has also considered whether page views generated on web browsers are an important 'input' into the production of ad inventory by publishers and ad tech providers operating in the open display segment. Some publishers have no alternative to web pages to make their content available to web users and generate ad inventory. Other publishers can make their content available through different channels (eg apps), but they have little control over which channel is used by web users, and it is unlikely that they could operate without making their content available on web pages altogether. As a result, publishers would not be able to respond to a deterioration in the functionalities of browsers by steering their audience on to apps or other channels.

4.6 Therefore, in the context of the Investigation, the CMA's preliminary view is that the relevant product market is no wider than that for the supply of web browsers.

4.7 The CMA has not concluded on whether it is necessary to segment this market further, for example by distinguishing between browsers and page views generated on different types of devices.

4.8 The CMA's preliminary view is that the relevant geographic market for the supply of web browsers, when viewed from the perspective of the page views they generate, is likely to be the UK. This is because, from the perspective of advertisers seeking to reach a UK audience, and from the perspective of publishers and ad tech providers seeking to meet this requirement, page views generated abroad are not a substitute for page views generated in the UK. However, the CMA has not concluded on whether the relevant geographic market should be widened, insofar as some advertisers might have a preference for running some campaigns on a global scale. Further, the CMA has considered that web users might access web browsers on a global scale but has not concluded on the exact geographic scope of the relevant market.

The supply of display ad inventory and search ad inventory to advertisers

4.9 Advertisers can reach web users through either search or display advertising. As set out in paragraph 3.18 above, the display advertising market comprises two channels: the owned and operated channel and the open display channel. In the Market Study, the CMA found that advertisers largely saw the owned and operated and open display channels as substitutes, but that there was currently more limited substitutability between search and display advertising.[25]

4.10 The CMA considers that, for the purposes of this Investigation, the relevant product market is likely to be that for the supply of display ad inventory to advertisers. However, the CMA considers that Google's position in the separate market for search advertising is also relevant for the purpose of assessing Google's incentives and the competitive effects of its proposals.

4.11 If Google's Proposals have the effect of reducing the attractiveness of display advertising to advertisers (eg by making display advertising less effective or more expensive), then some advertisers are likely to move some of their activity towards search advertising. In its Market Study the CMA found that, while there is currently limited substitutability between

[25] Market Study, paragraph 5.23.

search and display advertising, there is some evidence of convergence between the characteristics of these two channels at least for some types of advertisers. In a scenario where Google's Proposals reduce the attractiveness of display advertising, some advertisers might switch a share of their purchases to search advertising. For these reasons, while the CMA continues to consider that the search and display advertising markets are distinct, it also considers that Google's position in the search advertising market is relevant for the purpose of assessing its incentives with respect to any changes in the functionalities on Chrome.

4.12 The CMA's preliminary view is that the relevant geographic market for the supply of ad inventory to advertisers is the UK. This is because many advertisers are likely to seek to reach an audience on a UK basis.

The supply of ad tech services to publishers and advertisers

4.13 Advertisers and publishers rely on a range of ad tech intermediaries to select an ad to be served to a web user in real time and determine the price of doing so (as well as delivering related functionalities such as frequency capping, verification, and attribution). As set out in paragraphs 3.19 to 3.21 above, SSPs and publisher ad servers are the main types of ad tech intermediaries on the supply side, and DSPs are one of the main types of intermediaries on the demand side. Generally, services provided by different types of ad tech intermediaries vary but are complementary. The CMA considers that, for the purpose of assessing the competitive effects of Google's Proposals on the market for display advertising, it is appropriate to consider a market for ad tech services to publishers and advertisers.

4.14 Many ad tech providers operate internationally. However, the conditions of competition may vary across countries depending on regulations and market conditions.

4.15 The CMA considers that the relevant geographic market for the supply of ad tech services to publishers and advertisers is likely to be the UK but has not concluded on the precise scope of the relevant geographic market.

Google's position in the relevant markets

4.16 The CMA is of the preliminary view that Google has held a dominant position in the market for the supply of web browsers in the period covered by the Investigation (from January 2019 to date).

4.17 The CMA considers that the following factors are indicators that Google holds a dominant position in the market for the supply of web browsers: (i)

the market share of Chrome; (ii) the market share of other web browsers based on Chromium; (iii) the lack of other options for publishers, ad tech providers and web users; and (iv) the tendency of developers to optimise their pages for Chrome.

4.18 In the context of the Investigation a substantive question is whether the page views and user data generated by browsing on Chrome are an important 'input' into the generation of ad inventory by publishers and ad tech providers operating in the open display segment. Another relevant question is the extent to which different web browsers are able to capture web users' attention. Chrome's share of page views can be used as the starting point for considering these two substantive questions.

4.19 As discussed in paragraphs 4.7 and 4.8 above, the CMA has not yet concluded on whether the relevant product market for the supply of web browsers should be segmented by type of device, or on whether the relevant geographic market should be wider than the UK. Table 4.1 and Table 4.2 below set out shares of page views for different browsers on different types of devices in the UK and worldwide, respectively. This shows that, in the period covered by the Investigation, Chrome's share of page views across all devices has been consistently high (around 49% over the period) and significantly higher than that of its nearest competitor, Safari. There has been no material change to Chrome's share since the end of Q1 2021.

Table 4.1: Browser shares based on page views in the UK

		2019			2020			Q1 2021		
Browser	Browser engine	All devices (%)	Desktop (%)	Mobile (%)	All devices (%)	Desktop (%)	Mobile (%)	All devices (%)	Desktop (%)	Mobile (%)
Chrome	Chromium	48.9	63.2	40.4	49.0	60.0	41.5	49.0	59.2	40.5
Safari	WebKit	31.6	10.4	47.0	33.6	16.8	47.4	33.5	17.4	48.6
Samsung	Chromium	4.3	0.0	10.3	4.3	0.0	9.3	4.0	0.0	9.0
Firefox	Gecko	4.2	8.2	0.5	3.5	6.9	0.6	2.9	5.4	0.7
Edge	Chromium	4.7	9.4	0.1	5.4	11.0	0.2	6.4	13.2	0.0
Internet Explorer	Trident	3.3	6.9	0.2	1.5	3.1	0.0	0.9	1.7	0.0
Android	Chromium	1.3	0.0	0.4	1.1	0.0	0.2	1.0	0.0	0.1

Opera	Chromium	0.8	1.4	0.4	0.8	1.4	0.4	1.0	1.6	0.4
Others		0.9	0.7	0.6	0.8	0.8	0.5	1.2	1.4	0.6

Note: the column 'browser engine' reports the browser engine for the PC or Android versions of the browsers. The CMA understands that the iOS versions of some of these browsers rely on WebKit and as such may offer different functionalities in terms of user tracking and support for TPCs.
Source: Statcounter

Table 4.2: Browser shares based on page views worldwide

		2019		2020				Q1 2021		
Browser	Browser engine	All devices (%)	Desktop (%)	All devices (%)	Desktop (%)	Desktop (%)	Mobile (%)	All devices (%)	Desktop (%)	Mobile (%)
Chrome	Chromium	63.3	70.0	60.1	64.6	68.7	62.5	63.8	66.7	62.7
Safari	WebKit	15.9	6.8	20.8	17.8	9.0	24.1	19.2	10.3	24.9
Samsung	Chromium	3.5	0.0	6.9	3.4	0.0	6.5	3.4	0.0	6.2
Firefox	Gecko	4.6	9.5	0.4	4.2	8.7	0.5	3.7	8.1	0.5
Edge	Chromium	2.1	4.5	0.1	2.8	6.0	0.1	3.4	8.0	0.0
Internet Explorer	Trident	2.2	4.9	0.2	1.4	3.0	0.0	0.8	0.0	0.0
Android	Chromium	0.9	0.0	1.0	0.5	0.0	0.4	0.5	0.0	0.2
Opera	Chromium	2.6	2.4	2.9	2.0	2.4	1.7	2.2	2.6	1.9
Others		5.0	1.9	7.8	3.3	2.2	4.3	1.8	4.3	0.7

Note: the column 'browser engine' reports the browser engine for the PC or Android versions of the browsers. The CMA understands that the iOS versions of some of these browsers rely on WebKit and as such may offer different functionalities in terms of user tracking and support for TPCs.
Source: Statcounter

4.20 Google's browser shares are even higher (around 76% across all devices in Q 1 2021) if all Chromium-supported browsers are taken into account. The CMA has received submissions that Chromium is controlled by Google. For instance, changes to the Chromium source code made by an external contributor (ie someone who has not already been granted write access) are subject to a review process that ultimately involves only reviewers who work for Google, and all contributors must enter into a contributor licence agreement with Google. Google has told the CMA that the Chromium source code is provided under a permissive open source licence, implying that other browsers are in principle free to choose whether to implement changes introduced by Google. In practice, other browsers may do this by forking (creating their own copy of) Chromium that they are free to make changes to (without Google reviewers) and use in their

browser. However, the forked version of Chromium would not enjoy the ongoing updates and improvements that the original Chromium gets from that point forwards, and the browser that forked would have to maintain their new copy of Chromium themselves. In view of this, market participants have told the CMA that not adopting changes is likely to be costly to the developers of these browsers, and as such the CMA's preliminary view is that changes to Chromium influence the functionalities provided by these browsers as well.

4.21 The CMA also considers that the market share estimates presented in the tables above may significantly underestimate the importance of the page views generated on Chrome for publishers and ad tech providers. In particular, Apple and Mozilla have already taken steps to limit the functionalities of TPCs in their browsers (Safari and Firefox, respectively). As such, page views generated on these browsers do not appear to be an effective substitute for page views generated on Chrome for the purpose of generating high quality ad inventory where web users can be identified and associated with data. In the Market Study, the CMA found that the value of ad inventory on Safari and Firefox had dropped significantly below the value of equivalent ad inventory on Chrome, following Apple's and Mozilla's implemented changes to the functionalities of TPCs.[26] If browsing on Safari and Firefox were to be excluded from the relevant market, then Chrome's share of page views in the UK across all devices would increase further.

4.22 The CMA considers that entry and expansion in the market for the supply of web browsers is made difficult by high development costs, pre-installation arrangements, and default choice architectures. Consistent with these market features, new browsers introduced recently such as Brave or Edge are based on existing browser engines and have achieved only small market shares. Therefore, the CMA considers that barriers to entry and expansion in the market for the supply of web browsers are likely to be high.

4.23 Publishers and advertisers have little control over which browser is used to access their content or purchase their products. That choice is made by web users based on a combination of hardware and software considerations. Thus, publishers and ad tech providers have no countervailing buyer power.

4.24 Moreover, some market participants have told the CMA that developers often optimised their web pages (including many of Google's own web

[26] Appendix F of the Market Study presents evidence from three publishers indicating that they generate substantially lower revenue per page across Safari and Firefox compared to other browsers where TPCs are still enabled. Market Study, Appendix F, paragraphs 120 – 121.

pages) for Chrome specifically, with the result that many web pages 'worked best' with Chrome and would break or not render correctly in other browsers. Chrome frequently implements new web features that become de facto web standards, before the relevant standard setting body has adopted the standard. This further indicates that Chrome has a significant degree of market power.

4.25 For these reasons, the CMA considers that Google is likely to be dominant in the market for the supply of web browsers in the UK (and would also be likely to be dominant if the market were wider than the UK).

4.26 While Google's position in the supply of web browsers is central to the Investigation, Google also has a strong position in many of the advertising markets that will be affected by the Privacy Sandbox changes. In particular, as set out at paragraphs 3.17 to 3.21 above, and in the Market Study, Google also has a strong market position in:

(a) search and search advertising, with a share of supply in the UK in excess of 90%;[27]

(b) display advertising, including through YouTube which has a share of video display advertising in the UK of [15-20]%;[28] and

(c) markets for ad tech intermediation, including a share of supply of more than 90% in publisher ad serving in the UK.[29]

[27] Market Study, Appendix C, paragraphs 27 and 97.
[28] Market Study, Appendix C, paragraph 187.
[29] Market Study, Appendix C, paragraph 244.

5. The CMA's competition concerns

5.1 This section summarises the CMA's concerns regarding the impact of the Privacy Sandbox Proposals on competition and consumers.

5.2 The factual situation under consideration includes announcements of future conduct. In light of case law under the Act concerning such announcements,[30] the CMA has taken a two-part approach to summarising its competition concerns. First, the CMA has set out its preliminary view that the announced conduct, if implemented without regulatory scrutiny and oversight, would be likely to amount to an abuse of a dominant position. Second, the CMA has set out its preliminary view that the announcements themselves and implementing steps taken to date are likely to constitute an abuse in the specific circumstances of the case.

5.3 The CMA is concerned that Google's Proposals, if implemented without the regulatory scrutiny and oversight provided for by the Proposed Commitments, would be likely amount to an abuse of a dominant position in the market for the supply of web browsers in the UK. More specifically, the CMA is concerned that, without the Proposed Commitments, Google's Proposals would allow it to:

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

(b) self-preference its own ad inventory and ad tech services by transferring key functionalities to Chrome, providing Google with the ability to affect digital advertising market outcomes through Chrome in a way that cannot be scrutinised by third parties, and leading to conflicts of interest; and

(c) exploit its apparent 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.

5.4 The precise impact of the Privacy Sandbox Proposals will depend on the ways in which they will be designed and implemented, neither of which has yet been decided.

5.5 The CMA is also concerned that certain announcements made by Google with respect to the Privacy Sandbox Proposals are themselves likely to

[30] *Royal Mail plc v Office of Communications* [2019] CAT 27.

amount to an abuse of a dominant position in the market for the supply of web browsers in the UK in the specific circumstances of the case. In addition, the CMA's preliminary view is that Google has already started to implement its changes, and that where such implementation pre-empts the outcome of consultations, it risks not being competition on the merits.

5.6 More specifically, the CMA is concerned that Google's announcements to date, as it develops these proposals, 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 to date have shown (and created the expectation) that Google is 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. This uncertainty and concerns around Google strengthening its market position are likely to already be causing harm to Google's rival publishers and ad tech providers which rely on TPCs to perform their functions and compete with Google resulting in a lessening of competition over Google's activities in display advertising.

5.7 In this respect, the CMA considers that the concerns that market participants have expressed to it regarding the impact that the Privacy Sandbox Proposals are likely to have on competition reflect in part:

(a) 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

(b) a lack of confidence on the part of third parties regarding Google's statements concerning its intentions in developing and implementing the Privacy Sandbox Proposals. The CMA understands that this lack of confidence in part reflects the commercial incentives that Google faces in developing Google's Proposals and the lack of independent scrutiny of Google's Proposals and the process for their development.

5.8 The remainder of this section sets out:

- first, a summary of the Privacy Sandbox Proposals;
- second, the effects that the Privacy Sandbox Proposals would likely have on competition and consumers if they were

introduced without the regulatory scrutiny and oversight provided by the Proposed Commitments; and

- third, the impact that Google's announcements to date are likely to have on competition.

Summary of the Privacy Sandbox Proposals

5.9 The Privacy Sandbox Proposals are a set of proposed changes on Chrome that aim to:

- remove the cross-site tracking of Chrome users through TPCs and other methods of tracking such as fingerprinting; and
- create a set of alternative tools to provide the functionalities that are currently dependent on cross-site tracking.

Functionalities currently dependent on or associated with cross-site tracking

5.10 Currently TPCs and other forms of cross-site tracking serve a range of purposes within digital advertising markets and the broader operation of the open web. These include:

(a) Ad targeting, in particular **interest-based targeting** and **retargeting**: TPCs and other forms of cross site tracking allow for interest-based user profiles to be established and users to be targeted with ads corresponding to their profile (interest-based targeting). Cross-site tracking is also used to allow advertisers to retarget customers that have previously visited their website for remarketing purposes.

(b) **Measurement, attribution, frequency capping, and reporting**: Cross site tracking is also used to determine whether and how many ads have been served successfully to users (measurement), to help assess ad effectiveness by determining whether views and clicks on ads 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 outcomes of ad auctions to advertisers and publishers to facilitate payment and show performance of contracts.

(c) **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.

(d) **Federated log-in:** Allows the user to use a single method of authentication (eg 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 thereafter.

5.11 In addition, other important forms of web functionality, while not dependent on cross-site tracking, currently require the provision of information that is sometimes used to facilitate cross-site tracking. An example is the information provided through the user-agent string which provides information about the user's browser and device to the website that the user is visiting and which is useful 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). A further example is the Internet Protocol ('**IP**') address, which is useful for **detecting fraud and the geographical tailoring of content**.

Alternative tools to replace TPCs and other forms of cross-site tracking

5.12 Google has proposed a range of alternative tools to provide the functionalities set out above as a substitute for the use of TPCs and certain information associated with other forms of cross-site tracking. These tools are at different stages of development and none has been finalised. The key proposals are summarised here and described in more detail in Appendix 2.

First-Party Sets

5.13 Under the Privacy Sandbox Proposals, First-Party Sets are a mechanism by which a set of domains can be declared as belonging to the same party and thus be considered 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 be possible. Google has indicated that corporate ownership is a factor which could determine the boundaries of First-Party Sets.[31]

*Federated Learning of Cohorts ('**FLoC**')*

5.14 The FLoC proposal is aimed at allowing interest-based ad targeting by allowing market participants to target particular interest groups (cohorts). Under the FLoC proposal, the browser assigns itself to a cohort of users with a similar browsing history (as currently proposed, over seven days).

[31] Chrome Developers, Progress update on the Privacy Sandbox initiative, January 2021.

When accessing a web page, the browser sends a specific cohort ID to the website. Publishers can include these cohort IDs in their ad requests to target ads to a cohort.

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

5.15 Retargeting is the practice of serving targeted ads to specific individuals who have visited an advertiser's website. There have been a number of different proposals put forward by Google and other market participants aimed at allowing advertisers to retarget users, while preventing cross-site tracking.

5.16 Under the TURTLEDOVE/FLEDGE proposal, the advertiser's website asks visiting browsers to join one or more interest groups. The browser stores relevant information which allows it to run an on-device auction when it encounters an opportunity to display an ad on a different website.[32] The auction logic is determined by the seller (publisher) and buyers with eligible interest groups (the advertiser or its DSP) can bid, uploading information to a 'trusted' key-value server in advance. The browser executes each interest group's bidding logic. The governance and technical guarantees of the 'trusted' key-value server have yet to be fully developed.

5.17 Under the proposal, the winning interest-group ad is shown in a 'Fenced Frame'. The 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 to the website.[33] Google is exploring the development of a mechanism to allow sellers and bidders to learn the outcome of the auction in a way that does not reveal the interest group to visited websites (see paragraph 5.19 below).

Event Conversion Measurement API

5.18 This proposal is currently aimed at allowing last-click attribution.[34] The API allows the advertisers to attach a set of metadata (including intended conversion destination) to their ads. This data is stored by the user's browser when the ad is clicked. If the user visits the intended destination and converts, the browser records the conversion event and, with a delay,

[32] For each interest group, the browser stores information about who owns the group, JavaScript code for bidding logic, and how to periodically update that interest group's attributes.
[33] Fenced Frames are still under development.
[34] Last click attribution means that the credit for the conversion is given to the website hosting the ad that was last clicked before the conversion. All other ad clicks or views before the conversion are given no credit.

sends a report to the publisher and advertiser that a conversion occurred, without the inclusion of any information about the user. In addition to limiting the information available about the conversion event so that the conversion cannot be used to collect data about the user, the browser will add noise to the conversion. In the current proposals this means the browser would report random instead of actual conversion data 5% of the time.

Multi-browser aggregation service, Aggregate Conversion Measurement API, and Aggregated Reporting API

5.19 Google is also exploring development of a 'multi-browser aggregation service', a mechanism that could aggregate information from multiple sources without the entity performing the aggregation learning the underlying data from each source.[35] This service is intended to overcome the limitations of the Event Conversion Measurement API in that it could share more granular data if this data was aggregated over multiple users' browsers. Such information could facilitate view-through and multi-touch attribution, measuring reach (the number of distinct users that viewed an ad), and allow for a limited form of frequency capping.

Trust Token API

5.20 Websites currently rely on identifiers and cross-site tracking to establish whether a user is trustworthy or engaged in spam or fraud. The Privacy Sandbox Proposals include a proposal for a Trust Token API.[36] This API is intended to allow for trust signals to be transmitted between websites without creating a stable, global identifier unique to each user, by segmenting users in 'trusted' and 'untrusted' categories.

Removal of fingerprinting surfaces

5.21 Privacy Sandbox contains other proposals aimed at mitigating workarounds: methods that market participants can use to continue cross-site tracking without the use of TPCs. These proposals are aimed at combating fingerprinting by removing so-called fingerprinting surfaces.[37]

[35] See Multi-Browser Aggregation Service Explainer.

[36] Google, Trust Token API Explainer, August 2019.

[37] Fingerprinting is the practice of collecting, linking, and using a wide variety of information about the browser, other software, or the hardware of the user, in conjunction, for the purpose of identification and tracking. For an overview of fingerprinting see Market Study, Appendix G, pages 14–19.

User-Agent Client Hints API and Privacy Budget

5.22 A user-agent string provides information about the user's browser and device to the website the user is visiting. This information can be useful for websites (for instance, to select the most suitable version of a website for the user's browser and device, or to monitor for fraud and abuse), but the transmission of this information can also facilitate fingerprinting, by which the user can be identified and tracked. Under the User-Agent Client Hints proposal, the information that is made available to websites via the user-agent string will be minimised. Additional information that the website may require can be requested by a website from the browser. Whether the browser will provide correct information depends on how much information is requested and the website's available Privacy Budget.

5.23 Under the Privacy Budget proposal, the browser will assign an information budget to each website and monitor the information provided to each website. When a website has used up its budget, the browser will stop sending correct information, substituting it with imprecise or noisy results or a generic result. Budget increases for specific information can be requested.

*Global Network Address Translation Combined with Audited and Trusted CDN or HTTP-Proxy Eliminating Reidentification ('**GNATCATCHER**')*

5.24 This proposal aims at reducing the amount of information that websites see during network address translation by looking at the IP address.[38]

5.25 This would be done by allowing a browser to forward its hyper text transfer protocol ('**HTTP**') traffic through an IP privatising server, utilising end-to-end encryption thereby masking a user's IP address from the visited website. In addition, organisations could be required to self-certify that their servers are masking IP addresses when transferring information eg by use of an HTTP header.

WebID

5.26 The WebID proposal aims to prevent federated log-in being used for cross-site tracking, while preserving its intended functionality. At this stage, Google has explored three variations of potential solutions, and it is not yet clear which form the proposal will ultimately take (eg whether the variations complement each other or are mutually exclusive). It could mean that the

[38] The GNATCATCHER GitHub Explainer is set out here. The proposal is based on two previous proposals Near-Path NAT and Wilful IP Blindness.

browser adds more friction (eg in the form of permission prompts) or takes control of choice architecture around the use of federated log-in. It could also mean that website federated log-in systems could delegate a log-in to the browser, effectively making the browser a delegated representative of the identity provider.

Assessment of the likely impact of the Privacy Sandbox Proposals if implemented without regulatory scrutiny and oversight

5.27 This part sets out the CMA's preliminary view on the announced conduct.

5.28 The CMA is concerned that through the Privacy Sandbox Proposals, if implemented without regulatory scrutiny and oversight, Google would be likely to abuse its apparent 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. The following sections explore these concerns.

5.29 Although, as described in more detail below, the CMA is concerned about the impact of the Privacy Sandbox Proposals on Google's rivals, the CMA's remit is to protect the process of competition and the interests of consumers rather than protecting individual competitors.

Concern 1: unequal access to the functionality associated with user tracking

5.30 The CMA's first concern relates to the risk that Google's Proposals will limit the functionality available to its rivals in the open display market,[39] while leaving Google's ability to offer these functionalities relatively unaffected, thereby having a harmful impact on the ability of:

(a) publishers to sell ad inventory to advertisers in competition with Google's ad inventory; and

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

5.31 In the absence of regulatory scrutiny and oversight, the CMA's preliminary view is that this conduct would likely have anti-competitive effects and that using control over Chrome to distort competition in related markets does not amount to competition on the merits.

[39] For example, in terms of the amount of information about a web user that can be associated with an ad request, which facilitates targeting, frequency capping, verification, and attribution, or the other forms of functionality discussed above.

5.32 The Privacy Sandbox Proposals aim to replace TPCs with alternative solutions, while leaving first-party cookies unaffected.[40] TPCs are currently the principal means of achieving common identification of web users on web pages and are therefore a fundamental building block of the open display advertising used by publishers and ad tech providers. While publishers and ad tech providers depend on TPCs to collect information about web users and provide it to advertisers to target advertising and carry out related functionalities such as measuring conversions, Google could use first-party cookies to perform these functionalities in competition with publishers and ad tech providers.[41]

5.33 Although rivals can also use first-party data to provide digital advertising services (as the CMA found in the Market Study), their reach and the quality of their data is in many cases much more limited compared to that of Google. The extensive reach of Google's user-facing services and its ability to connect data with greater precision (because of its large base of users logged into their Google account) provide Google with a significant data advantage over others.[42]

5.34 In the absence of the Proposed Commitments, Google's 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". [43]

5.35 In the context of discussing potential solutions, the marketing material suggests: "Invest in a comprehensive first-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,

[40] What will be regarded as a first-party cookie depends on the definition given to first-party under the First-Party Set proposal, see paragraph 5.13 above.
[41] 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 third-party cookies, and would become unavailable after TPC removal.
[42] Market Study, Appendix F, paragraphs 52 to 63 and Appendix M, paragraphs 307 to 314.
[43] Google, Think with Google: The marketer's playbook for navigating today's privacy environment, July 2020, page 5.

and support all of Google's advertising and measurement products, including Google Ads, Google Analytics, Campaign Manager, Display & Video 360, and Search Ads 360".[44] Further, on a 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".[45]

5.36 Google's statements therefore suggest that removing TPCs, taken by itself, would likely reduce the effectiveness of open display advertising compared to that of advertising provided by Google. 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 which cannot sell personalised advertising when competing with those who can.[46]

5.37 Overall, the CMA's concern is that, in the absence of regulatory scrutiny and oversight, the removal of TPCs, and the Privacy Sandbox Proposals more generally, are likely to worsen various aspects of the quality of advertising (including targeting, frequency capping, verification and attribution) that rival publishers and ad tech providers can offer to advertisers and publishers, compared to that offered by Google. The following sections break down this overarching concern into two components:

(a) that the Privacy Sandbox tools will not be effective substitutes for the different forms of functionality provided by TPCs and other information deprecated by the Privacy Sandbox Proposals; and

(b) that Google will not be as affected by this as third parties because of its advantageous access to first-party user data.

Concerns relating to the effectiveness of the Privacy Sandbox tools

5.38 The CMA is concerned that the new tools being developed through the Privacy Sandbox Proposals will not be effective substitutes for the functionalities provided by TPCs and other information deprecated by the

[44] Google, Think with Google: The marketer's playbook for navigating today's privacy environment, July 2020, page 7.
[45] Why conversion measurement will be crucial - Think with Google, dated August 2020.
[46] 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.

Privacy Sandbox Proposals. The following sections summarise the concerns made known to the CMA in relation to some of the key new tools currently being developed as part of the Privacy Sandbox Proposals.

FLoC

5.39 As noted above, Google's interest-based targeting proposal (FLoC) would replace individualised personalised advertising with advertising to cohorts of users, which would be collated by Chrome by aggregating groups of users together on the basis of similar browsing habits. Advertisers would not be able to add information about a specific web user to this 'group-level' data, unless they are able to recognise and identify web users by other means, such as publishers requiring web users to log in and market participants sharing (on the server-side) other identifiers like email addresses.

5.40 Therefore, although the Privacy Sandbox 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 Google's Proposal as the audience would be determined by Google. Several market participants raised this concern in discussions with the CMA, saying that this is likely to lead to a homogenisation of ad inventory and ad tech services and would reduce the ability of rivals to provide a value proposition.

5.41 In the absence of the Proposed Commitments, Google could advantage itself in several ways. For example, Google's DSPs could be better able to interpret and form relevant inferences from users' cohort IDs than rival DSPs by associating users' 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 cohorts of web users identified by the browser to advantage itself when bidding on open display ad inventory. These concerns were raised by several market participants in discussions with the CMA.

TURTLEDOVE, FLEDGE and Fenced Frames

5.42 Similarly to FLoC, Google's retargeting proposal would give Chrome full and unique visibility of the interest groups to which users belong and the responsibility for joining these interest groups. Retargeting of individual

users on the basis of their own interests would be substituted by retargeting of groups of users who share similar interests. Google would determine the minimum size of these interest groups and, in so doing, rival publishers and ad tech providers would not be able to compete to offer their unique value proposition to advertisers. This would 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. This is further explained in the section below.

5.43 We have also heard a number of concerns about the Fenced Frame proposal, which Google is proposing to introduce in order to prevent the webpage on which an ad is shown from learning about the contents of the frame, to ensure this information cannot be used to track users. First, we have heard that this proposal could lead to brand safety concerns, by preventing the publisher from knowing what types of ad content is being rendered on its website, and preventing the advertiser from knowing on which publisher inventory its ad content is being placed. Second, we have heard that Fenced Frames may limit the ability of publishers to control, measure, and optimise content on their websites.

Reporting and Measurement APIs

5.44 The measurement and reporting data available to third parties under this proposal is more limited than under the current framework using TPCs. Following the implementation of the Privacy Sandbox Proposals, advertisers and the ad tech providers which act on their behalf would receive aggregated data at various intervals, rather than individual-level data in real time as is currently possible through TPCs. This would limit rival ad tech providers' ability to demonstrate the effectiveness of their services to advertisers and optimise their campaign spend. The CMA has also heard that none of the Privacy Sandbox 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

5.45 Google has put forward a number of proposals aimed at combating 'fingerprinting' by reducing the amount of identifying information which is

passed on to websites up until their attributed Privacy Budget is exhausted. However, much of the information that could be used in fingerprinting 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.

5.46 Specifically, the CMA has heard 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 has heard 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 (as a result of the User-Agent Client-Hints proposal) or a user's geographic location (as a result of the GNATCATCHER proposal).

WebID

5.47 As noted above, Google is exploring several variations of the WebID proposal, which aims to prevent federated log-in being used for cross-site tracking. Under one variant, the browser would provide warnings and consent notices to the user when a tracking risk appears.[47] A concern we have heard is that this could add friction to the user experience and lead to user frustration, reducing user visits. We have also heard that some variations might lead to the disintermediation of publishers with harmful consequences for their ability to track users on their properties.

Concerns relating to Google's data advantages

5.48 The CMA has heard concerns from several third parties that, should the Privacy Sandbox tools not prove to be effective substitutes for the functionality of TPCs and other information deprecated by the Privacy Sandbox Proposals, this will distort competition in digital advertising markets since Google will retain the ability to carry out the functionality affected through the use of first-party data.

5.49 An important aspect of these concerns is the precise definition that will be used to distinguish between third-party domains (tracking of users across which will be restricted under Google's Proposals) and first-party domains (tracking across which will be unaffected by Google's Proposals). As discussed above, First-Party Sets are a mechanism under the Privacy

[47] Further information on this 'permission-oriented' variation can be found on the WebID Github pages here and here.

Sandbox Proposals by which a set of domains can be declared 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 be possible.

5.50 Google has indicated that corporate ownership is a factor which could determine the boundaries of First-Party Sets. Such a definition would in principle give Google, which owns a very wide range of domains and user-facing services, the ability to track users extensively for the purposes of digital advertising.[48]

5.51 These concerns also stem from the extensive reach of Google's user and business-facing products and services, some of which, such as Chrome, are extensively used by web users to reach rival publishers' websites. Google's ability, following the implementation of the Privacy Sandbox Proposals, to share data collected from these services and use it for advertising purposes, could distort competition in digital advertising markets.

5.52 Table 5.1 below sets out the CMA's understanding of the main data sources which Google could continue to be able to use (whether or not it currently does so), in the absence of the Proposed Commitments, for digital advertising purposes (including targeting and measurement), on its owned and operated ad inventory, and on third-party non-Google ad inventory through its ad tech services, following the implementation of the Privacy Sandbox Proposals.

Table 5.1: Google's sources of user data that could be used for digital advertising purposes

Sources of data about web users' activities	Ad inventory for which data could be used
Google's user-facing services, including Android (eg data collected from Google Search).	Google owned and operated ad inventory (eg data from Google Search used to target ads on YouTube) and third-party web page ad inventory through Google ad tech services
Data uploaded via Customer Match.	Google owned and operated ad inventory.
Third-party web pages via Chrome browsing history synced with Google Account Web & App Activity.	Google owned and operated ad inventory, third-party web page ad inventory through Google ad tech services
Third-party web pages via Google analytics tools for businesses.	Google owned and operated ad inventory, third-party web page ad inventory through Google ad tech services.

Source: CMA analysis

[48] Competition and data protection in digital markets: a joint statement between the CMA and the ICO, May 2021, paragraphs 76-82.

5.53 Each of these data sources and uses is considered below.

Use of Google first-party data for advertising

5.54 In the absence of the Proposed Commitments, Google could use first-party data collected from web users to provide digital advertising services on its owned and operated properties and, through its ad tech providers, on third-party ad inventory.

5.55 In relation to first-party ad inventory, Google has confirmed that currently, subject to web user consent, the activity of web user A on Search can inform ads and related functionalities shown to web user A on YouTube.[49] When web users are logged into their Google accounts, Google would continue to use the activities of, say, user A on a device X on Search to target and carry out attribution in relation to the same user but on a different device and on another service, say, YouTube. When users are not logged into their Google accounts, Google could combine data collected from one service to target the same user on another service but on the same device.

5.56 In relation to third-party ad inventory, Google has told the CMA that, because of Google's own internal policy restrictions, Google Ads and DV360's use of Google first-party data to target ads when bidding on exchanges for non-Google display ad inventory is currently extremely limited. However, Google's privacy policy acknowledges that such targeting is possible, depending on a user's settings, and includes some examples of Google using first-party data to influence choice of ads on third-party ad inventory.[50]

5.57 The CMA further notes that, during the Market Study, in relation to Google's TPCs experiment on display ads served by Google's ad tech services on non-Google sites, Google stated that the data from the experiment does not cover traffic where the user was logged into a Google Account and Google's systems made full use of the user profile information via the Google log-in ID to supplement and enhance the information associated with the cookie.[51] Google noted further: "[t]he use of user

[49] Google has said that, in adherence to its own policy, it does not use web user data from Gmail, Translate, Drive, Photos or Google Fit for advertising purposes.
[50] Google, Privacy Policy, September 2020. For example: "For example, if you watch videos about baking on YouTube, you may see more ads that related to baking as you browse the web" or "Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for 'mountain bikes', you may see an ad for sports equipment when you're browsing a site that shows ads served by Google".
[51] Market Study, Appendix F, paragraph 148 and footnote 47.

signed-in data for display advertising is not fully launched, and Google is at the stage of applying this functionality to 75% of traffic as of September [2019]".[52]

5.58 From the above, the CMA infers that, for a material portion of traffic handled by Google's ad tech services, in the absence of the Proposed Commitments, Google could use its first-party data to provide digital advertising services such as targeting and attribution on both first and third-party display ad inventory.[53] Further, CMA discussions with market participants suggest that there is a widely held view that Google does or could combine data in this way. While Google has told the CMA that Google currently makes 'extremely limited' use of first-party data when bidding on exchanges for third-party ad inventory, Google retains the ability to do so through its privacy policies.

Use of third-party data uploaded via Customer Match for advertising

5.59 In the absence of the Proposed Commitments, Google could continue to allow advertisers to upload their own first-party customer data and match this against Google users 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.[54]

Use of Chrome browsing history data for advertising

5.60 In the absence of regulatory scrutiny and oversight, the CMA is concerned that, while third parties would be unable to effectively track individual web users on Chrome following the implementation of the Privacy Sandbox Proposals, Google itself would retain that ability. In particular, 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 could combine any declared age and gender information from a web user's account with his/her Chrome data to offer personalised advertising to advertisers and publishers when acting as an ad tech provider or selling ad inventory.

5.61 On its Safety Centre web page, Google states that "[p]artner websites and apps use your online activity to create ads that are more useful to you …

[52] Market Study, Google's response to the CMA's follow-up questions from Google's response to Question 18 of the CMA's Request for Information dated 10 October 2019.
[53] Google has told the CMA that it could only do this after some engineering investment.
[54] Google Ads Help, About Customer Match.

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".[55] This and Google's current approach to signed-in users indicate that Google has the capacity to track at least some individual Chrome web users in a way that is not contingent on TPCs, and that, in the absence of the Proposed Commitments, could continue to do so in a way that is likely to give Google a significant advantage over rival ad tech providers and publishers. Several market participants have raised this as a concern in discussions with the CMA.

5.62 Although Google has told the CMA that Google intends to make use of the alternative technologies developed in the context of the 'Privacy Sandbox' to power key ads functions that currently rely on TPCs, it is unclear whether this would be to the exclusion of additional data that Google could gather through Chrome. Moreover, the CMA understands that this intention is a matter of company policy rather than the reflection of hard technical or legal barriers, and, in the absence of the Proposed Commitments, Google could unilaterally reverse this policy as it did in the past when it changed its privacy policy to permit, with user consent, the combination of activity from websites that use Google's advertising services with account data from logged-in Google users.[56]

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

5.63 Google provides a number of analytics tools to websites to understand their traffic. For instance, Google Analytics is used to track site activity, such as session duration, pages per session and bounce rates of individuals visiting the site, and information on the source of traffic.

5.64 Google has stated that it only uses data from Google Analytics for its own purposes if the customer has enabled data sharing with Google.[57] Some market participants have told the CMA that, in the absence of regulatory scrutiny and oversight, Google could use its analytics tools to collect first-party data and use it for advertising purposes, both on its owned and operated ad inventory and for third-party non-Google ad inventory, through its own ad tech providers.

[55] Google Safety Centre, Your Privacy: Ads and Data, accessed on 4 February 2021.
[56] Market Study, Appendix F, paragraph 133.
[57] Market Study, Appendix F, footnote 17.

Preliminary view on Concern 1

5.65 Several market participants have told the CMA that Google's ability to combine data from a range of sources would give Google a significant advantage over its rivals. In particular, while the removal of TPCs and the implementation of the Privacy Sandbox Proposals would impede rivals from combining individual-level data across the web, it is claimed that this would be largely unchanged for Google within its ecosystem.

5.66 Overall, the CMA's preliminary view is that the removal of TPCs and information deprecated by the Privacy Sandbox Proposals and the implementation of the Privacy Sandbox Proposals, without regulatory scrutiny and oversight, would likely foreclose rival publishers and ad tech providers by worsening the quality of the ad inventory that they can offer to advertisers in the open display market, while having no or limited impact on the quality of Google's ad inventory and Google's ad tech services to advertisers and publishers. This would give Google a significant competitive advantage over rival publishers and ad tech providers operating in the open display market. As discussed in paragraph 4.11 above, this might also lead to some advertisers moving a share of their budgets from display to search advertising, to the benefit of Google which has more than a 90% share of this market in the UK.

5.67 While Google has stated that, as a matter of internal policy, it does not share data collected from certain of its web user and/or business-facing services for the purposes of providing advertising on its owned and operated or third-party ad inventory, the CMA understands that these internal restrictions are not based on technical or legal barriers and, therefore, in the absence of the Proposed Commitments, could be changed by Google in the future.

Concern 2: self-preferencing Google's own ad tech providers and owned and operated ad inventory

5.68 The CMA's second concern relates to the role of Chrome under the Privacy Sandbox Proposals in deciding which ads to show to a given web user. Google owns Chrome, while at the same time operating as a publisher and as an ad tech provider. In the absence of the Proposed Commitments, this is likely to lead to conflicts of interest, whereby Google may have 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. The existence of these conflicts of interest is also likely to affect Google's incentives on how to engage with the industry and take on board any suggested alternative

solutions to the Privacy Sandbox Proposals which could minimise or eliminate 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.

5.69 The Privacy Sandbox Proposals would move some of the functions currently performed by ad tech providers (DSPs, SSPs and/or the publisher ad server) to Chrome. In the absence of regulatory scrutiny and oversight, this would give Google the opportunity to leverage its likely dominant 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 compared to rivals (eg reduced latency), or Google could use its control over the device on which the auction will take place (eg Android devices) to grant its own services a technical advantage in the form, for example, of additional processing power.

5.70 The CMA is also concerned that the new tools being developed through the Privacy Sandbox Proposals could be used by Google to self-preference its own advertising services. The following sections summarise some of the concerns that the CMA has heard in relation to how some of these tools could be used in such a way.

FLoC

5.71 Currently, market participants analyse and draw their own inferences from users' browsing histories using TPCs and other identifiers which they use to target digital advertising and provide related functionalities. Under the most recent Privacy Sandbox Proposals, this would change as advertisers, publishers and ad tech providers would face restrictions on using certain identifiers that are often used for cross-site tracking. They would instead have access to cohort IDs (from FLoC) which Google Chrome would create by assigning users to cohorts on the basis of their similar browsing habits. By being the only entity to be able to track users and responsible for determining the cohorts to which users belong and broadcasting them to rivals, Chrome would be in a gatekeeper position for the ad tech ecosystem. The CMA has heard concerns that the way in which Google would define cohorts would be a black box which could give Google the ability to self-preference its own advertising businesses.

5.72 In addition, there are design uncertainties in the FLoC whitepaper that might lead to self-preferencing. One is whether Google intends to make cohort interest profiles publicly available or not. If not, and if Google itself is able to use these cohort interest profiles in its advertising businesses, other

market participants may not know what defines a cohort, so a cohort ID might be less useful to them than to Google.

5.73 Even if it is made public, the nature of the definition may be less transparent in nature to other players.[58] Finally, if data dependencies to FLoC are proprietary to Google, cohort IDs may be less useful to other market participants.

TURTLEDOVE and FLEDGE

5.74 In the current ecosystem, DSPs apply their own bidding logic to determine what bid to return (if any) to a bid request. Under the Privacy Sandbox Proposals, this could change in the case of retargeting. For this use case, DSPs would share part of their bidding logic with the browser, which would then execute it when a retargeting opportunity arises. This would introduce new opportunities for conflicts of interest, as Google (which operates the browser) would know how its rival DSPs would bid on retargeting opportunities. Should this information be shared with its own DSP, it could provide a significant advantage as Google would have visibility of its competitors' bidding strategies. Google could also benefit from having access to additional or higher quality data, such as reporting data in TURTLEDOVE auctions. These are concerns that some market participants expressed in discussions with the CMA.

5.75 The CMA notes that Google has refined its proposal for retargeting, where a 'Trusted Server' will be responsible for storing some of the information about a campaign's bid and budget.[59] However, some market participants have told the CMA that, although the 'Trusted Server' could give ad tech providers more control than under the previous version of this proposal, if this was placed under Google's control there would still be room for conflicts of interest to arise and for Google to favour its own operations over those of its competitors.

Reporting and Measurement APIs

5.76 The important activity of reporting to advertisers and media agencies on ad campaign performance, including measurement and attribution, is currently carried out by the advertiser ad server. Under the Privacy Sandbox

[58] If, for example, a cohort interest profile is defined as the top 10 topic categories as in the final test in the FLoC whitepaper. Although Google makes public a list of topic categories, the ground truth on a topic category is proprietary to Google as it is defined by a proprietary classifier and training data and therefore less semantically meaningful to other market participants.

[59] The current explainer First "Locally-Executed Decisions over Groups" ('FLEDGE') (March 2021) sets out refinements of Google's previous TURTLEDOVE proposal for retargeting capability.

Proposals, Chrome would replace the advertiser ad server and be responsible for tracking impression events (when a web user views, but does not necessarily click on an ad), matching such events with conversions 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, and when advertisers also use Google DSPs, Google would be in a position of 'marking its own homework' as it would provide advertiser advisory services and the services meant to check the successful delivery of ads. This is analogous to the current situation where Google operates the most popular advertiser ad server and DSPs. However, moving this functionality to the web browser would give rise to greater conflicts of interest because while advertisers currently have the possibility to choose an independent advertiser ad server, they would have very limited influence (if any) over the web browser chosen by web users.

Gnatcatcher, WebID and X-Client Data

5.77 We have also heard a range of concerns from parties that Google will have the ability to use a range of information that will be available to Chrome after the introduction of the Privacy Sandbox Proposals to self-preference its own advertising inventory and ad tech services.

5.78 For example, since Chrome will still have access to IP addresses, while rivals will have access to more limited data under the GNATCATCHER proposals, Google could in principle choose to share this information with Google's ad tech services for the purposes of tracking users after the introduction of the Privacy Sandbox proposals. Similarly, under some variants of the WebID proposal, Chrome would have access to all the user's log in data, [60] which it could choose to share with Google's advertising services after the introduction of the proposals. Further, we have heard concerns that, 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 use to optimise the performance of its services – and, in principle, track users across the web.[61]

5.79 Overall, the CMA is concerned that, in the absence of the Proposed Commitments, the shift of functionalities currently performed by ad tech providers to Chrome would give Google discretion over decision making in ways that cannot be scrutinised or challenged by third parties. This could lead to the emergence of conflicts of interest and a lack of confidence on

[60] The delegation-oriented variant of WebID can be found on the WebID Github pages here and here.
[61] Google told the CMA that X-Client Data header is used to help Chrome test new features before rolling them out, not to identify or track individual users.

the part of third parties regarding Google's intentions and criteria which will be used to develop and implement the Privacy Sandbox Proposals.

Concern 3: imposition of unfair terms on Chrome web users

5.80 The CMA is also concerned that, in the absence of regulatory scrutiny and oversight, Google would be able to exploit its likely dominant position by denying Chrome web users any substantial choice in terms of whether and how their personal data is used for the purpose of targeting and delivering advertising to them. The CMA considers that web users are likely to have different attitudes and preferences with respect to the collection and processing of their personal data. While some users may prefer not to have their personal data collected and processed by their browser and/or third parties, others might be willing to consent to such data usage in return for seeing more relevant ads, avoiding repeated ads, or other rewards. As such, 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.

5.81 The CMA considers that a browser developer operating under normal and sufficiently effective competition would face an incentive to give its users significant control over whether and how their personal data is used, subject to suitable defaults and an adequate choice architecture. The CMA notes that Chrome's two largest competitors, Firefox and Safari, 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.

5.82 In contrast, under Google's Proposals, it is unclear whether Chrome web users would have the option of keeping TPCs enabled on their browser. In addition, Chrome web users could have little or no control with respect to whether and how their personal data is used by the browser to provide the functionalities envisaged in the Privacy Sandbox Proposals.[62] The CMA understands that under the current proposals, web users may have limited options to disable ad targeting in Chrome, or select which aspects and what proportion of their browsing history and online behaviour would be used to form cohorts and support retargeting. The CMA is concerned that, in the absence of the Proposed Commitments, such restrictions 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

[62] Google stated that it would release the first user controls for the 'Privacy Sandbox' in April 2021 and would expand these controls in future Chrome releases. See Chromium Blog, Privacy Sandbox in 2021: Testing a more private web, January 2021.

preventing them from adjusting the level of privacy and targeting in line with their preferences.

Assessment of the impact of the Privacy Sandbox announcements

5.83 This part sets out the CMA's preliminary view that the announcements themselves are likely to constitute an abuse in the specific circumstances of the case.

5.84 The CMA is concerned that Google's announcements relating to the Privacy Sandbox Proposals and/or taking implementing steps, are likely to, individually and/or collectively, amount to an abuse of its likely dominant position in the market for the supply of web browsers in the UK. This is set out in the following sections.

The announcements and implementing steps

5.85 As mentioned in paragraph 3.22 above, Google has made a number of announcements in 2019-2021 in relation to its planned changes to Chrome.

5.86 On 14 January 2020 Google announced that "… we plan to phase out support for third-party cookies in Chrome. Our intention is to do this within two years." This was followed by other announcements made on 7 May 2019, 22 August 2019, and 25 January 2021, as set out in paragraph 3.22 above.

5.87 In addition, Google has also taken a number of steps since then towards implementing the Privacy Sandbox Proposals. For example:

(a) In February 2020, Google introduced its SameSite update, requiring web developers to explicitly label cookies to make them available for third-party access. All unlabelled cookies would be by default limited to first-party access only.[63]

(b) In July 2020, Chrome updated its default HTTP Referrer policy to strict-origin-when-cross-origin. Developers remain free to set their preferred referrer policy, but the default has changed.[64]

(c) In September 2020, Google rolled out User-Agent Client Hints API functionality allowing web developers to request the exact

[63] Chromium Blog: SameSite Cookie Changes in February 2020: What You Need to Know.
[64] A new default Referrer-Policy for Chrome: strict-origin-when-cross-origin (google.com).

information they need from the browser, in addition to accessing existing user-agent strings.[65]

5.88 The CMA understands that the original announcement of TPC deprecation was escalated to the Google executive level and that subsequent announcements were made by senior employees, such as the Director of Chrome Engineering.[66]

5.89 Overall, the CMA's preliminary view is that the content of the announcements, as well as the seniority of Google staff making these announcements, was such as to have a likely anti-competitive effect in the specific circumstances of this case, with the intention communicated to market participants being that Google would proceed with changes in the relevant areas, and remove TPCs "within two years" of its first announcement.

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

5.90 Google has encouraged market participants to engage and provide feedback, including through the World Wide Web Consortium ('**W3C**'), on the Privacy Sandbox Proposals.[67] The CMA notes that in this and other fora, some market participants have suggested amendments to the Privacy Sandbox Proposals, some of which were fully or partly implemented by Google in further developments. For example, there has been a number of proposals from market participants aimed at allowing advertisers to retarget users, which the CMA understands have been taken into account in the more recent TURTLEDOVE Proposal.

5.91 However, several market participants have expressed concerns in discussions with the CMA about Google's engagement and transparency with the industry in relation to Google's Proposals. These concerns are summarised below:

(a) Some market participants have claimed that Google's engagement with stakeholders, through the W3C, has been limited and of a very technical nature, which limits the potential for participation and examination of Google's Proposals by third parties. They say that Google has engaged in ad hoc discussions to gather feedback,

[65] User Agent Client Hints - The Chromium Projects.
[66] This relates to the announcements of 7 May 2019, 22 August 2020 and 25 January 2021.
[67] For example, in Google's announcements dated 14 January 2020 and 25 January 2021.

rather than the usual process for when new standards are being discussed and agreed.

(b) The CMA has heard that Google has provided little detail and transparency on the Privacy Sandbox Proposals and their effectiveness compared to TPCs. Market participants said that there is a lack of transparency over how Google intends to test the effectiveness of the Privacy Sandbox Proposals, including the criteria it will use in evaluating their effectiveness and how feedback from market participants will be taken into account. For example, Google's test of the effectiveness of FLoC, as a replacement signal for TPCs, has been seen to reflect Google's use cases only. Further, where Google has made claims about the effectiveness of the Privacy Sandbox Proposals, some market participants say that insufficient underlying evidence has been provided to allow third parties to assess such claims.[68]

(c) There is concern that FLoC and other Privacy Sandbox 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 or audited, by anyone outside Google.

(d) Some market participants argue that Google has made no, or insufficient, statements of any ambition to minimise distortions of competition.

5.92 We consider that these concerns reflect the strong asymmetry of information between Google and market participants as well as the commercial incentives that Google faces in developing the Privacy Sandbox 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. 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 a competitive advantage from its likely dominant position in browsers.

[68] 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 advertisers can expect to see at least 95% of the conversions per dollar spent when compared to cookie-based advertising". However, it did not publish any details of the underlying data or the methodology of simulations that it used to reach this conclusion.

Announcements not competition on the merits

5.93 The CMA's preliminary 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.

5.94 In view of this awareness that the announcements would reduce competition, the CMA's preliminary view is that these announcements were not competition on the merits.

Likely effects

5.95 Market participants have expressed concerns in discussions with the CMA about the impact that these announcements have on the relationship with their clients and expected trajectory of their businesses.

5.96 For the reasons set out in the previous section, the CMA's preliminary view is that the implementation of the Privacy Sandbox Proposals, without regulatory scrutiny and oversight, would be likely to lead to a reduction in competition and adverse impacts on Google's competitors in open display advertising, in the absence of commitments or other changes to mitigate these effects. The announcements and/or implementing steps made by Google to date have created an expectation that there is likely to be a reduction in competition and there is a lack of transparency and asymmetry of information between Google and third parties.

5.97 Given Google's position on the relevant and related markets, its status as an unavoidable trading partner and its commercial incentives, 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.

Summary of concerns

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

(a) 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;

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

(c) 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.

5.99 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 to date have shown (and created the expectation) that Google is 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.

5.100 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:

(a) 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

(b) 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.

6. The CMA's assessment of the Proposed Commitments

6.1 Google has offered the Proposed Commitments to the CMA with the stated purpose of addressing the CMA's competition concerns (as described in section 5).[69] The Proposed Commitments are set out in Appendix 1.

6.2 Pursuant to section 31A of the Act, for the purposes of addressing the competition concerns it has identified, the CMA may accept from such person (or persons) concerned as it considers appropriate, commitments to take such action (or refrain from taking such action) as it considers appropriate.

6.3 The Procedural Guidance states that the CMA is likely to consider it appropriate to accept commitments only in cases where (i) the competition concerns are readily identifiable; (ii) the competition concerns are addressed by the commitments offered; and (iii) the proposed commitments are capable of being implemented effectively and, if necessary, within a short period of time.[70] However, the CMA will not accept commitments where compliance with such commitments and their effectiveness would be difficult to discern and/or where the CMA considers that it would undermine deterrence not to complete its investigation and make a decision.[71]

6.4 Following engagement with Google, the CMA has reached the provisional view that its competition concerns would be addressed by the Proposed Commitments and that the other criteria set out in the Procedural Guidance are met. Formal acceptance of the Proposed Commitments would result in the CMA terminating its Investigation and not proceeding to a decision on whether the Act has been infringed. A decision by the CMA accepting commitments would not include any statement as to whether Google's conduct under Investigation has infringed Chapter II of the Act prior to the acceptance of these commitments.

6.5 The rest of this section provides:

(a) a high-level summary of the way in which the Proposed Commitments meet the competition concerns set out in Section 5;

(b) a more detailed description of the key provisions of the Proposed Commitments, and the CMA's assessment of them;

[69] Google has said that the offering of Commitments does not constitute an admission of wrongdoing on its part.
[70] Procedural Guidance, paragraph 10.18.
[71] Procedural Guidance, paragraph 10.20.

(c) the CMA's assessment against the other criteria for accepting commitments set out in the Procedural Guidance; and

(d) the CMA's overall provisional conclusion.

Summary

6.6 As set out in section 5, the CMA has competition concerns relating, first, to the likely impact of the Privacy Sandbox Proposals, if they are implemented without appropriate regulatory scrutiny and oversight and second, Google's announcement of the relevant proposals and/or implementing steps.

6.7 The CMA has three concerns in relation to the likely impact of the Privacy Sandbox Proposals, if implemented without regulatory scrutiny and oversight:

(a) that by restricting third parties' ability to track users (and associated functionality, including the ability to target and measure the effectiveness of digital advertising) while retaining Google's ability to do so, the Privacy Sandbox Proposals would be likely to distort competition in the supply of ad inventory and ad tech services in the UK;

(b) that by transferring key functionalities to Chrome, Google's Proposals give Google the opportunity to self-preference its own ad inventory and ad tech services, affecting digital advertising market outcomes through Chrome in a way that cannot be scrutinised by third parties; and

(c) that the Privacy Sandbox Proposals would be likely to 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.

6.8 The extent to which these concerns are actually borne out in the future will depend on the design and implementation of Google's Proposals, which has not yet been finalised. For example, if the alternative technologies developed through the Privacy Sandbox Proposals are demonstrated to be adequate substitutes for the functionalities lost through stopping user tracking, this could address the first concern. Similarly, the Privacy Sandbox Proposals could be designed to minimise the risk of self-preferencing and to give users sufficient choice.

6.9 In relation to Google's announcement of the relevant proposals and/or implementing steps, 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 reflect in part:

(a) 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

(b) 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.

6.10 The CMA has reached the provisional view that the Proposed Commitments, once implemented, would address these competition concerns. In particular, the Proposed Commitments:

(a) **Establish a clear purpose of the Proposed Commitments** that will ensure that Google's Proposals are developed in a way that addresses the above competition concerns, by avoiding distortions to competition, whether through restrictions on functionality or self-preferencing, and avoiding the imposition of unfair terms on Chrome's web users.

(b) **Establish the criteria that must be taken into account in designing, implementing and evaluating Google's Proposals**. These include the impact of the Privacy Sandbox Proposals on: privacy outcomes and compliance with data protection principles; competition in digital advertising and in particular the risk of distortion to competition between Google and other market participants; the ability of publishers to generate revenue from ad inventory; and user experience and control over the use of their data.

(c) **Provide for greater transparency and consultation with third parties over the development of Google's Proposals**, including a commitment publicly to disclose the results of tests of the effectiveness of alternative technologies. This would help to overcome the asymmetry of information between Google and third parties regarding the development of the Privacy Sandbox Proposals;

(d) **Provide for the close involvement of the CMA in the development of Google's Proposals** to ensure that the purpose of the Proposed Commitments is met, including through regular meetings and reports, working with the CMA without delay to identify and resolve any competition concerns before the removal of TPCs, involving the CMA in the evaluation and design of tests of Google's Proposals. This would ensure that the above concerns about the potential impacts of the Privacy Sandbox Proposals are addressed and contribute to addressing the lack of confidence on the part of third parties regarding Google's intentions in developing and implementing Google's Proposals;

(e) **Provide for a Standstill Period** of at least 60 days before Google proceeds with the removal of TPCs , giving the CMA the option, if any outstanding concerns cannot be resolved with Google, to reopen its Investigation and, if necessary, impose any interim measures necessary to avoid harm to competition. This provision would strengthen the ability of the CMA to ensure its competition concerns are in fact resolved;

(f) Include specific **commitments by Google not to combine user data** from certain specified sources for targeting or measuring digital advertising on third-party and first-party ad inventory. This would contribute to addressing the competition concerns arising from Google's greater ability to track users after the introduction of Google's Proposals; and

(g) Include **specific commitments by Google not to design any of the Privacy Sandbox Proposals in a way which could self-preference Google**, not to engage in any form of self-preferencing practices when using the Privacy Sandbox technologies and not to share information between Chrome and other parts of Google which could give Google a competitive advantage over third parties. This would address the above concerns relating to the potential for discrimination against Google's rivals.

6.11 Overall, the CMA's provisional view is that, in combination, the Proposed Commitments would address the competition concerns that the CMA has identified in relation to the Privacy Sandbox Proposals, and provide a robust basis for the CMA and third parties to influence the future development of Google's Proposals to ensure that the Purpose of the Commitments is achieved.

The CMA's assessment of the Proposed Commitments

6.12 This section provides a more detailed description of the key provisions of the Proposed Commitments, and the CMA's assessment of them. The discussion follows the structure of Google's Proposed Commitments as set out in Appendix 1.

Purpose of the Commitments

6.13 The purpose of the Proposed Commitments – referred to in the Proposed Commitments, and in this notice, as the '**Purpose of the Commitments**' – is to ensure that the design, development and implementation of the Privacy Sandbox Proposals does not lead to a distortion of competition in the digital advertising markets, (whether through restrictions on functionality associated with user tracking or through self-preferencing of Google's advertising products, services and ad inventory), and/or the imposition of unfair terms on Chrome's web users.[72]

6.14 The Proposed Commitments require Google to design, implement and evaluate the Privacy Sandbox Proposals by taking into account a number of specific factors (the '**Development and Implementation Criteria**').[73] The Development and Implementation Criteria will be used to form the basis of an assessment as to whether the Purpose of the Commitments has been met. The Development and Implementation Criteria relate to the impacts of Google's Proposals on different considerations:

(a) the impact on privacy outcomes and compliance with data protection principles;

(b) the impact on competition in digital advertising and in particular the risk of distortion to competition between Google and other market participants;

(c) the impact on publishers (including in particular the ability of publishers to generate revenue from ad inventory) and advertisers (including, in particular, the ability of advertisers to obtain cost-effective advertising);

(d) the impact on user experience, including the relevance of advertising and transparency over how personal data is used for advertising purposes and user control; and

[72] Proposed Commitments, section C.
[73] Proposed Commitments, paragraph 9.

(e) technical feasibility, complexity and cost involved in Google designing, developing and implementing the Privacy Sandbox Proposals.

6.15 The CMA's provisional view is that the Development and Implementation Criteria cover the relevant considerations that should be taken into account in developing the Privacy Sandbox Proposals and that, in combination, the Purpose of the Commitments and the Development and Implementation Criteria would ensure that the Privacy Sandbox Proposals are developed in a way that addresses the CMA's competition concerns.

Transparency and consultation with third parties

6.16 The Proposed Commitments require Google to make a clear public statement specifying that in developing the Privacy Sandbox Proposals, it intends to pursue its objective of making the web more private and secure for web users, while:

(a) supporting the ability of publishers to generate revenue from ad inventory and the ability of advertisers to secure value for money from advertising spend;

(b) supporting a good user experience in relation to browsing the web and digital advertising;

(c) providing users with substantial transparency and control over their data as they browse the web; and

(d) not distorting competition between Google's own advertising products and services and those of other market participants.[74]

6.17 The public statement will also specify that Google intends to design, develop and implement the Privacy Sandbox in line with the Development and Implementation Criteria, that Google will involve the CMA on an ongoing basis in relation to the design, development and implementation of the Privacy Sandbox and that Google will also regularly consult with publishers, advertisers and ad tech providers on the Privacy Sandbox Proposals.[75]

6.18 The Proposed Commitments also require Google publicly to disclose the timing of key Privacy Sandbox Proposals, including updates on these as timings change or become more certain and, in relation to the use cases

[74] Proposed Commitments, paragraphs 11.a.
[75] Proposed Commitments, paragraphs 11.c. and 11.d.

set out in Annex 1 to the Proposed Commitments, including information on the earliest date for availability, the timings of origin trials, the implementation of the Privacy Sandbox Proposals and removal of TPCs. Such disclosures may be made in particular within specifically named groups such as the blink-dev discussion group, the W3C and/or in a blog post, a dedicated microsite, and will aim to enable publishers, advertisers and ad tech providers to influence the Privacy Sandbox and to adjust their business models. Google would provide a single webpage where all such disclosures can be accessed.[76]

6.19 To improve transparency, the Proposed Commitments also require[77] Google publicly to disclose the results of the tests it carries out that are material to evaluating the effectiveness of alternative technologies to TPCs, including a granular description of the underlying data and methodology used. Google has offered to consult with the CMA prior to publishing this information, which would be made available in Google blogs or a dedicated microsite.[78]

6.20 Google has also offered to facilitate the involvement of the CMA in discussions on the Privacy Sandbox Proposals in the World Wide Web Consortium or any other fora requested by the CMA.[79]

6.21 The CMA is of the provisional view that these Proposed Commitments would provide market participants with greater transparency and reassurance about the approach that Google will take in developing the Privacy Sandbox Proposals and help overcome the asymmetry of information between Google and market participants.

6.22 The public statement described at paragraph 6.16 above, by clarifying the development and implementation criteria, would provide market participants with greater transparency on how Google would assess the effectiveness of the Privacy Sandbox Proposals.

6.23 In addition, the public disclosure of the results of tests on the effectiveness of alternative technologies, at a sufficient level of granularity, would allow market participants to evaluate Google's claims about their effectiveness, and assess the likely impact on their businesses. This would provide them with greater confidence when making investment decisions on solutions aimed at working with the Privacy Sandbox Proposals, or considering

[76] Proposed Commitments, paragraph 12.
[77] Proposed Commitments, paragraph 16.c.v.
[78] Google would not publicly disclose personal data, Google proprietary software code, algorithms or other business secrets. However, the CMA may request that such data is disclosed to the CMA in order for the CMA to assess the effectiveness of the Privacy Sandbox Proposals.
[79] Proposed Commitments, paragraph 13.

whether to develop alternatives. Similarly, disclosing key timings would ensure that market participants are provided with adequate notice of future changes to the Privacy Sandbox Proposals so that they are able to plan and make decisions on how best to allocate advertising budgets and provide advertising solutions.

Involvement of the CMA in the Privacy Sandbox proposals

6.24 Google has offered to engage with the CMA in an open, constructive, and continuous dialogue regarding the development and implementation of the Privacy Sandbox Proposals to ensure the Purpose of the Commitments can be achieved, taking into account the Development and Implementation Criteria.[80]

6.25 Specifically, the CMA would be involved through the following mechanisms:

(a) Efforts by Google to identify and resolve any CMA concerns quickly;

(b) Regular status meetings and updates;

(c) CMA involvement in the testing of Alternative Technologies; and

(d) CMA involvement in the plans for and testing of user controls.

6.26 In addition, Google acknowledges that the CMA will involve the ICO to achieve the Purpose of the Commitments.[81]

6.27 The CMA provisionally considers that the involvement of the CMA and the ICO in the design, development and implementation of the Privacy Sandbox Proposals would address the concerns relating to the lack of regulatory oversight of Google's Proposals and the lack of confidence regarding Google's statements and intentions in developing and implementing the Privacy Sandbox Proposals.

Efforts to identify and resolve concerns quickly

6.28 Google has undertaken proactively to inform the CMA of any changes to the Privacy Sandbox Proposals that are material to ensuring that the Purpose of the Commitments is achieved.[82] In addition, Google has undertaken in the Proposed Commitments to work with the CMA without delay to identify and resolve any competition concerns the CMA may have about the Privacy Sandbox Proposals. If the CMA were to have competition

[80] Proposed Commitments, paragraph 14.
[81] Proposed Commitments, paragraph 17.
[82] Proposed Commitments, paragraph 16.a.i.

concerns, the CMA would notify Google to that effect.[83] The CMA's expectation is that, should such concerns be raised, Google will resolve those concerns. The CMA would be accepting the Proposed Commitments on that understanding.

6.29 If, contrary to the CMA's expectations, such competition concerns are not resolved within 20 Working Days of a notification in writing by the CMA, there would be reasonable grounds for believing that there has been a material change of circumstances since the Proposed Commitments were accepted. In that scenario, the CMA could reopen its Investigation under section 31B(4) of the Act and, where necessary, could impose interim measures under section 35 of the Act to avoid harm to competition.[84]

6.30 The CMA provisionally considers that Google's undertaking to resolve any competition concerns that the CMA has, and the CMA's ability to reopen the Investigation if necessary would (in the overall context of the Proposed Commitments) ensure that the CMA's competition concerns are addressed.

Regular status meetings and updates

6.31 In the Proposed Commitments, Google has undertaken to hold regular (at least monthly) discussions with the CMA on the progress of the Privacy Sandbox Proposals.[85] Regular updates will also be provided to the CMA in accordance with Google's reporting and compliance obligations.[86]

6.32 The CMA provisionally considers that, in combination, these provisions would ensure that it has adequate access to information about the development of Google's Proposals to allow the CMA to ensure that the Purpose of the Commitments is achieved.

Testing Alternative Technologies

6.33 The Proposed Commitments involve a number of requirements relating to the testing of Alternative Technologies to TPCs and the involvement of the CMA in these tests. In particular, Google will:

(a) test the effectiveness of individual Alternative Technologies and also their effectiveness in combination to fully assess the impact of the Removal of Third-Party Cookies;

[83] Proposed Commitments, paragraph 16.a.
[84] Proposed Commitments, paragraph 16.a.iii.
[85] Proposed Commitments, paragraph 16.b.
[86] Proposed Commitments, paragraph 15 and eg paragraph 27.a.

(b) engage with the CMA to agree the specific parameters for the evaluation and overall design of the tests before they are carried out, reflecting the Development and Implementation Criteria (as described at paragraph 6.14 above); and

(c) share with the CMA the results of all tests carried out and, at the CMA's request, the relevant underlying data and analyses.[87]

6.34 If Google and the CMA cannot reach an agreement regarding appropriate testing parameters the CMA may notify Google of its preferred parameters.[88] If Google does not within 20 Working Days, agree to carry out a test according to the CMA's parameters, the CMA may reopen its Investigation under section 31B(4) of the Act.[89]

6.35 As noted above in paragraph 6.19, Google has undertaken to publicly disclose the results of the tests it carries out that are material to evaluating the effectiveness of alternative technologies to TPCs, including a granular description of the underlying data and methodology used.[90] The evaluation of the effectiveness of alternatives to TPCs would be assessed by reference to the Development and Implementation Criteria, including the extent to which they have an impact on privacy, publishers, advertisers and users as well as their impact on competition.[91] Google may carry out its own tests in addition [92] but would inform the CMA if these were to result in material changes to the Prvacy Sandbox proposals.[93]

6.36 The CMA provisionally considers that these provisions strengthen its ability to address its competition concerns relating to the Privacy Sandbox Proposals and in particular the first competition concern, that Google's Proposals will limit the functionality available to its rivals in the open display market, while leaving Google's ability to offer these functionalities relatively unaffected. This concern could be addressed by the identification of Privacy Sandbox Proposals that are demonstrated to provide effective substitutes for the key functionalities that would be lost by the removal of TPCs and other forms of cross-site tracking.

6.37 The fact that the CMA would agree with Google the design and testing of the Alternative Technologies individually and in combination, before the removal of TPCs, would provide greater clarity and transparency to market

[87] Proposed Commitments, paragraph 16.c.ii.
[88] Proposed Commitments, paragraph 16.c.iii.
[89] Proposed Commitments, paragraph 16.c.iv.
[90] Proposed Commitments, paragraph 16.c.v.
[91] Proposed Commitments, eg paragraphs 9 and 16.c.v.
[92] Proposed Commitments, paragraph 16.c.vi.
[93] Proposed Commitments, paragraph 16 i

participants on the effectiveness of these alternatives for the performance of key functions such as targeting, frequency capping and attribution and would ensure that TPCs would not be removed until the CMA's competition concerns had been addressed.

6.38 If through testing the CMA considered that its competition concerns were not fully met, the CMA may consider it necessary for Google to make modifications to the design of the Privacy Sandbox Proposals to ensure that the CMA does not have remaining concerns relating to impacts on competition and user choice and control.

6.39 The CMA notes that the provisions of paragraph 16.c. of the Proposed Commitments relate specifically to the testing of the Alternative Technologies, defined as substitutes for TPC, rather than to the entirety of the Privacy Sandbox Proposals. However, the Development and Implementation Criteria would provide the framework for evaluating the future development of the entirety of the Privacy Sandbox Proposals, to ensure that they achieve the Purpose of the Commitments, and the CMA will be involved in this broader evaluation and assessment.[94] This includes, for example, elements of the Proposals such as First Party Sets, which may not be amenable to formal testing and trialling but will still be subject to development, evaluation and assessment by the CMA under the Proposed Commitments.

User controls

6.40 Google has offered to provide, at least once a quarter, updates to the CMA on Google's plans and decisions on user controls in relation to the Privacy Sandbox Proposals, including default options and choice architectures as well as the underlying user research and testing which underpin Google's decisions on user controls.[95]

6.41 The Proposed Commitments would enable the CMA to assess the proposed user controls before they are implemented. They would further ensure that Google takes into account any observations the CMA may make so that the Privacy Sandbox Proposals are designed and developed in a way that gives meaningful choice and control to users over the way in which they interact with the Privacy Sandbox Proposals, including whether and how their personal information is shared with publishers, advertisers and ad tech providers.

[94] Proposed Commitments, paragraphs 9 and 14.
[95] Proposed Commitments, paragraph 16.d.

6.42 At this early stage, the CMA considers that there may be a number of areas in which greater user choice and control could be introduced into the Privacy Sandbox Proposals. For example, under the FLoC proposal, web users could be given visibility and control over the cohort they have been assigned to and the option of sharing data from their behaviour on certain websites and not others. Similarly, under the Privacy Budget proposal, web users could be given the option of flexing the amount of data shared with different websites or publishers. It will be important to ensure that any such choices are subject to appropriate defaults and choice architectures, with the objective of supporting informed choice and protecting web users that do not engage with the detail of how their personal data is shared with third parties.[96]

CMA consultation with the ICO

6.43 In offering the Proposed Commitments, Google acknowledges that the CMA would involve and consult with the ICO as necessary and subject to the applicable legislation.[97]

6.44 The CMA intends to involve the ICO closely and on an ongoing basis in its assessment of the Privacy Sandbox Proposals. This reflects the central importance of data protection and privacy in the Privacy Sandbox Proposals and the close relationship between data protection and competition considerations in digital markets, as discussed in the CMA and ICO recent joint statement.[98] The CMA has worked closely with the ICO on these issues over the last year and will look to continue this close working relationship in the context of the Privacy Sandbox Proposals.

6.45 In its consideration of the Proposals, the CMA would look to involve the ICO in particular in the assessment of impacts on privacy outcomes and compliance with data protection principles. More specifically, the CMA is likely to consult the ICO when assessing the design of default options and choice architectures related to user controls. Both the CMA and ICO have substantial experience of designing effective choice environments from their engagement with web users and their work on consumer protection and can draw on behavioural scientists with specific expertise in this area.

6.46 The CMA provisionally considers that its involvement in consultation with the ICO would provide third parties with greater confidence in the development of the Privacy Sandbox Proposals, ensuring that both

[96] In the Market Study, the CMA found that consumer engagement with currently available privacy setting and controls is low. Market Study, paragraphs 4.84-4.108.
[97] Proposed Commitments, paragraph 17.
[98] Competition and data protection in digital markets: a joint statement between the CMA and the ICO, May 2021.

competition and data protection considerations are taken into account in the development of the Privacy Sandbox Proposals.

Standstill Period before the removal of TPCs

6.47 The CMA's intention is that, through the involvement of the CMA and ICO in the development of the Privacy Sandbox proposals, the distortions to competition listed in paragraph 8 of the Proposed Commitments will be avoided. The CMA's expectation is that, if the Proposed Commitments operate as intended, the CMA's competition law concerns should have been addressed at the time the Privacy Sandbox Proposals are finalised by Google.

6.48 However, as competition assessments can be complex, it is appropriate to build in an opportunity for the CMA to reflect and consult on Google's final proposals, to ensure that its competition law concerns are addressed.

6.49 To enable such reflection and consultation, Google has offered to refrain from implementing the removal of TPCs until the Standstill Period of at least 60 days after Google notifies the CMA of its intention to implement the removal of TPC has expired. At the CMA's request, Google will increase the Standstill Period by a further 60 days to a total of 120 days.[99]

6.50 Before triggering the Standstill Period, Google has offered to carry out a test of the Alternative Technologies in combination to fully assess the impact of the removal of TPCs. Google would share with the CMA the results of these tests and, at the CMA's request, the relevant underlying data and analyses.[100]

6.51 Drawing on the results of the final tests of the Alternative Technologies and its assessment of the other aspects of the Privacy Sandbox Proposals, the CMA would undertake a further public consultation to gather views from market participants on the Privacy Sandbox Proposals. Following this consultation, the CMA would notify Google if the CMA has any remaining competition concerns.

6.52 If the CMA were to have remaining competition concerns, the CMA would notify Google to that effect. The CMA's expectation is that, should such concerns be raised, Google will resolve those concerns. The CMA would be accepting the Proposed Commitments on that basis.

[99] Proposed Commitments, paragraph 18.
[100] Proposed Commitments, paragraphs 16.c.ii.

6.53 If, contrary to the CMA's expectations, such competition concerns are not resolved, there would be reasonable grounds for believing that there has been a material change of circumstances since the Proposed Commitments were accepted.[101] In that scenario, the CMA could reopen its Investigation under section 31B(4) of the Act and, where necessary, could impose interim measures under section 35 of the Act to avoid harm to competition.

6.54 The CMA provisionally considers that the continued involvement of the CMA and the ICO throughout the development of the Privacy Sandbox Proposals, the inclusion of the Standstill Period, and the opportunity to reopen the Investigation if necessary would (in the overall context of the Proposed Commitments) ensure that the CMA's competition concerns are addressed.

Google's use of data

6.55 After the removal of TPCs, the Proposed Commitments require Google not to use any of the individual-level user data from the following sources for targeting or measuring digital advertising on third-party inventory: [102]

- Google's current and future user-facing services, including Android;
- a user's Chrome browsing history, including synced Chrome history;
- a publisher's Google Analytics account; and
- data uploaded by an advertiser to Customer Match.

6.56 Further, the Proposed Commitments require Google not to use data on a web user's Chrome browsing history, including synced Chrome history, and data from a publisher's Google Analytics account to provide advertising services on its owned and operated inventory after the removal of TPCs.[103]

6.57 The CMA's provisional view is that these provisions (set out in paragraphs 23 to 24) would directly address many aspects of the CMA's first competition concern – that Google's Proposals would limit the functionality available to its rivals in the open display market, while leaving Google's

[101] Proposed Commitments, paragraph 20.
[102] Proposed Commitments, paragraph 23. For the avoidance of doubt, this is not intended to prevent Google from using the alternative technologies developed as part of Privacy Sandbox in the same way as third parties can use those technologies.
[103] Proposed Commitments, paragraph 24.

ability to offer these functionalities relatively unaffected through the use of data from its own user-facing services in Google's advertising businesses.

6.58 Specifically, in relation to third party inventory, paragraphs 23 to 25 would remove Google's ability to use all the sources of data set out in Table 5.1 above to its advantage when competing with rival ad tech providers to offer digital advertising services to third-party websites.

6.59 The Proposed Commitments would also prevent Google from using individual-level user data from two key sources (a user's Chrome browsing history and a publisher's Google Analytics account) for the purposes of targeting and measuring digital advertising on its own inventory. Both of these were key areas of concern identified by stakeholders.

6.60 Paragraphs 23 to 25 do not, however, explicitly prevent Google from sharing data collected from its user-facing services and Customer Match to target and measure advertising on its owned and operated inventory.

6.61 Nevertheless, the CMA provisionally considers that the Proposed Commitments are sufficient to address the CMA's competition concerns for two reasons.

6.62 First, the Proposed Commitments give the CMA the ability to influence the design and development of the Privacy Sandbox Proposals to avoid distortions to competition.[104] For example, if through the process of development, testing and trialling set out above, the Privacy Sandbox tools were shown to be fully effective substitutes for the functionality provided by TPCs and the other information deprecated by the Proposals, this could address concerns that the implementation of the Proposals would give Google a competitive advantage over rival publishers and ad tech providers. Even if the Privacy Sandbox tools were not shown to be fully effective substitutes these functionalities, the design of other elements of the Privacy Sandbox Proposals (notably First Party Sets) could be used to address any remaining competition concerns through directly determining the extent of data sharing which could occur within Google (and other large businesses). Even if the Privacy Sandbox tools were not shown to be fully effective substitutes these functionalities, the design of other elements of the Privacy Sandbox Proposals (notably First Party Sets) could be used to address any remaining competition concerns through directly determining

[104] The criteria that the CMA and Google would use to assess the effectiveness of alternative technologies would give the CMA the opportunity to evaluate whether and the extent to which Google's data advantage would distort competition in digital advertising markets (in paragraph 9).

the extent of data sharing which could occur within Google (and other large businesses).

6.63 Second, if, before the withdrawal of TPCs, the CMA were to have remaining competition concerns, the CMA would notify Google to that effect. The CMA's expectation is that, should such concerns be raised, Google will resolve those concerns. If, contrary to the CMA's expectations, such competition concerns are not resolved, the CMA could reopen its Investigation under section 31B(4) of the Act and, where necessary, the CMA could impose interim measures under section 35 of the Act to avoid harm to competition. In this context, the CMA could consider other interventions to address the remaining competition concerns, such as imposing separation of certain sources of data used by Google to advertise on its own ad inventory.

Obligation not to discriminate

6.64 Google has offered not to discriminate against its rivals in favour of its own advertising and ad tech businesses, in particular by:

(a) committing not to design and develop the Privacy Sandbox Proposals in a way that will distort competition by self-preferencing Google's advertising products and services;

(b) committing not to implement the Privacy Sandbox in ways that will distort competition by self-preferencing Google's advertising products and services; and

(c) committing not to use competitively sensitive information provided by an ad tech provider or publisher to Chrome in a way that distorts competition.[105]

6.65 As described in section 5 above, the CMA's second competition concern is that in the absence of accepting the Proposed Commitments, the Privacy Sandbox Proposals would give Google the opportunity to self-preference its own ad inventory and ad tech services and affect digital advertising market outcomes through Chrome in a way that cannot be scrutinised by third parties.

6.66 The CMA's provisional view is that the Proposed Commitments, and in particular the provisions of paragraph 26, address this competition concern.

[105] Proposed Commitments, paragraph 26.

6.67 First, the Proposed Commitments would require Google to design and develop the Privacy Sandbox Proposals in a manner that ensures that it does not distort competition by discriminating against rivals in favour of Google's own advertising products and services.[106] This Proposed Commitment would limit Google's ability to advantage itself through, for example, the availability and transparency of cohort interest profiles and data dependencies in FLoC.

6.68 Second, the Proposed Commitments would require Google not to implement the Privacy Sandbox Proposals in ways that will distort competition by self-preferencing Google's advertising products and services.[107] Under this Proposed Commitment, Google would not be able to advantage itself through, for example, increased interoperability with the Privacy Sandbox tools or increased device processing power compared to rivals, or by not sending ad requests to its competitors or sending them with some delay and making it more difficult for them to send a bid in time. Further, Google would not be able to use information on users to which it would have privileged access through Chrome after the introduction of the Proposals to gain advantage for its advertising products and services. For example, it would not be able to use the IP addresses to which it would have access through Gnatcatcher, the information on user logins to which it would have access through the WebID proposal, or information on device characteristics through X-Client-Data, to track users.

6.69 Third, the Proposed Commitments would prohibit Google from using competitively sensitive information provided by an ad tech provider or publisher to Chrome in a way that distorts competition.[108] This Proposed Commitment would remove Google's ability to use a rival's information to its own advantage. For example, Google would not be able to access rivals' bidding strategies included in the bidding logic which rivals would need to provide to Chrome to execute when a retargeting opportunity arises.

Reporting and compliance

6.70 In order for the CMA to monitor Google's compliance with the Proposed Commitments effectively, Google has offered to provide the CMA with quarterly compliance and monitoring statements. Google will provide quarterly compliance reports in the form of Annex 2 to the Proposed

[106] Proposed Commitments, eg at paragraph 26.a.
[107] Proposed Commitments, paragraph 26.b.
[108] Proposed Commitments, paragraph 26.c.

Commitments, and quarterly monitoring statements in a form to be agreed with the CMA.[109]

6.71 Google will also take certain other steps for reporting and compliance purposes. For example, Google will promptly notify the CMA if Google becomes aware of any breach of the Proposed Commitments, and commits to providing information concerning the nature and duration of such breach.[110]

6.72 The CMA's provisional view is that these obligations will ensure that the CMA remains in a position to monitor effective compliance by Google with the Proposed Commitments, and to take appropriate enforcement steps if required.

Duration

6.73 Google has offered the Proposed Commitments to be in force until the earlier of: (i) the two year anniversary of Google's removal of TPCs; or (ii) five years from the date of the CMA's acceptance of the Proposed Commitments (unless released earlier).[111] Given the likely timing of Google's removal of TPCs, the Proposed Commitments would likely be in force for at least three years from the date of their acceptance by the CMA.

6.74 The CMA's provisional view is that such a duration would be appropriate for the Proposed Commitments. It would allow for a sustained period in which the CMA could assess further the Privacy Sandbox Proposals and their impact (including in light of any market developments since the Proposed Commitments came into effect).

Assessment against the other criteria set out in CMA guidance

6.75 In addition to the Proposed Commitments addressing the CMA's competition concerns, the CMA has reached the provisional view that it is appropriate to accept commitments in this Investigation because:

(a) the Proposed Commitments are capable of being **implemented effectively** and, if necessary, within a short period of time as Google would undertake to act in accordance with the Proposed

[109] Proposed Commitments, paragraphs 27.a.–27.b. and Annex 2.
[110] Proposed Commitments, paragraphs 27.c.–27.e. and 28. The compliance and monitoring statements would relate to paragraphs 23, 24 and 26 of the Proposed Commitments.
[111] Proposed Commitments, paragraph 29.

Commitments as of the date the CMA publishes any decision accepting the Proposed Commitments;

(b) accepting commitments in the Investigation **would not undermine deterrence**. Accepting commitments in the Investigation would demonstrate that the CMA is acting swiftly and decisively when identifying competition concerns. By accepting the Proposed Commitments at this early stage of the Investigation, the CMA would be able to resolve its competition concerns quickly and with an opportunity to scrutinise the further development of the Privacy Sandbox Proposals, address any issues before they are finalised and involve the ICO as appropriate. This would provide market participants with greater transparency and certainty at an earlier stage than could be achieved through continuing with the Investigation;

(c) **compliance** with and the effectiveness of the Proposed Commitments would **not be difficult to discern**. The compliance and reporting obligations, regular meetings and close involvement of the CMA as described at paragraphs 6.70 to 6.72 above would ensure that the CMA remains at all times in a position throughout the process to monitor effective compliance by Google, and to take appropriate enforcement steps if required;

(d) the Proposed Commitments do not preclude the CMA from taking further enforcement action in relation to other breaches of competition law and/or related markets which raise competition concerns and harm consumers.

Relationship with the Digital Markets Unit and new regulatory regime for online platforms

6.76 All of the Proposed Commitments, including those relating to Google's use of data, are subject to monitoring to ensure compliance and maintain trust in the Proposed Commitments. As set out above, the CMA is of the provisional view that Google's reporting and the CMA's involvement in the development of the Privacy Sandbox Proposals would ensure effective compliance monitoring.

6.77 As set out in the Market Study and the Digital Markets Taskforce's advice to HM Government,[112] regulatory oversight is important to ensure that

[112] CMA, A new pro-competition regime for digital markets: Advice of the Digital Markets Taskforce, December 2020.

restrictions are adhered to in practice and to build trust through independent regulatory scrutiny. While for the duration of the Proposed Commitments, the role of monitoring the implementation of the Proposed Commitments would fall to the CMA, in the medium term, the establishment of the Digital Markets Unit in the UK, along with a code of conduct for firms with Strategic Market Status,[113] could provide a framework for regulatory oversight and scrutiny.

[113] In the Market Study, the CMA reached the conclusion that Google was highly likely to meet any criteria for Strategic Market Status. Market Study, paragraph 7.58.

7. The CMA's intentions and invitation to comment

7.1 In light of the above, the CMA provisionally considers that the Proposed Commitments, as set out in Appendix 1, are sufficient to address its competition concerns. Therefore, the CMA intends to accept the Proposed Commitments by a means of a formal commitments decision.

7.2 As required by paragraph 2(2)(d) of Schedule 6A of the Act, the CMA now invites interested third parties to make representations on the Proposed Commitments and will take such representations into account before making its final decision whether to accept the Proposed Commitments.

Invitation to comment

7.3 As noted above, the CMA has not reached a final view and invites all interested parties to submit observations and evidence in order to assist the CMA in its final assessment of the Proposed Commitments.

7.4 Any person wishing to comment on the Proposed Commitments should submit written representations to Angela Nissyrios and Simon Deeble at 50972-Consultation@cma.gov.uk by **8 July 2021 at 5pm**. Please quote the case reference 50972 in all correspondence related to this matter.

7.5 The CMA is interested to hear from anyone wishing to comment on the Proposed Commitments. Any non-disclosure agreement a party may have in place with Google should not prevent them from responding to this consultation. How the CMA handles confidential information is set out in paragraph 7.8 below.

7.6 The CMA is particularly interested to hear any views on whether the Proposed Commitments, as set out in Appendix 1, are sufficient to address the competition concerns set out in section 5 above regarding:

(a) unequal access to the functionality associated with user tracking;

(b) self-preferencing Google's own ad tech providers and owned and operated ad inventory;

(c) imposition of unfair terms on Chrome's web users.

7.7 In any representations to the CMA on the Proposed Commitments, please refer as far as possible to the relevant heading(s) and/or paragraph(s) within the Proposed Commitments.

Confidentiality

7.8 The CMA does not intend to publish the responses to the consultation with any commitments decision or notice to provisionally accept any modified commitments. However, the information contained in the responses may be used or summarised on an anonymous basis in these documents.

7.9 In the event that the Proposed Commitments are not accepted and the CMA is considering disclosing the information (such as in or with a statement of objections), it will revert to the provider of that information to obtain representations on confidentiality. The CMA will then consider those representations before deciding whether the information should be disclosed under Part 9 of the Enterprise Act 2002.

Appendix 1: The Proposed Commitments

CMA - Case 50972 - Privacy Sandbox
Google Commitments Offer

A. Introduction

1. In August 2019, Google launched its Privacy Sandbox initiative to develop a set of open standards to enhance privacy on the web.[1]

2. In January 2020, Google declared its goal of making the web more private and secure for users, while also supporting publishers. Google expressed its confidence that privacy-preserving and open-standard mechanisms like the Privacy Sandbox can sustain a healthy, ad-supported web in a way that will render Third-Party Cookies obsolete. Google explained that, once these approaches had addressed the needs of users, publishers and advertisers, and Google had developed the tools to mitigate workarounds, it planned to phase out support for Third-Party Cookies in Chrome.[2]

3. On 7 January 2021, the CMA commenced an investigation under section 25 of the Act in relation to Google's Privacy Sandbox proposals. The CMA subsequently informed Google that the CMA was concerned that Google's proposals, if implemented without regulatory scrutiny and oversight, would be likely to amount to an abuse of a dominant position.

4. To address the CMA's competition concerns, Google UK Limited and Google LLC offer Commitments under section 31A of the Act. These Commitments provide for scrutiny and oversight by the CMA over implementation of, and announcements relating to, Google's Privacy Sandbox proposals.

5. Consistent with sections 31A and 31B of the Act, and subject to section 31B(4) of the Act, the Commitments are offered on the basis that if the CMA accepts the Commitments in accordance with section 31A(2) of the Act, it will not continue the investigation, make a decision within the meaning of section 31(2) of the Act, or give a direction under section 35 of the Act.

6. The offering of Commitments by Google does not constitute an admission of wrongdoing and nothing in these Commitments may be construed as implying that Google agrees with any concerns identified by the CMA in its investigation, including in a Commitments Decision. Google has not been the subject of any infringement decision or statement of objections in respect of the investigation.

B. Definitions

7. For the purposes of these Commitments, the following definitions apply:

   "**Act**" means the Competition Act 1998;

   "**Alternative Technologies**" means the technologies designed, developed and implemented by Google as alternatives to Third-Party Cookies in Chrome and Chromium;

[1] *Building a more private web*, 22 August 2019.
[2] *Building a more private web: A path towards making third party cookies obsolete*, 14 January 2020.

"**CMA**" means the Competition and Markets Authority;

"**Commitments**" means the commitments given by Google pursuant to section 31A of the Act;

"**Commitments Decision**" means a formal decision by the CMA under section 31A of the Act to accept Commitments, such that section 31B of the Act applies;

"**Compliance Statement**" means the quarterly statement provided by Google confirming its compliance with the Commitments;

"**Effective Date**" means the date on which the CMA notifies Google of a Commitments Decision;

"**Google**" means Google UK Limited (company number 03977902) and Google LLC and any other member of their corporate Group operating a business involved in the Privacy Sandbox;

"**Group**" includes those companies with which either Google UK Limited or Google LLC has the links described in Article 5(4) of Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings;

"**ICO**" means the Information Commissioner's Office;

"**Individual-level User Data**" means personal data (including pseudonymised data) on a given, individual user;

"**Monitoring Statement**" means the quarterly statement provided by Google explaining how it will ensure that it monitors internally that it remains compliant with the Commitments;

"**Privacy Sandbox**" means Google's proposals relating to the Removal of Third-Party Cookies, addressing workarounds[3] that facilitate continued cross-site tracking on Chrome, and the design, development and implementation of the Alternative Technologies as described on Google's website;[4]

"**Purpose of the Commitments**" has the meaning given in paragraph 8;

"**Removal of Third-Party Cookies**" and "**Removal**" refer to Chrome ending support for Third-Party Cookies or clearing Third-Party Cookies more frequently than every 30 days, whichever is first;

"**Third-Party Cookies**" means cookies which are created by a website other than the website that the user is visiting;

"**Working Day**" means any day other than a Saturday, Sunday or any other day that is a public holiday in England.

[3] Such workarounds include other forms of cross-site tracking beyond Third-Party Cookies, including fingerprinting (via information such as IP address or User Agent HTTP header) and CNAME cloaking.
[4] A dedicated website for Privacy Sandbox set up by Google exists here. There is also more information available on Chromium's website here.

C. Purpose of the Commitments

8. The "**Purpose of the Commitments**" is to address the CMA's concerns that, without sufficient regulatory scrutiny and oversight, the design, development and implementation of the Privacy Sandbox has the potential to:

    a. 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;

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

    c. cause the imposition of unfair terms on Chrome's web users.

9. Google will design, implement and evaluate the Privacy Sandbox proposals by taking into account the following factors (the "**Development and Implementation Criteria**"), which will inform the answer to the question of whether or not the Purpose of the Commitments has been achieved. The Development and Implementation Criteria are:

    a. impact on privacy outcomes and compliance with data protection principles;

    b. impact on competition in digital advertising and in particular the risk of distortion to competition between Google and other market participants;

    c. impact on publishers (including in particular the ability of publishers to generate revenue from advertising inventory) and advertisers (including in particular the ability of advertisers to obtain cost-effective advertising);

    d. impact on user experience, including the relevance of advertising, transparency over how personal data is used for advertising purposes, and user control; and

    e. technical feasibility, complexity and cost involved in Google designing, developing and implementing the Privacy Sandbox.

10. These Commitments are organised as follows:

    a. Section D provides for transparency and consultation with third parties;

    b. Section E provides for involvement of the CMA in the Privacy Sandbox proposals;

    c. Section F provides for a standstill before the Removal of Third-Party Cookies;

    d. Section G provides for Google's use of data;

    e. Section H provides for non-discrimination; and

    f. Sections I to M provide for reporting and compliance; duration; variation or substitution; effect of invalidity; and governing law and jurisdiction.

D. Transparency and consultation with third parties

11. Having agreed the wording with the CMA, by the day the Commitments Decision is published, Google will make a public statement in a blog post, a dedicated microsite or equally prominently (to which a link may be added in the CMA's webpages) specifying:

    a. that, in developing the Privacy Sandbox proposals, Google intends to pursue its objective of making the web more private and secure for users, while:

        i. supporting the ability of publishers to generate revenue from advertising inventory and the ability of advertisers to secure value for money from advertising spend;

        ii. supporting a good user experience in relation to browsing the web and digital advertising;

        iii. providing users with substantial transparency and control over their data as they browse the web; and

        iv. not distorting competition between Google's own advertising products and services and those of other market participants;

    b. the Development and Implementation Criteria;

    c. that Google intends to design, develop and implement the Privacy Sandbox in line with the Development and Implementation Criteria; and

    d. that Google will involve the CMA on an ongoing basis in relation to the design, development and implementation of the Privacy Sandbox and Google will also regularly consult with publishers, advertisers and ad tech providers pursuant to paragraphs 12 and 16(c)(v) below.

12. Google will publicly disclose the timing of the key Privacy Sandbox proposals as set out in Annex 1. Google will also publicly update the information provided for in Annex 1 as timings change or become more certain. Such disclosures may be made in particular within the blink-dev discussion group, within the World Wide Web Consortium and/or in a blog post, a dedicated microsite or equally prominently, and will aim to enable publishers, advertisers and ad tech providers to influence the Privacy Sandbox and to adjust their business models. Google will provide a single webpage from which all such disclosures can be accessed.

13. Google will, at the CMA's request, seek to facilitate the involvement of the CMA in discussions on the Privacy Sandbox in the World Wide Web Consortium or any other fora.

E. Involvement of the CMA in the Privacy Sandbox proposals

14. Google will engage with the CMA in an open, constructive and continuous dialogue in relation to the development and implementation of the Privacy Sandbox proposals, with a view to achieving the Purpose of the Commitments, taking into account the Development and Implementation Criteria.

15. Updates to the timeline at Annex 1 will be provided to the CMA in accordance with paragraph 27(a). This is to assist the CMA in planning its own involvement in the process.

16. Google and the CMA will organise their dialogue by mutual agreement. Such dialogue will in particular involve:

    a. **Efforts to identify and resolve concerns quickly.**

        i. Google will proactively inform the CMA of changes to the Privacy Sandbox that are material to ensuring that the Purpose of the Commitments is achieved.

        ii. Google will work with the CMA without delay to seek to resolve concerns raised and address comments made by the CMA with a view to achieving the Purpose of the Commitments. Google will inform the CMA of how it has responded to those comments.

        iii. In the event that Google and the CMA cannot reach mutual agreement or resolve concerns within 20 Working Days of a notification in writing by the CMA, unless extended by mutual consent, the CMA may take action pursuant and subject to the provisions of section 31B(4) of the Act.

    b. **Status meetings.** Google and the CMA will schedule regular meetings at least once a month until the Removal of Third-Party Cookies and at regular intervals thereafter to discuss progress on the Privacy Sandbox proposals.

    c. **Testing Alternative Technologies.** During the period from acceptance of these Commitments until the Removal of Third-Party Cookies, Google will seek to agree with the CMA parameters which are material for the design of any significant tests for evaluating the effectiveness of the Alternative Technologies according to the Development and Implementation Criteria. Such testing will be carried out on the following basis:

        i. Google will test the effectiveness of individual Alternative Technologies and also, before triggering the standstill period as set out in paragraph 18 below, will test their effectiveness in combination to fully assess the impact of the Removal of Third-Party Cookies.

        ii. Google will involve the CMA in the design of such tests, and will share with the CMA the results of such tests and, to the extent necessary for the CMA to understand and evaluate the results, explanations of the data used and underlying analyses as well as, on request and where practicable, relevant analyses retained in Google's systems for the purpose of the experiment results. Google will work with the CMA to enable the CMA to understand and have confidence in the results.

iii. If Google and the CMA cannot reach an agreement regarding appropriate testing parameters the CMA may notify Google of its preferred parameters.

iv. If Google does not within 20 Working Days, unless extended by mutual consent, agree to carry out a test according to the CMA's parameters, the CMA may take action pursuant and subject to the provisions of section 31B(4) of the Act.

v. In consultation with the CMA, Google will publish the results of tests that are material to evaluating the effectiveness of the Alternative Technologies by reference to the Development and Implementation Criteria. The publication will be made in a blog post, a dedicated microsite or equally prominently. When Google publishes the results of these tests, it will also publish a description of the underlying data and methodology used that is sufficiently granular to enable publishers, advertisers and ad tech providers to understand the results and obtain an informed view of the relevance of the test and its outcome for their own businesses. For the avoidance of doubt, Google will not publicly disclose personal data, Google proprietary software code or algorithms or other business secrets. However, Google may need to disclose such data to the CMA if such data is necessary for the CMA to assess the effectiveness of the Alternative Technologies.

vi. This provision shall not prevent Google from carrying out alternative tests on the basis of its own parameters and design.

d. **User controls.** At least once a quarter, Google will update the CMA on its plans for user controls in relation to the Privacy Sandbox proposals, including default options and choice architectures, and it will share with the CMA the user research and testing which underpins its decisions on user controls. Google will take into account any observations the CMA may make with a view to ensuring that the Purpose of the Commitments is achieved.

17. **The ICO.** Google acknowledges that the CMA will involve the ICO to achieve the Purpose of the Commitments as agreed between the CMA and the ICO and subject to applicable legislation. The CMA will consult the ICO before issuing any notification under paragraph 19.

F. Standstill before the Removal of Third-Party Cookies

18. Google will not implement the Removal of Third-Party Cookies before the expiry of a standstill period of no less than 60 days after Google notifies the CMA of its intention to implement their Removal. Google may increase the length of such a standstill period at any time between giving such notice and the period's expiry. At the CMA's request, Google will increase the length of this standstill period by a further 60 days to a total of 120 days.

19. During the standstill period, the CMA may notify Google that competition law concerns remain concerning Removal of Third-Party Cookies such that the Purpose of the Commitments will not be achieved.

20. If Google and the CMA do not resolve those competition law concerns during the standstill period referred to in paragraph 18, the CMA may take action pursuant and subject to section 31B(4)(a) of the Act. In such circumstances the CMA will have reasonable grounds for believing that there has been a material change of circumstances since the Commitments were accepted.

21. Nothing in these Commitments prevents the application of any part of section 31B(4) or other provisions of the Act.

22. Where section 31B(4) applies, the CMA may continue the investigation, make a decision within the meaning of section 31(2) of the Act, or give directions under section 35 (interim measures) of the Act.

G. Google's use of data

23. **Third-party inventory.** Google commits not to use any Individual-level User Data from the sources listed below in its ads systems to track users for the targeting or measurement of digital advertising on third-party inventory on the web after the Removal of Third-Party Cookies:

    a. Google's current and future user-facing services, including Android;

    b. a user's Chrome browsing history, including synced Chrome history;

    c. a publisher's Google Analytics account;[5] and

    d. uploaded by an advertiser to Customer Match in accordance with Google's Customer Match policy.

24. **Google owned and operated inventory.** Google commits not to use any Individual-level User Data from the sources listed below in its ads systems to track users for the targeting or measurement of digital advertising on Google owned and operated inventory on the web after the Removal of Third-Party Cookies:

    a. a user's Chrome browsing history, including synced Chrome history; and

    b. a publisher's Google Analytics account.[6]

25. Nothing in paragraphs 23 or 24 prevents indirect use of the data types listed**,** use to prevent spam and fraud, or use in or for Google services not included under paragraphs 23 and 24.

H. Non-discrimination

26. Google will design, develop and implement the Privacy Sandbox proposals in a manner that is consistent with the Purpose of the Commitments and takes account of the Development and

[5] Google Analytics plans to continue to allow customers to use their first-party data to support publisher monetization within their own sites. Google Analytics does not use data across unaffiliated publishers for publisher monetization, though customers may choose to share or export their analytics data, including through a linked Google Ads account for ads targeting and/or measurement elsewhere.

[6] See footnote 5. Note that Google owned and operated properties are third-party with respect to non-Google publishers.

Implementation Criteria mentioned in paragraph 9, ensuring that it does not distort competition by discriminating against rivals in favour of Google's advertising products and services. In particular, Google will not:

a. Design and develop the Privacy Sandbox proposals in ways that will distort competition by self-preferencing Google's advertising products and services;

b. Implement the Privacy Sandbox in ways that will distort competition by self-preferencing Google's advertising products and services; or

c. Use competitively sensitive information provided by an ad tech provider or publisher to Chrome in a way that distorts competition.

I. Reporting and compliance

27. Google will:

a. provide the CMA with quarterly reports within three Working Days of the end of each three-calendar-month period following the Effective Date about: progress on the Privacy Sandbox proposals; updated timing expectations; and explanations of how Google has taken into account observations made by the CMA. The quarterly reports will include a signed Compliance Statement in respect of paragraphs 23, 24 and 26 of these Commitments. The Compliance Statement will be signed by the CEO (or an individual with delegated authority) on behalf of each company giving the Commitments and will be in the form included in Annex 2 to these Commitments;

b. provide in respect of paragraphs 23, 24 and 26 above a quarterly Monitoring Statement in a form agreed upon with the CMA within three Working Days of the Effective Date and every three-calendar-month period thereafter explaining the means by which Google will ensure that it monitors internally that it remains compliant with those paragraphs of the Commitments;

c. promptly notify the CMA, as soon as practicable (and, at the latest within five Working Days) by email at [RemediesMonitoringTeam@cma.gov.uk], if it becomes aware of any breach of the Commitments, and commits to providing information concerning the nature and duration of such breach. Google will not be taken to be aware of a breach for a reasonable period during which it is considering whether conduct is or is not in compliance;

d. promptly take all actions reasonably required to remedy a breach; and

e. provide to the CMA any information and documents which the CMA requests for the purposes of enabling the CMA to monitor and review the operation of the Commitments or any provisions of the Commitments or for the purposes of their enforcement.

28. Google UK Limited and Google LLC will not in any way circumvent, by actions and/or omissions any of the Commitments, including by selling, assigning or otherwise transferring

any part of the businesses involved in the Privacy Sandbox to any other entity within the Google corporate Group as a result of which that entity would do anything that is prohibited by these Commitments.

J. Duration

29. The Commitments will terminate on the earlier of (i) the two year anniversary of the Removal of Third Party Cookies; and (ii) five years from the date they are accepted by the CMA, unless released at an earlier date in accordance with section 31A(4) of the Act.

K. Variation or substitution

30. Google may offer a variation or substitution of the Commitments as envisaged by section 31A(3) of the Act.

L. Effect of invalidity

31. Should any provision of these Commitments be contrary to law or invalid or unenforceable for any reason, Google will continue to observe the remaining provisions, which shall remain valid and enforceable.

M. Governing law and jurisdiction

32. The Commitments will be governed by and construed in all respects in accordance with English law.

33. Disputes arising concerning the Commitments will be subject to the exclusive jurisdiction of the courts of England and Wales.

34. Google LLC irrevocably appoints Sisec Limited, 21 Holborn Viaduct, London EC1A 2DY as its agent to receive on its behalf in England or Wales service of any proceedings in connection with these Commitments. Such service shall be deemed completed on delivery to such agent and shall be valid until such time as the CMA has received prior written notice that such agent has ceased to act as agent. If for any reason such agent ceases to be able to act as agent or no longer has an address in England or Wales, Google LLC shall forthwith appoint a substitute acceptable to the CMA and deliver to the CMA the new agent's name and address within England and Wales.

**

Annex 1

Google will provide the following information in relation to the use cases set out below, by reference to each quarter (e.g., Q3 2021, Q4 2021...):

1. Currently anticipated opening of application programming interface (API) origin trial
2. Currently anticipated start of notice period prior to Removal of Third-Party Cookies
3. Currently anticipated Use Case general availability
4. Currently anticipated Transition Period for Removal of Third-Party Cookies

The use cases for which such information will be provided, and distinct APIs for which information will be shown, are as follows (if the development of an API is discontinued, and/or an alternative API developed, such changes will be reflected):

1. Use Case: Show relevant content and ads
    - FLoC
    - FLEDGE

2. Use Case: Measure digital ads
    - Core Attribution API
    - Aggregate Reporting API
    - Cross-environment Attribution API
    - Aggregation Service Reference API

3. Use Case: Fight spam and fraud on the web
    - Trust tokens

4. Use Case: Improve the web platform infrastructure
    - First-Party Sets
    - Fenced Frames
    - Shared Storage
    - CHIPS
    - Storage Partitioning

Information on the earliest anticipated date for availability will be provided for the following measures to promote a more private web (if the development of a measure is discontinued, and/or an alternative measure developed, such changes will be reflected):

- UA-Reduction
- Same-Site cookies
- Origin-bound cookies
- DoH
- Network state partitioning
- IP address privacy
- Privacy Budget
- Web ID

Annex 2
Template Compliance Statement

[Note: Quarterly Compliance Statements will be provided to the CMA within three Working Days of the end of each three-calendar-month period following the Effective Date for the duration of the Commitments]

I, [insert full name], [Chief Executive Officer/title of authorised delegate] of Google confirm that for the three months to [amend date as appropriate], [Google] has complied with the following obligations in the preceding three-calendar-month period dated [insert dates covered by this Compliance Statement]:

Relating to Google's use of data:

1. Google commits not to use any Individual-level User Data from the sources listed at paragraph 23 of the Commitments in its ads systems to track users for the targeting or measurement of digital advertising on third-party inventory on the web after the Removal of Third-Party Cookies;

2. Google commits not to use any Individual-level User data from the sources listed at paragraph 24 of the Commitments in its ads systems to track users for the targeting or measurement of digital advertising on Google owned and operated inventory on the web after the Removal of Third-Party Cookies;

Relating to non-discrimination:

3. Google will design, develop and implement the Privacy Sandbox proposals in a manner that is consistent with the Purpose of the Commitments and takes account of the Development and Implementation Criteria, ensuring that it does not discriminate against rivals in favour of Google's advertising products and services.

This includes, but not is limited to, the actions listed at paragraph 26 of the Commitments.

Any failures to meet the Commitments during this three-calendar-month period were notified to the CMA within five Working Days of Google becoming aware of them and are also listed below for completeness.

Signed.....

Full name.....

Date.....

[Commitments to be listed on following page for completeness]

**

Appendix 2: Google's Privacy Sandbox Proposals

1. Google's Privacy Sandbox refers to Google's proposal to phase out support for TPCs and other means of cross-site tracking and introduce a number of alternatives to replace some of the functionality of TPCs.

2. This Appendix sets out the CMA's current understanding of proposals included in the Privacy Sandbox which are relevant for this notice of intention to accept commitments.[114]

First-Party Sets

3. Currently, the web standards community defines a TPC as a cookie which has been set by a domain which is different to the domain that a user is currently on. Cross-site tracking more generally is also defined by this pattern: identifiers are used to link a user's behaviour across different sites, also known as domains.

4. Following Google's intention to remove TPCs and other forms of cross-site tracking,[115] Google's proposal is to introduce "a mechanism by which a set of registrable domains (a "First-Party Set") can declare themselves to be the same "party" or entity, such as web properties owned by the same company, or domains with different ccTLDs used by the same website".[116]

5. Google has told the CMA that "Under the First-Party Sets mechanism, developers of multiple domains belonging to the same organisation will maintain the ability to access their own cookies […] across their own domains, as these domains will be treated as first-party properties for this purpose."[117] Such cookies will not therefore be categorised by Chrome as TPCs and will enable cross-site tracking across multiple domains or web properties, where those domains or web properties belong to the 'same organisation'.

6. Google has told the CMA and the ICO that First-Party Sets is at an early stage of development and that therefore this definition is potentially subject to change.

---

[114] To form its understanding the CMA has relied on publicly available information such as blog posts and discussions in relevant developer fora as well as meetings with and submissions by Google and third parties. See, in particular, The Privacy Sandbox - The Chromium Projects. For more information on the Privacy Sandbox see Digging into the Privacy Sandbox (web.dev), December 2020 and What is the Privacy Sandbox? - Chrome Developers, May 2021

[115] See paragraph 3.22 above.

[116] Google, Intent to Experiment: First-Party Sets and 'SameParty' cookie attribute, February 2021.

[117] Google, Submission of 29 January 2021 in response to Questions 8, 14, 15 and 18 of CMA's RFI dated 7 January 2021, paragraph 11.

Interest-based targeting

7. Currently, market participants use TPCs and make use of other web functionality as tracking methods such as link decoration, localStorage, iframes, User-Agent HTTP header and IP addresses to track users across multiple websites on Chrome,[118] to form profiles and infer individual user interests from browsing histories, in order to target individual users with relevant advertising (interest-based targeting, also known as behavioural targeting). The below proposal is Google's suggested replacement for interest-based targeting using TPCs.

Federated Learning of Cohorts ('FLoC')

8. Under the FLoC proposal, the user's browser would use a clustering algorithm to assign itself to a cohort based on the user's browsing history. Users with similar browsing histories would be more likely to be assigned to the same cohort. Cohort assignments would be re-allocated regularly, based on the user's recent browsing history (the current proposal is seven days). When the user accesses a web page, the browser would send a cohort ID to the website, which the publisher could include in ad requests, allowing ads to be targeted based on cohort.[119] Google aims to ensure that cohorts have a minimum size of k users, so that users cannot be distinguished from others in that cohort (k-anonymity).

9. Google has experimented with different methods to cluster users into cohorts.[120] These methods have different requirements for collecting and processing users' browsing histories centrally.

    a) Simpler clustering algorithms can calculate a user's cohort ID without using any other user's information, so there is no need for centralised collection of users' browsing history. However, to enforce minimum cohort size and ensure k-anonymity, a central server is needed to track the size of each cohort, so browsers need to send some information to a central server.

    b) By contrast, centralised clustering algorithms use information across multiple users to assign a cohort ID to each individual. Some implementations would require a centralised server to have access to the raw browsing history of all users but could achieve more

[118] Often these methods are combined to provide a robust signal that tracks a user across sites. For example, in this blog post iframes and localStorage are combined to achieve cross-site tracking. localStorage can hold more data (5MB) than a cookie (4KB).
[119] In addition to this, publishers can make use of a cohort ID for profiling themselves, if they wish.
[120] Google Research & Ads, Evaluation of Cohort Algorithms for the FLoC API, 21 October 2021.

useful cohorts for a given minimum cohort size. Google at one point considered using federated learning to overcome this requirement and keep user-level data on-device (the devices of users on which their browsers run) but has yet to demonstrate how this would work in practice.

10. Currently, market participants analyse and draw their own inferences from users' browsing histories (which they collate using TPCs and other forms of tracking) that are relevant and useful for their own purposes. By contrast, under the FLoC proposal, all advertisers and market participants will have access to the same set of FLoC cohort IDs.

11. It is not yet clear: (i) whether other browser providers (should they choose to implement FLoC) will use the same central server to track cohort sizes, with the same clustering algorithm, using the same topic categories or domains to extract user browsing features for clustering; (ii) how Google will ensure that cohorts cannot be abused by supporting inferences about sensitive category data; (iii) what controls users will have about their cohort ID and which parts of their browsing history will be used for FLoC; or (iv) whether Google will have a competitive advantage relative to other market participants in interpreting the interests or characteristics of each cohort.

Retargeting

12. Retargeting is the practice of serving targeted ads to specific individuals who have visited an advertiser's website. For example, an advertiser may wish to show an ad of the specific product that a user has browsed or placed in a basket on its website. For retargeting to be possible following the deprecation of TPCs, a mechanism is needed for advertisers to create their own targeting cohorts or 'interest groups'.

13. There have been a number of different proposals put forward by Google and other market participants aimed at allowing advertisers to retarget users, whilst meeting Google's aim of preventing cross-site tracking. Google's proposal is TURTLEDOVE, which it has refined over time in response to feedback and ideas in counterproposals (such as SPARROW, PARROT, TERN and Dovekey). FLEDGE is an early prototype to experiment with ad serving using TURTLEDOVE ideas. The CMA understands that Google's latest position on TURTLEDOVE is set out in its explainer for FLEDGE.[121]

[121] See turtledove/FLEDGE.md at main · WICG/turtledove · GitHub

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

14. Advertiser websites ask browsers that visit to join one or more interest groups for a limited amount of time. A key difference with current retargeting approaches using TPCs is that the advertiser does not keep information about which browsers are in which interest groups. For each interest group, the browser stores information about who owns the group, JavaScript code for bidding logic,[122] and how to periodically update that interest group's attributes. Browsers will prevent individual-level targeting by only showing ads and allowing updates for interest groups that are targeted to at least 100 people (although it is unclear how this can be enforced without a centralised server, similar to how a central server is needed to track the size of each FLoC cohort). Later, when a browser visits a different webpage with an opportunity to show a display ad, the browser will run an on-device auction,[123] using appropriate auction logic determined by the seller. The auction may produce no winning ad, in which case the seller may choose to show a contextually targeted ad.[124]

15. Eligible interest groups have an opportunity to bid. The browser executes each interest group's bidding logic. For each eligible interest group, the browser may make an uncredentialed (cookieless) fetch from a 'trusted' key-value server,[125] allowing the buyer (the advertiser or DSP) controlling the interest group to make the browser take account of real-time data (such as the remaining budget of the ad campaign). Advertisers and DSPs upload information (key-value pairs) to the trusted server in advance. The governance and technical guarantees of this 'trusted' key-value server have yet to be fully developed. As part of the proposal, at a minimum, the server must not do any event-level logging or allow other market participants to be able to access information that would enable them to correlate or link interest group requests with other bid requests (such as for contextual ads) that are sent when users visit a website.

16. The winning interest-group ad is rendered in a **Fenced Frame**, a mechanism that is under development that would prevent the surrounding webpage from learning about the contents in the frame, and thereby leaking information

[122] This contrasts with a number of other counterproposals, such as SPARROW, which allow for the bidding logic to be hosted by a trusted server (a Gatekeeper) rather than in the browser.
[123] Again, this contrasts with SPARROW, which allows the auction to be run by a trusted 'Gatekeeper' server rather than in the browser.
[124] At the moment, more design work is needed for TURTLEDOVE and FLEDGE to be able support multi-level decision-making which are commonly used in modern adtech supply paths, with multiple auctions, header bidding, etc.
[125] For FLEDGE, as a temporary mechanism, buyers can use any server.

about the user's ad interests.[126,127] Google's original proposal is that the browser will only serve ad content that was previously downloaded (that is, requiring the browser to pre-download interest-group ads). In the explainer for FLEDGE, Google entertains the possibility that advertisers and DSPs could upload ads on to a 'trusted' CDN server that does not keep logs of the resources it serves, from which browsers could render ads. As with the trusted key-value server, the governance and technical guarantees of the trusted CDN server have yet to be fully developed.

17. TURTLEDOVE will need to allow sellers and bidders to learn the outcome of the auction. As a temporary mechanism, FLEDGE as originally proposed would allow sellers and buyers to send event-level reports to their servers, to perform logging and reporting on the auction outcome (as well as verification of viewability, etc.). More design work is needed on a 'trusted-server' reporting mechanism that does not allow reporting to be used to learn the interest groups of users visiting the publisher's site.

Measurement, attribution and reporting

18. Currently, TPCs are used to determine whether and how many ads have been served successfully to users that were in targeted groups (measurement), and to help assess ad effectiveness by determining whether views and clicks on the ads led to conversions (attribution). The outcomes of ad auctions and delivery need to be reported to advertisers and publishers (reporting), to facilitate payment and show performance of contracts.

19. Privacy Sandbox contains some proposals for measurement, attribution and reporting following the removal of TPCs.[128]

Event Conversion Measurement API

20. This proposal would allow advertisers to attach a set of metadata (including an impression ID, intended conversion destination, expiry dates) to their ads, which would be stored by the user's browser when the ad is clicked. If the user visits the intended destination page and converts, the browser records the conversion event and, with a delay (potentially one day), sends a report to the publisher and advertiser (potentially via a common ad tech intermediary) that a conversion occurred which can be attributed to a click on an impression, without the inclusion of any information about the user.

[126] As a temporary mechanism, FLEDGE will allow frames to communicate with outside servers.
[127] For the explainer of Fenced Frames see, Google, GitHub - shivanigithub/fenced-frame, May 2021.
[128] See, Google, Attribution Reporting - Chrome Developers, May 2021.

21. Under Google's proposal, there are some limits on the amount of information that would be stored by the browser. The browser will store a 64-bit identifier for each ad click, enough for a unique ID for every click, so every click can be mapped to detailed data about the user. The browser will only allow 3-bits of conversion data (ie eight distinct values) to be attached to the conversion event, so that conversion events cannot be mapped to detailed data about the user. Chrome will add noise to the conversion data, so that (as currently proposed) 5% of the time Chrome will report a random 3-bit value instead of the actual conversion data.

22. Chrome will report up to three conversion events per click and will send up to three reports (if the browser is open) within reporting windows (eg 2 days after ad click, 7 days after ad click, and a maximum of 30 days after ad click).

23. Market participants currently use a variety of attribution models (ie ways of assigning credit for a conversion to events leading up to it). Google's proposal allows only for last-click attribution, ie all the credit for the conversion is given to the website hosting the ad that was last clicked, and all other relevant ad clicks or views before the conversion are given no credit.

24. Future extensions to this proposal, potentially integrated with an aggregation service (discussed in the next section), could support view-through attribution, multi-touch attribution models, web conversions that started in a mobile app, multiple reporting endpoints, and measuring causal differences in conversion (ie additionality).[129]

25. The Event Conversion Measurement API was made available to developers for origin trials on 6 October 2020, and the current trial is expected to end on 14 July 2021.[130]

Aggregated reporting: Multi-browser aggregation service, Aggregate Conversion Measurement API, and Aggregated Reporting API

26. Google has explored designs for a 'multi-browser aggregation service', a mechanism that would be able to aggregate information from multiple sources (such as browser clients or websites) in a privacy-preserving way, without the entity performing the aggregation from learning the underlying data from each source.[131]

[129] Google, A more private way to measure ad conversion, the Event Conversion Measurement API, 6 October 2020.
[130] Chrome Origin Trials, Trial for Conversion Measurement, ending July 2021.
[131] Google, Multi-Browser Aggregation Service Explainer, April 2020.

27. Google explores how some of the limits of the Event Conversion Measurement API (discussed in the previous section) can be overcome, without compromising on privacy, through aggregating data across multiple users' browsers. For example, it may be possible for market participants to have more granular conversion data (more than 3-bits), view-through and multi-touch attribution models. Using a multi-browser aggregation service, an Aggregate Conversion Measurement API could combine information from multiple browser clients in a report that is only sent if there is sufficient aggregation.[132]

28. In addition, the aggregation service may also support a generic Aggregated Reporting API, which can combine information across multiple websites into a single report, supporting use-cases like measuring reach (the number of distinct users that viewed an ad), and a form of frequency capping (although this would be a per-user per-publisher cap, rather than a per-user cap, which is calibrated using aggregated data).[133]

Combating Spam and Fraud

29. Websites currently rely on identifiers and cross-site tracking to establish whether a user is trustworthy or engaged in spam or fraud. Privacy Sandbox Proposals include proposals for a Trust Token API.[134] The aim of this API is for trust signals to be transmitted between websites without creating a stable, global identifier unique to each user. Rather the Trust Token API aims at segmenting users in 'trusted' and 'untrusted'. To do so a website that established a user's trustworthiness would be able to issue that user's browser with trust tokens. These tokens could then be redeemed on other websites establishing trust without identifying the user or providing information on the origin of the token.

Limiting Data Collection – Combating Fingerprinting

30. Privacy Sandbox contains other proposals to mitigate workarounds that market participants may use to continue cross-site tracking without the use of TPCs.

31. This section focuses on selected proposals that aim explicitly to combat fingerprinting, the practice of collecting, linking and using a wide variety of information about the browser, other software, or the hardware of the user, in conjunction, for the purpose of identification and tracking. Unlike cookies,

[132] Google, Conversion Measurement with Aggregation Explainer, May 2021.
[133] Google, Aggregated Reporting API, September 2020.
[134] Google, Trust Token API Explainer, August 2019.

which can be deleted by users to prevent identification via that particular vector, many of the browser and system characteristics used for fingerprinting cannot be modified by the user easily (such as system fonts).[135]

32. Much of the identifying information that could be used in fingerprinting is part of how the internet and World Wide Web currently work and is requested and used by websites that do not engage in fingerprinting to provide necessary and useful functionality to users.

User-Agent Client Hints API and Privacy Budget

33. Currently, when browsers send requests to a web server to load content, browsers send a user-agent string which tells the web server information about the user's browser and device. This information can be useful for websites (for instance, to select the most suitable version of a website for the user's browser and device, or to monitor for fraud and abuse), but it also reveals extra information that can be used for fingerprinting.

34. Under the Privacy Sandbox Proposals, the amount of information that is made available to websites via the user-agent string will be reduced. Instead, websites can request additional information from browsers about specific features, and browsers may give specific 'hints' in response. Whether the browser will provide correct information will depend on how much information is requested (in the sense of how 'uncommon' or identifying that information is), and the website's available Privacy Budget.[136]

35. Under the Privacy Budget proposal, Chrome will assign an information budget to each website and monitor the information provided to each website. When a website has used up its budget, Chrome will stop sending correct information, substituting it with imprecise or noisy results or a generic result that does not vary between users. Budget increases for specific information can be requested.

[135] For an overview of fingerprinting see Market Study, Appendix G, pages 14–19.

[136] Privacy Budget is measured in bits as done in information theory. Bits are the units of entropy and self-information, which are measures of information content. To illustrate, suppose an identifier X can only take one of two values (A or B) with equal probability (0.5). If we learn for an individual that the value of the identifier is A, then the 'self-information' of this particular outcome is 1 bit. The entropy is the expected value of the self-information of all possible outcomes and indicates how 'informative' or 'surprising' learning the value of that identifier would be on average. 33 bits of identifying information would be enough to uniquely identify a single person out of 7.8 billion people. Crucially, in practice, the amount of entropy of an identifier depends on context and what else is already known. For example, if an individual's postcode is known, the added information of their city gives no additional bits of information.

Global Network Address Translation Combined with Audited and Trusted CDN or HTTP-Proxy Eliminating Reidentification ('GNATCATCHER')

36. IP addresses have primarily carried out two functions: to identify the host of a network interface; and to provide the addressable location of the host in the network, allowing a path to that host to be established. However, by their very nature, IP addresses also are a close-to unique identifier for web users, and a unique identifier for a browser at a point in time, and they can be found easily on and routed over the open internet.

37. Given widespread availability of IP addresses and their ability to provide a somewhat stable signal over some amount of time, they are often used by advertisers, publishers and ad tech providers in conjunction with other identifiers to identify and track users across sites. When used in combination with additional geolocation software, can also be used to determine the approximate geographic position of a user's device for localised advertising. IP addresses are also important identifiers in the enablement of cross-device tracking.[137]

38. The GNATCATCHER proposal, which combines two previous proposals 'Near-Path NAT' and 'Wilful IP Blindness', has the goal of reducing the amount of information available in a given IP address that websites see during network address translation.[138]

39. The Near-Path NAT proposal allows a browser to forward its HTTP traffic through an IP privatising server, utilising the end-to-end encryption of TLS.[139] This would mask a user's original IP address from other third-party organisations, by allowing users to send their traffic through the same server, so it appears to originate from the same pool of IP addresses.[140] This service, applied across Google Chrome would operate similarly to services that already exist in market for consumers wishing to hide their IP address when using the internet (ie Virtual Private Network services or like a traditional NAT).

40. The Wilful IP Blindness proposal would give sites the option to self-certify that their servers are masking IP addresses when transferring information. This

[137] Cross-device tracking is discussed in the Market Study, Appendix G, paragraphs 14-47.
[138] The GNATCATCHER GitHub Explainer is set out here. The GitHub explainers for both previous proposals can be found here (Near-Path NAT) and here (Wilful IP Blindness). Network address translation (NAT) is the method of translating (mapping) between one IP address space and another by putting information in IP header of packets while in transit.
[139] Transport Layer Security (TLS) is a cryptographic protocol to encrypt communications over a computer network. It is used as the main network security mechanism for the application layer of network communication on the web, and is what puts the S in HTTPS.
[140] Routing traffic through a proxy-server causes all traffic to appear to originate from the same pool of IP addresses.

could be implemented, for example, by use of a HTTP header. The intention behind this is to make IP addresses an active surface, that can be accounted for in Privacy Budget, rather than a passive one.[141] Under the proposal, the policy could be enforced by introducing audits and spot-checks (accounted for in the Privacy Budget). Parties who do not opt into Wilful IP Blindness may be subject to the Near-Path NAT, or alternatively both could be implemented across the board.

Federated Log-in

41. Federated log-in allows users to use a single method of authentication (eg username and password) to access multiple websites, rather than creating a new username and password for each website. This is commonly experienced by users as 'log in with identity provider X to website Y'. Another common application is to log in to enterprise accounts in one place and be signed in in many places thereafter, although this is more precisely referred to as 'single sign-on'.

42. Currently, some federated log-in systems use cookies, link decoration and redirects, and it is possible that the identity provider and websites can use federated log-in systems to track users across multiple websites and build a profile about users' browsing activity.[142]

WebID

43. The WebID proposal aims to prevent federated log-in being used for cross-site tracking, while preserving its intended functionality. At this stage, Google has explored three variations of potential solutions, and it is not yet clear which form the proposal will ultimately take (eg whether the variations complement each other or are mutually exclusive). It could mean that the browser adds more friction (eg in the form of permission prompts) or takes control of choice architecture around the use of federated log-in. It could also mean that website federated log-in systems could delegate a log-in to the browser, effectively making the browser a delegated representative of the identity provider.

44. The weaker variations of the proposal include the 'permission' variation. Under this variation, the user-agent (the browser) would provide warnings and consent notices to the user when a tracking risk appears during the handshake between the website the user wants to log into (referred to as the

[141] More on passive fingerprinting surfaces is discussed in the Privacy Budget repository on Github.
[142] More on the threat model of various non-essential to login related tracking is set out on the WebID GitHub page here.

'relying party') and the identity provider. The tracking risk this variation mitigates is that of the relying party accessing user data without the user's awareness. The challenge of this variation is that it may add friction to user experience or lead to warning fatigue.[143]

45. The stronger variations of the proposal include the 'mediation' and 'delegation' variations.

    (a) Under the mediation-oriented variation, the consent prompts are bundled in with the user's initial action to request to sign-in with an IDP. There would be some controls in general browser settings about this.[144,145]

    (b) Under the delegation-oriented variation, the identity provider fully delegates the presentation of identity assertions to the browser.[146]

[143] More on the permission-oriented variation can be found on the WebID Github pages here and here.
[144] For example, the user could change their default settings as to whether they want to opt-in to sharing their directed profile (a set of fields including identifiers such as email address) when logging in to a site via an identity provider.
[145] More on the mediation-oriented variation can be found on the WebID Github pages here and here.
[146] More on delegation-oriented variation can be found on the WebID Github pages here and here.