CMA Q1 2024 update report on implementation of the Privacy Sandbox commitment

April 2024

CONTENTS

Summary

1. This report sets out the CMA's updated views on the issues we identified in our January 2024 report concerning Google's proposed Privacy Sandbox changes (see **Annex 1**). Our analysis is based on the framework for assessment set out in the legally binding Commitments that Google made in February 2022 to address competition concerns relating to its proposals to remove third-party cookies from Chrome. The January 2024 report set out our provisional views on the impact of the Privacy Sandbox on competition, publishers and advertisers and user experience.

2. We outline Google's response to the concerns we identified in that report and the steps it is taking to resolve pending issues. We have also considered the feedback received from market participants on these points. We have included a summary of this feedback in the sections below.

3. This report also incorporates the preliminary assessment of the Information Commissioner's Office (**ICO**) on the privacy and data protection impacts of the Privacy Sandbox. Having consulted with the ICO, we set out our current views on these concerns for each of the APIs.

4. Although there are a number of concerns to work through, based on the available evidence, we consider that from 1 January 2024 to 31 March 2024 (the relevant reporting period), Google has complied with the Commitments. This means that in our view Google has followed the required process set out in the Commitments and is engaging with us (and the ICO) to resolve our remaining concerns ahead of third-party cookie deprecation. However, further progress is needed by Google to resolve our competition concerns ahead of deprecation.

5. We will continue to work with Google to resolve our concerns[1] between now and the point at which Google triggers the Standstill Period.[2] We will provide an update on progress in our next update report.

6. Testing of the Privacy Sandbox tools is also currently underway. The test results will form part of a wider evidence base that we will use to assess the

[1] Paragraph 17.a.ii of the Commitments enables us to raise issues with Google, and for Google to work with the CMA without delay to seek to resolve concerns raised.

[2] Under paragraph 19 of the Commitments, Google must allow for a Standstill Period of at least 60 days before third-party cookies can be removed. This period can be extended to 120 days.

effectiveness of the Privacy Sandbox. The test period runs until the end of June this year.

7. Given the time needed to resolve outstanding issues and take account of testing results, we have agreed with Google that there should be a limited delay to third-party cookie deprecation. Subject to resolving our remaining competition concerns, Google is now aiming to proceed with third-party cookie deprecation starting in early 2025. Under the Commitments, it is for Google to decide when the Standstill Period is triggered.

8. We encourage market participants taking part in testing to submit their results directly to us by the end of June deadline. We also welcome any additional feedback from stakeholders on the concerns identified in this report. Our contact details are included at the end of this report.

Dashboard

Dashboard: summary of CMA view on current position, January-March 2024

Relevant section of Commitments	Compliance	Level of focus by CMA[3]	Key actions during period	Summary of planned next steps
D - Transparency and consultation with third parties	**Compliant**	**Higher focus**	• Engagement with Google and market participants on the development of individual proposals (e.g. Protected Audience API) • Following up on the recently published update to our guidance on testing	• Engaging with Google and other market participants to resolve concerns relating to the development of the Privacy Sandbox tools • Following up on the recently published update to our guidance on testing
E - Involvement of the CMA in the Privacy Sandbox proposals	**Compliant**	**Higher focus**	• Encouraging testing and trialling by Google and other market participants • Engaging on design issues including approach to Related Website Sets, Protected Audience API and Attribution Reporting API	• Engaging with Google and other market participants to resolve concerns relating to the development of the Privacy Sandbox tools • Encouraging testing and trialling by Google and other market participants and engaging with market participants that intend to test
F - Standstill before the Removal of Third-Party Cookies	**Compliant**	**Medium focus**	• Preparing for the standstill, including by identifying remaining competition concerns and through testing and trialling	• Continuing to prepare for the standstill, including through resolving remaining competition concerns and through testing and trialling (see above)
G - Google's use of data	**Compliant**	**Medium focus**	• Focus on Google's internal data control systems (particularly anti-abuse activities and paragraph 26 data use) • Work to ensure that necessary data use protections are fully implemented well in advance of third-party cookie deprecation	• Resolving additional questions regarding Google's internal data control systems (with a particular focus on paragraph 27) • Continuing to develop a framework for ongoing monitoring following third-party cookie deprecation
H - Non-discrimination	**Compliant**	**Medium focus**	• Continued engagement with Google around attestation and enrolment, design decisions (including Related Website Sets, Protected Audience API, Attribution Reporting API), and governance following third-party cookie deprecation • Further testing Google's internal decision-making process, particularly at key decision points. Incorporation of market commentary and testing feedback • Applying technical knowledge to monitoring artifacts and logs	• Continuing engagement with Google regarding attestation and enrolment, design decisions, and governance following third-party cookie deprecation • Continuing to monitor artifacts and logs
I - Reporting and compliance	**Compliant**	**Lower focus**	• Completion of regular monitoring report(s)	• Google to continue demonstrating ongoing compliance • Preparing for next monitoring report(s)

Note: this is a summary, so it cannot provide comprehensive details on all topics

Context and framework of our assessment

9. We have set out below our current views on the proposed Privacy Sandbox changes. The framework for our assessment, which is based on the Development and Implementation (**D&I**) Criteria set out in Google's Commitments, is summarised in **Annex 2**.

10. We have been consulting the ICO on the aspects of the Privacy Sandbox that relate to matters of privacy and data protection.[4] The ICO has shared with us its provisional views on the impact of the Privacy Sandbox on privacy outcomes and compliance with data protection principles and the Applicable Data Protection Legislation. For each of the APIs, it has summarised key outstanding privacy and data protection concerns.

11. We have considered the ICO's views on privacy and data protection concerns and incorporated these into our report for each of the APIs in the section below. An overview of the ICO's approach to reviewing the Privacy Sandbox tools is included in **Annex 2**.

12. The CMA-ICO joint statement on competition and data protection explores the intersection between our regimes.[5] Both this joint statement as well as the ICO's Opinion on data protection and privacy expectations for online advertising proposals dated 25 November 2021 (**2021 Opinion**),[6] note that the CMA and ICO will work closely to assess the Privacy Sandbox, with a view to supporting positive competition and privacy outcomes in online advertising markets. In the Privacy Sandbox context, it may be the case that specific examples of Google interventions to improve alignment with data protection principles and the Applicable Data Protection Legislation have negative impacts on some ad tech firms, and advertiser and publisher outcomes. We are mindful of this risk and the need for careful consideration of these issues so that competition and data protection objectives are promoted overall to the benefit of consumers.

[3] While all aspects of the Commitments are important, this column refers to the relative priorities of the CMA, and which have required a greater focus, during the course of the reporting period.

[4] See paragraph 18 of the Commitments.

[5] CMA-ICO joint statement on competition and data protection law dated 19 May 2021.

[6] See the 2021 Opinion.

Overall competition concerns

13. The January 2024 report identified a series of areas that could raise competition concerns, which relate to the design of the individual the APIs. Since the last report was published, we have received further submissions from Google on some of the concerns and additional views from stakeholders, including on new concerns identified. Our updated views on each tool based on this feedback are set out in the next section.

14. In addition, we set out in our January 2024 report several key concerns that Google will need to resolve ahead of third-party cookie deprecation:

    (a) **Ensuring that Google does not design, develop or use the Privacy Sandbox tools in ways that reinforce the existing market position of its advertising products and services, including Google Ad Manager (GAM).** GAM is Google's integrated ad server and supply side platform (SSP), accounting for more than 90% of the display ads served in the UK.[7] For example, we set out our concerns on GAM's proposed approach to Protected Audience auctions in the section below. We are continuing to discuss with Google how these concerns could be resolved.

    (b) **Clarifying the longer-term governance arrangements for Privacy Sandbox.** Google currently retains significant discretion over how Privacy Sandbox works, develops over time, and the conditions for using Privacy Sandbox (e.g. requiring attestations). This creates a risk of self-preferencing or of the perception of self-preferencing. We are continuing to engage with Google as it works to develop and refine a governance model for Privacy Sandbox. Our current view is that the model should ensure that decisions are consistent with the Development and Implementation Criteria set out in the Commitments, include elements of independent decision-making, support transparency and provide opportunities for stakeholder engagement.

15. In addition, we are discussing with Google what further restrictions may be applied on **Google's use of first-party data to target and measure ads on Google's owned and operated (O&O) inventory**.[8] We are conscious of the risk that ad spend could move away from open display and into O&O

[7] See page 270 of the CMA's Online platforms and digital advertising market study dated 1 July 2020.
[8] The Commitments already impose some restrictions (see sections G and H).

inventory (or 'walled gardens') – depending on the overall impact of the Privacy Sandbox changes.

16. Finally, market participants have raised concerns that Google's aim to restrict all cross-site tracking will **harm third-party businesses seeking to provide interest-based targeting and measurement in competition with Privacy Sandbox**. For example, concerns have been raised in the context of Google's Bounce Tracking Mitigations proposal in the section below. Although the obligations under the Commitments relate specifically to the impact of Google's introduction of the Privacy Sandbox proposals and not Google's approach towards other market participants' alternative technologies, Google's market position allows it to have a significant impact on the viability of alternative technologies that may compete with the Privacy Sandbox tools following the removal of third-party cookies.[9] Both the Privacy Sandbox tools and possible third-party alternatives will need to comply with applicable data protection legislation.[10] We are continuing to discuss this issue with Google.

17. We have raised our competition concerns with Google following the process envisaged under paragraph 17.a.ii of the Commitments. We have held a series of meetings with Google to discuss these issues. Where we have identified concerns, this does not mean that we currently think the Privacy Sandbox changes cannot go ahead, but it is important that the concerns are resolved, either through design changes, assurances from Google about action it will take or refrain from, or other evidence which resolves our concerns.

18. We will provide an update on how Google intends to resolve our concerns in the report we will publish at the end of July 2024.

Potential concerns and current views on the individual Privacy Sandbox tools

19. This section is organised by the function or use case that Privacy Sandbox APIs are intended to serve, and within each use case, by API. A summary of the relevant use cases is included in **Annex 1.**

20. We outline the concerns we have identified for each of the APIs based on the Commitments framework (**D&I A – Privacy outcomes**, **D&I B – Digital**

[9] See paragraph 4.324 of the Decision to accept commitments offered by Google in relation to its Privacy Sandbox proposals dated 11 February 2022 (**Commitments Decision**).

[10] See paragraph 4.325 of the Commitments Decision.

advertising, **D&I C – Impact on publishers and advertisers** and **D&I D – User experience**; see **Annex 2**).

Showing relevant content and ads

Topics API

Overview

21. The Topics API is intended to enable interest-based targeting.[11] It uses an on-device classifier model to generate a list of topics reflecting the user's interests based on their browsing history. The topics are selected from a human-curated, publicly available taxonomy, currently containing 469 topics.[12] Human curation is intended to ensure that topics are interpretable, for example 'Arts & Entertainment', and that sensitive topics are excluded.

22. The on-device classifier uses the site's hostname, including subdomains. For example, the site news.bbc.co.uk is assigned 'news' and the site sport.bbc.co.uk is assigned three topics: 'news', 'sport' and 'soccer'.[13] The classifier only considers the hostname.

23. Every week, Chrome will calculate (locally on the user's device) the top five topics from the user's browsing history of sites that use the Topics API that week (epoch). When callers (including third-party ad tech or advertising providers) call the Topics API, the API will return at random for the user up to three topics in total from the top five topics for each of the last three weeks; once a topic is selected for a week, user, and top-level site, it will remain constant. Google selects 'top' topics, first based on their utility ('high' or 'standard'), and then by their frequency count.[14]

Potential concerns

24. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

[11] An overview of the Topics proposal can be found here (accessed on 22 April 2024).

[12] The taxonomy is listed on the Topics GitHub page here (accessed on 22 April 2024).

[13] Accessed via chrome://topics-internals/ (accessed on 22 April 2024).

[14] See Google Developer Blog on 'Enhancements to the Topics API' here (accessed on 22 April 2024).

25. For the purposes of assessing the compliance of the Privacy Sandbox tools with data protection principles and the Applicable Data Protection Legislation, as defined in the Commitments, the ICO has drawn upon its 2021 Opinion and its Update report into ad tech and real time bidding dated 20 June 2019 (**2019 Report**).[15]

Potential concerns	**Provisional CMA views based on ICO's preliminary assessment**
Google does not provide sufficient clarity to individuals regarding how their data is used by the Topics API.	We are concerned that the Topics consent user interface may not adequately inform users about how their personal data is used or how the topics generated may be used for purposes wider than interest-based advertising (e.g. as determined by organisations that decide to use the API). To address this concern, Google has agreed to update the Topics API consent interface and to strengthen developer guidance to highlight the requirement to obtain purpose-specific consent prior to calling the API. We are awaiting the results of these updates.
Topics API makes cross-site insights available to API callers with no Google-imposed restrictions limiting the purpose of topics data to interest-based advertising only.	The ICO's 2021 Opinion[16] sets expectations that future proposals must 'clearly articulate specific purposes for processing […] and demonstrate how [they] uphold the integrity of the purpose limitation principle'. Based on the ICO's preliminary assessment, we are concerned that topics data may be used for purposes outside that specified by the API, and in so doing may harm the user and breach Applicable Data Protection Legislation. Google believes that the Topics API will primarily be used for interest-based advertising. However, Google does acknowledge that entities calling the API might use the data for other purposes. Google views the risk to users in relation to potential harmful use cases as low. However, in addition to agreeing to review the API's user transparency and developer guidance (see issue above), Google is now exploring ways to monitor potential abuse of the API. Once we receive further updates from Google on these assurances, we will consider, after consulting with the ICO, whether our concerns have been resolved.
Topics will be stored and accumulated beyond the three-epoch period (currently three weeks).	Google has stated that the Topics API has a storage limit of three epochs, with one epoch equivalent to one week (therefore equating to a three-week period overall). Google views three epochs as an appropriate amount of entropy to share with API callers. It has reached this view after assessing the

[15] See the 2019 Report and the 2021 Opinion.
[16] See page 44 of the 2021 Opinion.

Potential concerns	Provisional CMA views based on ICO's preliminary assessment
	risk of re-identification on the part of a single API caller, finding that three epochs establishes a suitable level of difficulty for doing so. The ICO's 2021 Opinion states that new solutions should ensure data is processed 'for the minimum amount of time necessary' in line with the data minimisation principle.[17] The ICO has also noted that solutions should avoid 'augmenting, matching or combining personal data without strong justification, transparency and control'.[18] Although the chosen epoch period may provide a proportionate storage limitation limit for topics data where it is used for the purposes of interest-based advertising, based on the ICO's preliminary assessment, we have concerns that API callers may process data beyond this limit without providing the user with the types of strong justification, transparency and control that the ICO's 2021 Opinion refers to thereby potentially breaching Applicable Data Protection Legislation. This raises a corresponding risk of harm. To address these concerns, Google proposes to issue improved developer guidance to communicate the responsibilities API callers have regarding consent requirements. As regards identifiability, Google is also exploring how governance and monitoring may inform future API design. We are awaiting Google providing further details of these planned changes to guidance and proposed governance measures.
The future changes to the Topics API taxonomy could introduce new privacy risks without appropriate mitigations.	We understand that Google's privacy controls regarding identifiability are constructed and informed by the granularity of the taxonomy. We also understand it is Google's view that increases to the number of categories in the taxonomy may directly improve utility and revenue for API callers, pending additional evidence. The ICO's 2021 Opinion stated that with new initiatives, organisations must consider 'any new risks they introduce, and how they will mitigate them before processing takes place'.[19] The Topics API taxonomy is a key variable when assessing privacy risk with this tool. We agree with the ICO that future utility-based changes to the taxonomy could introduce new privacy risks. Currently, we are concerned that compensating privacy controls will not be sufficiently considered, documented or implemented if utility-focussed changes to the taxonomy are undertaken. Google will need to ensure that users are put at the heart of the decision-making process as set out in the ICO's 2021 Opinion expectations, which could potentially lead to breaches of the Applicable Data Protection Legislation. Google acknowledges the sensitivity of changes to the taxonomy. An appropriate oversight and governance approach is under consideration.

[17] See page 45 of the 2021 Opinion.
[18] See page 45 of the 2021 Opinion.
[19] See page 44 of the 2021 Opinion.

26. Based on stakeholder feedback and our own analysis of the API, we have considered the following potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns identified based on further submissions from Google and other market participants since our last report was published in January 2024. New concerns raised by stakeholders during the reporting period are included at the end of the table.

Potential concerns	**CMA views in January 2024 report**	**Updated CMA views**
The Topics API is likely to disadvantage small ad techs who have a more limited 'reach' and access to targeting information compared to large ad techs.	Google's view is that the three-topic constraint applies equally to all ad techs and that ad techs are likely to supplement topics with other (e.g. contextual) signals. We consider that the impact will vary based on the degree to which an ad tech relies on the Topics API as a targeting signal. Some ad techs may have access to other sources of information about a user (e.g. through data sharing arrangements, data on logged in users or from Protected Audience interest group membership). However, unequal access to data is not a new problem, it exists today for ad techs using third-party cookies. The 'reach' problem is also not specific to Privacy Sandbox; ad techs with a larger reach have more opportunities to use third-party cookies. Privacy Sandbox means that ad techs have fewer options to extend their reach by sharing information with one another within the browser (e.g. cookie syncing, fingerprinting and bounce tracking are all limited). That does not stop them from sharing data on the server side, although this opportunity also exists today (e.g. via controller-to-controller data sharing agreements, data clean rooms or other means). Therefore, compared to the status quo, we do not consider that smaller players are likely to be disadvantaged with the introduction of the Topics API.	Since the publication of our last report, we have received further stakeholder feedback that the limitations imposed by the Topics API are not equal. Specifically, stakeholders are concerned that access to the Topics API requires certification (the process for which is governed by Google), and that GAM will have broader information about user topics compared to competitors because it is embedded on most sites. Our current view is that Google's certification process does not impose unequal limitations on stakeholders. We also consider that any information advantage received by GAM as a result of being embedded on most sites is not exacerbated by the introduction of the Topics API. We therefore maintain our view that unequal access to data is not a new problem and that, compared to the status quo, small players are unlikely to be disadvantaged as a result of the introduction of the Topics API.
Google will be less reliant on the	Sections G and H of the Commitments already impose some	Our discussions with Google are ongoing on this point.

Potential concerns	CMA views in January 2024 report	Updated CMA views
Topics API than other market participants, given its access to first-party data.	restrictions on Google's use of its first-party data. The Monitoring Trustee has a continuing role to play in verifying Google's compliance with the relevant sections of the Commitments. We will consider whether additional restrictions may be needed to resolve this concern.	
Google might advantage itself by manipulating the Topics API taxonomy which it currently controls.	Google has told us it is developing robust governance arrangements for decision-making on issues relevant to the development of the APIs. Google has said that it remains interested in stakeholder feedback on the future governance of the taxonomy and discussion of how other industry bodies can play a more active role in developing and maintaining it. We consider that transitioning ownership to an external, industry-run group could resolve concerns that Google might advantage itself by manipulating the Topics API taxonomy. The timing of such transfer will need to be discussed further with Google.	Google has informed us that it does not exclude the possibility of involving external bodies in the governance of the Topics taxonomy in the long-term. However, Google does not yet have near-term plans to transfer governance of the Topics taxonomy to an external body. We wait for Google to provide further details on the governance framework for the Topics API. Our evaluation of the governance model will consider whether the proposed approach will adequately mitigate the risks to user privacy that may occur as a result of increasing the granularity of the Topics taxonomy. As stated in our D&I A assessment of the Topics API above, any utility-focussed changes to the taxonomy will need to be accompanied by compensating privacy controls.
The level of granularity of the taxonomy may have an impact on the utility of the API for publishers and advertisers and on publishers' first-party data strategies.	Given the diversity of actors in the ad tech ecosystem, we anticipate that discussions on the most appropriate size and level of granularity for Topics taxonomy will continue. Striking the appropriate balance will be a key question for the future governance model.	Our views remain unchanged, and we await Google providing further details on its proposals for the future governance model. Our evaluation of the governance model will consider whether the proposed approach will adequately mitigate the risks to user privacy that may occur as a result of increasing the granularity of the Topics taxonomy. As stated in our D&I A assessment of the Topics API above, any utility-focussed changes to the taxonomy will need to be accompanied by compensating privacy controls.
Classification based only on hostname means that sites covering many topics contribute	Google's Q3 2023 update report states that it 'previously considered offering functionality to classify sites into topics based on page content and made the decision not to move	We maintain our view that classification based on hostname is a reasonable trade off. If we become aware of new proposals to develop the classifier model in

Potential concerns	CMA views in January 2024 report	Updated CMA views
less useful information than niche sites. For example, YouTube is assigned 'Online Communities', 'TV & Video' and 'Arts & Entertainment'.	forward based on privacy and security concerns'. We are aware of proposals from market participants that aim to balance privacy and security concerns against improving utility, for example by using permissions policies.[20] Our current view is that classification based on hostname is a reasonable trade off, but we are open to proposals to develop the classifier model in the future.	future, we will evaluate these to ensure that any potential risks to user privacy are addressed.
Publishers are concerned that their sites could be misclassified or not assigned a topic and want to control the topics that are associated with their sites.	Google has expressed concern about the risk of misclassification, e.g. where the Topics API classifier assigns a topic that the site owner considers to be incorrect.[21] Our current view is that Google's response resolves the misclassification concern and agree with Google's view that allowing site owners to control classification risks incentivising site owners to game the system.	Google's original response to this concern stated that 'the specific sites that are misclassified are no more and no less harmed by this than any other sites. This is because a site's contextual information will always be available for auctions on their site, which would provide comparable information to the correct topic, even in the case of misclassification'. Since the publication of our last report, we have received further stakeholder feedback on how the misclassification issue can be reduced. Stakeholders have requested a mechanism through which a classification can be reviewed, or at least some additional transparency on how the classification model works and determines its categories. We have relayed these suggestions to Google.
Allowing sites to selectively contribute to a user's topics could create a free-riding problem, i.e. that some ad techs can choose to observe topics without contributing to	We are aware of specific stakeholder concerns relating to SSP 'free riding' and feedback on the way Google's Q3 2023 report addressed the issue.[22] We have raised the concern with Google and will update in our next quarterly report.	Google has said that if an API caller never invokes the functionality for the browser to observe topics, the caller will never receive any topics. This means that there is no incentive for callers not to contribute to a user's set of topics. Our current view is that allowing selective observation of a user's topics is a reasonable way of maximising the utility of the API, as it

[20] See for example, issue #224 on the Topics repository on GitHub here (accessed on 22 April 2024).

[21] See page 9 of Google's Q2 2023 progress report (accessed on 22 April 2024).

[22] See issue #92 on the Topics repository on GitHub here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
the set of topics stored on the user's device.		allows callers to avoid filling the user's top five topics with items that are generic or commercially irrelevant. However, we are aware that this may have a negative impact on advertisers, as the SSPs they work with could selectively use topics to misrepresent user cohorts that are lower value (e.g. those that use Made For Advertising (MFA) and pirate sites). Our understanding is that API callers can mitigate this concern by taking commercially reasonable measures to provide advertisers with the URLs of pages where their ads were placed. We are keen to hear further feedback from stakeholders who believe they may be affected by this issue.
A site's decision to support (or not to support) the Topics API should not influence its Google Search ranking.	Google has confirmed to us that Google Search will not use a site's decision to opt-out of the Topics API as a ranking signal.[23] We consider that Google's assurance that a site's decision to support (or not to support) the Topics API will not influence its Google Search ranking should also extend to the other Privacy Sandbox tools.	We are awaiting Google's response on this point.
The Topics API relies on user consent. If consent rates are low such that Topics are unavailable, there may be knock-on effects for interest-based targeting and publisher revenue.	We recognise that Google needs to request user consent for the Topics API to operate. We anticipate that the Chrome-facilitated testing period in early 2024 will provide further information about Topics availability.	Stakeholders continue to express concern about the availability of the Topics API if consent rates are low. We expect that the Chrome-facilitated testing period will provide further information about Topics availability and its potential impact on revenue. As noted in the D&I D section below, we are continuing to engage with Google about the user choice and controls for the Topics API to ensure that users can make effective choices.
The one-week epoch means that topics are likely to be out of	Although reducing the epoch length could increase utility for advertisers, given the likely impact on privacy, on	As noted in the D&I A section above, Google defined the Topics epoch after assessing re-identification risk.

[23] See page 34 of Google's Q4 2022 progress report (accessed on 22 January 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
date, with implications for showing ads where the user may already have acted on their interest (e.g. by making a purchase).	balance, we currently consider that an epoch of 7 days may be appropriate.	Therefore, we currently consider the one-week epoch to be reasonable.
Topics API will be difficult to test until it is stable and fully implemented in Chrome.	N/A	We have received new concerns from ad techs stating that they cannot test the Topics API until it is stable and fully implemented in Chrome. While we are aware that the Topics API was shipped in Chrome M115 (on 1 August 2023), stakeholders have said that the updated Topics taxonomy only became available on the majority of traffic in mid-November 2023. They therefore seek greater assurance that the taxonomy will not change in order to meaningfully test it. We consider it reasonable for stakeholders to expect that the Topics taxonomy will change over time. We anticipate that Google's forthcoming proposals for the future governance of the Topics API will give stakeholders sufficient time to plan and provide input on the design of the API before testing and deploying it.

27. As regards the application of **D&I D – User experience**, although there have been some positive developments in the design of user controls for the Topics API, e.g. users can review the topics assigned to them and proactively add or block topics, concerns remain about the transparency of the information presented to users via the consent dialogue box and the extent to which users adequately comprehend and engage with the Topics choice.

28. We are continuing to engage with Google on resolving these concerns and asking it to take measures such as further user research and testing to enhance information transparency and user engagement with the dialogue box. Additionally, while repeated consent pop-ups, e.g. surfaced upon interacting with every publisher site, could lead to prompt fatigue and degrade user experience, we consider that providing users with adequate opportunity to revisit their Topics API preferences is important for effective decision-making. Therefore, we are exploring potential platforms for prompting users to review their preferences with Google.

Summary

29. Google needs to resolve our concerns for the Topics API, and it has agreed to take the following steps:

(a) Update the Topics API consent user interface to provide sufficient clarity to individuals on how their data is used by the Topics API.

(b) Strengthen developer guidance to highlight the requirement to obtain purpose-specific consent prior to calling the API.

(c) Implement ways to monitor potential abuse of the Topics API, particularly where it is used for purposes other than interest-based advertising.

(d) Explore how governance and monitoring may inform the future design of the Topics API.

(e) Ensure there is adequate governance of the taxonomy. We remain concerned that Google retaining governance of the taxonomy creates a risk of distorting competition between Google and other market participants. We want Google to set out a plan, with a timeline, to reassure market participants that decision-making on issues relevant to the taxonomy will be transparent and accountable to stakeholders. This could include transferring governance to an independent third party, with clear Terms of Reference to ensure that the taxonomy evolves in a way that balances utility for interest-based targeting with minimising re-identification risks.

30. In addition to these steps, our current view is that Google should:

(a) Surface the Topics dialogue box periodically and consider approaches, based on user research, to remind or prompt users to revisit other Privacy Sandbox settings.

Protected Audience API

Overview

31. The Protected Audience (**PA**) API (formerly known as FLEDGE) is primarily intended to support remarketing and other custom audience use cases.[24]

[24] For more information on PA API and how it works see Google Developer Blog on ‘Protected Audience API’ here (accessed on 22 April 2024).

Remarketing is the practice of serving targeted ads to individuals based on their activity on an advertiser's website. PA allows sites to assign users to interest groups. The browser stores information about interest groups including the name of the interest group, the group's owner, and information about the interest group's configuration.

32. PA has several components, intended to work together to facilitate privacy preserving remarketing. Google has published a timeline showing the status of each component.[25] The timeline is high level, indicating the quarter in which Google expects the feature to be available.

Potential concerns

33. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

Potential concerns	**Provisional CMA views based on ICO's preliminary assessment**
At third-party cookie deprecation, PA will be deployed without a number of key technical privacy controls.	We understand that a range of planned Privacy Enhancing Technologies (PETs) will be required no sooner than 2026. These include: Trusted Execution Environments (TEEs)[26] for Key/Value servers; Fenced Frames; a replacement for event level reporting; and a solution to Navigation URL leaks. Based on the ICO's preliminary assessment, we are concerned that the absence of these features will allow API callers to join user activity across the sites they visit. We understand it is Google's current position that industry adoption of the API is a priority: PA is already a significant change to third-party cookie-based remarketing and, if planned PETs are too rapidly introduced, it could have a significant impact on the ecosystem and adoption of the API. While all key dates and delivery are hard to forecast, Google has said that it is working on delivering privacy mitigations for known cross-site tracking risks. Google has said that it plans to outline how the implementation of privacy-related controls will be accounted for in a wider, to-be-proposed governance process. Without sufficient controls, in the short term, the ICO has expressed concern that PA will not mitigate key privacy risks identified. Longer term, we await sight of Google's proposed governance process to determine if it provides sufficient assurance

[25] See Google Developer Blog on 'Status of pending Protected Audience API capabilities' here (accessed on 22 April 2024).

[26] Google describes Trusted Execution Environments (TEEs) as 'a special configuration of computer hardware and software that allows external parties to verify the exact versions of software running on the computer. TEEs allow external parties to verify that the software does exactly what the software manufacturer claims it does—nothing more or less.' See Google Developer Blog on Aggregation Service here (accessed on 22 April 2024).

Potential concerns	Provisional CMA views based on ICO's preliminary assessment
	that planned controls will be delivered as currently outlined in the product roadmap.
The delegation of Interest Group (IG) creation to third parties will not be transparent to the user.	After consulting with the ICO, we are concerned that site owners may not clearly disclose who is processing the user data and the purpose for which it is used, including obtaining valid consent from visitors. Moreover, we believe that the current UX does not adequately inform users that a range of parties beyond the first-party site may be processing their data, potentially in combination with third-party data collected outside the site they are currently visiting. Google is considering updates to the UX to address these concerns, including undertaking further user research.
Permissionless delegation of IGs will impact transparency, fairness and lawfulness.	We understand that site owner permissions for creating IGs (joinAdInterestGroup) are currently set to 'allow all' by default. Based on the ICO's preliminary assessment, we are concerned that with these permissions site owners will not have full control or visibility of the parties processing users' personal data. As a result, the ICO is concerned that third parties creating IGs will undertake data processing without sufficient transparency being provided to the user and without an appropriate lawful basis. We understand that Google has defaulted site permissions to 'allow all' to facilitate successful testing and adoption of the PA API. In Google's view, the requirement for site owners to make changes to their sites would create an unwanted barrier to adoption while transitioning from third-party cookie-based remarketing. Google has said it has undertaken market research that shows site owners are concerned about leaking their audiences via third parties operating without explicit permissions, and that site owners would require 12 months' notice to prepare for a change in default permissions. We understand that Google will enact this change based on advertising industry feedback no earlier than 2025; however, no set timeline is given. We view this as a risk that will persist until at least the second half of 2025.
Third-party/cross-site data will be combined with first-party data in the PA IG.	We understand that k-anonymity controls (previously in place to prevent microtargeting in early iterations of the proposal formerly known as FLEDGE) no longer apply to IGs. As a result, it is possible to create IGs bespoke to individuals rather than some minimum number or people. Further, it is also possible to store deterministic identifiers as part of the IG and use them in the ad selection process. This may lead to a situation where cross-site data and profiles from third-party sources can be leveraged in PA. The ICO is concerned that combining first- and third-party data in the PA API will not address a range of data privacy concerns potentially leading to non-compliance with Applicable Data Protection Legislation. The ICO, for example, is concerned that: • sufficient information will not be presented to users to ensure transparent and fair processing; and

Potential concerns	Provisional CMA views based on ICO's preliminary assessment
	• excessive profiling will occur that exceeds the API's remarketing use case. We share this concern. Google has acknowledged that it is possible to leverage third-party data in PA's ad selection process. In the context of Google's stated API goal of preventing cross-site reidentification, Google's view is that, when all planned PETs are implemented post-2026, no *additional* cross-site information is leaked. Put another way, for a third party with access to audience profiles, a future iteration of PA will not leak cross-site data to enable additional enrichment/augmentation of profiles. Google has also agreed to update its developer guidance to stress the importance of transparency requirements when using the API. Further, Google is exploring whether it is possible for API callers to flag when an IG utilises cross-site data and how this information could be surfaced to users. We await Google's updated developer guidance and further information on possible changes to PA UX to understand if this concern is resolved.
That utility-focussed updates to the API are undertaken without sufficient consideration for privacy impacts.	Across the development and testing of the PA API we have observed a range of changes made to the original API design. The majority of significant updates to the proposal have been focussed on improving utility (for example, removing k-anonymity controls for IGs). Based on these observations, we are concerned that privacy is not appropriately considered by Google. As a result, over time, there is a risk that the PA API will be evolving in a direction potentially leading to non-compliance with Applicable Data Protection Legislation. In response, Google has said that the API must offer sufficient utility to ensure adoption. However, Google has acknowledged that there is a risk that too much compromise in this area would undermine a core aim of the project. To address this concern, Google is developing governance arrangements to ensure privacy is correctly balanced against utility and the immediate priority of adoption. We await Google's updated approach to governance.

34. Based on stakeholder feedback and our own analysis of the API, we have considered the following potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns identified based on further submissions from Google and other market participants since our last report was published in January 2024. New concerns raised by stakeholders during the reporting period are included at the end of the table.

- *PA Concerns*

Potential concerns	CMA views in January 2024 report	Updated CMA views
IG design currently excludes traffic shaping, the practice of filtering or curating bid requests to prioritise DSP responses based on some information about the bid opportunity.	Google has responded to the traffic shaping concerns by recommending that SSPs can use caching or DSPs can make increased use of Trusted Key/Value servers to address these use cases.[27] We recognise that traffic shaping contributes to efficient use of ad tech resources. Some ad techs are constrained by limits on the number of queries per second they can process, and traffic shaping can help them to prioritise bids. We are keen to hear further stakeholder feedback on whether Google's recommendation addresses this use case.	We remain concerned that a lack of effective traffic shaping could distort competition between DSPs with a larger capacity to respond to bid requests, which may therefore be less reliant on traffic shaping, and those which rely heavily on traffic shaping. Given that Google's DSPs have a large capacity to respond to bid requests, we are therefore concerned that the lack of traffic shaping could favour Google's DSPs. Since the publication of our last report, stakeholders have also raised concerns that caching is complex to implement, creates a dependency on SSPs and hides the 'true' shape of traffic from DSPs. We have shared this feedback with Google and await its response.
PA does not currently support effective IG delegation, (i.e. where one party assigns a user to an IG and allows another party to bid on that IG in a PA auction).	Google believes that its implementation accommodates all use cases and states that it should 'build additional support to make some use cases flow more smoothly in the future'.[28] We have raised the issue with Google and are seeking clarification on the timeline.	Google has repeated its view that PA currently supports contract-based approaches to IG delegation. We have not received any updates on the timeline for the 'additional support' referenced in Google's Q3 2023 feedback report. As stated in the D&I A section above, IG delegation should be transparent to the user.
PA auctions only allow buyers to bid on one IG. Buyers cannot combine IGs, for example to bid when a user is a member of both IG A and B.	Google has stated that PA does not support this type of ad targeting, and that combining IGs is incompatible with PA's current privacy model.[29] We currently agree with the approach to restricting remarketing and other custom audience use cases to one IG	We are aware of stakeholder comments that it would be possible for DSPs and ad servers to develop joint buying/selling logic. We are exploring whether this could allow ad servers and DSPs with a strong relationship (e.g. those owned by Google) to work around the restrictions in PA.[30]

[27] See 'Traffic shaping' in Google's Q2 2023 feedback report (accessed on 22 April 2024).

[28] See 'Publisher Interest Group Control' in Google's Q3 2023 feedback report (accessed on 22 April 2024).

[29] See issue #818 on the FLEDGE repository on GitHub here (accessed on 22 April 2024).

[30] See Issue #1028 on the FLEDGE repository on GitHub here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
	and will discuss our assessment of privacy issues (D&I A) in relation to the PA privacy model further in a future quarterly report.	
PA auctions allow one ad auction per placement slot and each slot is treated independently. This creates challenges of competitive ad separation, i.e. ensuring that ads for competing brands do not appear in ad slots on the same page.	Competitor ad separation is an important industry use case. Stakeholders have suggested adding 'whole page'[31] or 'multi-tag'[32] auctions to PA. Google has identified increased complexity and privacy risks associated with this feature. Our understanding is that Google is considering the feature request, and we will continue to monitor the issue. We are keen to hear further stakeholder feedback, and suggestions for other design changes that could help to address the issue.	Google has argued that competitor ad separation is not entirely possible in today's digital advertising ecosystem. Google has said that, presently, direct sold ad serving by the publisher is the only reliable method for ensuring competitor ad separation.[33] We recognise that competitor ad separation could have contractual and revenue implications for the ad tech ecosystem. We are also aware that other browser vendors have proposed implementations that allow for coordinated ad placement via multi-tag support in the scoreAds function.[34] We await more detail on Google's response to the feature requests, and its proposed solutions or mitigations to the privacy and security challenges that Google has previously identified.
PA auctions offer limited support for negative targeting, i.e. excluding some users from seeing a particular ad.	Discussions on negative targeting capabilities in PA are ongoing. Google has introduced functionality in response to stakeholder requests. However, some stakeholders continue to express concern that this does not fully address their cases. The ecosystem continues to propose improvements and Google has indicated that it	Google has addressed the majority of stakeholder concerns on this issue. We are following the ongoing discussions related to the potential facilitation of excluding an entire IG, as opposed to filtering ads within that group[36] and other alternative methods.[37]

[31] See issue #98 on the FLEDGE repository in GitHub here (accessed on 22 April 2024).

[32] See issue #846 on the FLEDGE repository on GitHub here (accessed on 22 April 2024).

[33] See 'Competitive Separation' in Google's response to the IAB Tech Lab's report here (accessed on 22 April 2024).

[34] See 'API difference highlights' in the privacy-preserving-ads repository on GitHub here (accessed 22 April 2024).

[36] See issue #896 in the FLEDGE repository on GitHub here (accessed on 22 April 2024).

[37] See Issue #1096 on the FLEDGE repository on GitHub here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
	will take some proposals on board.[35] We will continue to monitor the issue, noting that we do not expect the Privacy Sandbox tools to replicate all the functionality currently available to ad techs using third-party cookies.	
GAM will not participate in PA component auctions unless it is the top-level PA seller. This means that publishers have to use GAM in order to access AdX demand.	Our understanding of the current approach is that GAM will only participate in PA component auctions where GAM also run the top-level PA auction. We have identified this as a priority area for Google to address. We are also exploring whether parties other than the publisher ad server should be able to run the top-level PA auction. Our current understanding is that some ad server functionality (e.g. pacing) may not be available unless the ad server runs the top-level PA auction.	Google has confirmed our understanding that GAM will only participate in PA component auctions where GAM also runs the top-level PA auction. Google's position is that running both the component and PA auctions enables the ad server to provide functionality (e.g. pacing, forecasting) for publishers. Our understanding is that publishers wanting to access demand from Google's SSP in PA auctions would therefore have to choose GAM as the top-level PA seller. We are concerned that this could extend GAM's market power in the publisher ad server market to limit competition among parties wishing to run PA auctions as top-level seller. We are aware that some stakeholders have expressed a desire for GAM to share information about the winning contextual bid with a third party, allowing that third party to run the top-level PA auction.[38] We are continuing to discuss these concerns with Google. This is a high priority area for us to resolve.
PA reduces the information available to publishers compared with the status quo. Publishers will only receive information on the top-level winning bid, with no visibility over	PA is currently not designed to provide publishers full control over auction dynamics and data related to their advertising inventory. This design raises concerns that GAM, or any other top-level seller will receive more data and understanding of the	Google is considering options to provide view and click information to buyers, in response to stakeholder feedback. Our understanding is that ad techs could use this information to optimise their approach to PA auctions. We encourage the

[35] For example, see issue #896 in the FLEDGE repository on GitHub here (accessed on 22 April 2024).
[38] See Issue #10690 here and #9481 here on the Prebid repository on GitHub (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
component auction winners.	relative value of impressions than either publishers or component sellers. We are exploring this further with Google and other market participants. Several stakeholders have proposed that the publisher's top seller should be able to share all the data (beyond price) with any component sellers the publisher may select.	ecosystem to provide feedback on Google's proposed design.[39] As regards the concerns about GAM's access to information which would benefit Google's services over other market participants, we are considering what further assurances Google can provide to resolve this concern.
Information on PA component auction winners will be visible to GAM, raising concerns about unequal access to information.	Our current understanding is that each PA component auction returns the outcome of the scoreAd function to the top-level auction. Google has informed us that information on individual component auctions never leaves the auction worklets. We are currently discussing with Google whether GAM has access to information that is not shared with the publisher.	Google has told us that, based on its commitments to the French Competition Authority on the online advertising case,[40] GAM in its role as ad server is prohibited from sharing bid data with any entity participating in an auction, including GAM's ad exchange. Furthermore, Google has explained that GAM's ad exchange functionality is prohibited from using third-party SSP prices in order to optimise bids in a way that third-party SSPs cannot reproduce. However, Google has said that GAM as an ad server can use these bids for its 'ad server functionality' (e.g. for computation of the Minimum Bid to Win). We are considering what further assurances Google can provide to resolve this concern.
GAM proposes to use machine learning to decide whether to trigger a PA auction. This raises concerns about a lack of transparency for publishers about how the system decides whether to trigger a PA auction and a lack of publisher control.	GAM has told us that its proposed model will optimise for total publisher revenue from all sources including direct deals, AdX programmatic auctions and revenue from other SSPs. GAM has clarified that publishers will have the option to turn off the machine learning feature when there are other sellers who want to participate in the PA auction.	We are continuing to discuss this point with Google.

[39] See Issue #957 on the Fledge repository on GitHub here (accessed 22 April 2024).

[40] See Decision 21-D-11 regarding practices implemented in the online advertising sector dated 7 June 2021 (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
	Our understanding is that the option is for publishers to either opt-in or out of the machine learning trigger. We are keen to hear feedback on whether this binary control addresses publisher concerns. Stakeholders have expressed concern that machine learning throttling could remove discretion from the ad tech ecosystem. Some publishers want to have the option to trigger a PA auction, and access to the information necessary to decide whether to trigger that auction. We are focusing on GAM's approach to PA as one of our top priorities and in-depth discussions are ongoing. We expect to be able to provide further updates in our next quarterly report.	
URLs for loading scripts into PA auctions must have the same origin as the IG owner.	Ad tech vendors commonly host applications on separate subdomains, moving these to the same origin could incur infrastructure costs and complicate reporting use cases. Google has indicated that design changes are possible, subject to resolving concerns around the web security model.[41] We will continue to monitor this issue and welcome further stakeholder feedback on prioritisation, i.e. is this a critical issue for the ecosystem.	Google has indicated that design changes are possible, subject to resolving concerns around the web security model. We will continue to monitor this issue.

[41] See issue #818 on the FLEDGE repository on GitHub here (accessed on 22 April 2024).

- *PA Services Concerns*

Potential concerns	CMA views in January 2024 report	Updated CMA views
Latency for on-device auctions. Testing suggests that PA auctions may be slower, either due to device constraints (e.g. processing power available), auction design (e.g. waiting for information on the winning contextual bid before completing the PA auction) or network requests (e.g. fetching bidding or scoring logic).	Google proposes to address these concerns via design changes in Chrome and by publishing guidance for ad techs on optimising their approach to PA. The design changes add controls for sellers, allowing sellers to set limits on the time and resources buyers can consume.[42] The guidance includes recommended best practice for buyers and seller.[43] We are monitoring latency issues closely, recognising that high latency can lead to unsold ad inventory and negatively impact user experience. We expect that the Chrome-facilitated testing period will provide further data and we welcome ongoing stakeholder feedback, particularly on whether the tools and recommendations Google has implemented are sufficient.	Our views remain unchanged. We anticipate that stakeholders will be able to provide more specific feedback on latency at the end of the Chrome-facilitated testing period.
Moving processing to the device can raise concerns about overall page or device performance, with implications for search engine optimisation and user experience.	Our understanding is that Chrome uses separate worklets for the PA auction and page rendering. This allows page rendering to complete before the PA auction and should minimise impact on page load times. We anticipate that the Chrome-facilitated experiments period will provide further data on device performance issues. We welcome specific feedback from market participants on this issue.	Our views remain unchanged. We anticipate that stakeholders will be able to provide more specific feedback on latency at the end of the Chrome-facilitated testing period.

[42] See 'Performance of Protected Audience Auctions' in Google's Q3 2023 feedback report (accessed on 22 April 2024).

[43] See Google Developer Blog on 'Improve Protected Audience API auction latency' here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
Fenced Frames restricts available ad formats. They do not currently support native, or video ads and stakeholders have requested native support for dynamic ad sizing.	We recognise significant stakeholder concerns around video and native ads once Fenced Frames are required. Google currently intends to require Fenced Frames no earlier than 2026. Google says that it has not yet designed a solution to render video in Fenced Frames. Stakeholders have raised support for the VAST standard as a specific concern. While Google is not obligated to support all existing standards, we are aware of the potential disruptions that a lack of VAST support could cause. Discussion on native ads and sizing is ongoing.[44] We are monitoring the issue and recognise the potential impact on publishers, advertisers, and users. Restricting ad formats could hinder the feasibility of dynamic content within existing native ad formats, limiting the potential for rivals and new entrants to introduce innovative advertising formats beyond walled gardens and potentially diminishing the overall user experience.	Google has now confirmed its commitment to ensuring support for major ad formats before enforcing a requirement for Fenced Frame rendering. Stakeholders have also raised concern that PA API with iframes might also lack support for video and native ad formats. This would be of greater concern given its immediate impact at third-party cookie deprecation, Google has in response published a demo showing one option for handing VAST in PA using iframes[45]. We would welcome further industry feedback on the extent to which this resolves this concern. We note that discussions with Google concerning the future governance arrangements for Privacy Sandbox are ongoing. Google's work to develop and implement Fenced Frames are expected to be incorporated under that governance model.
Uncertainty about the impact of restrictions on transmitting signals from video players in Fenced Frames.	Our understanding is that video ads currently send real time signals to external systems, including for reporting purposes. The restrictions imposed under Fenced Frames will block these signals. We will continue to monitor this issue as Google implements a solution for video requirements ahead of the required use of Fenced Frames no earlier than 2026.	See above

[44] See issue #741 here and issue #311 here on the FLEDGE repository on GitHub (accessed on 22 April 2024). On how the one ad-size gets decided, see issue #908 here; On the possibility of enabling multi-sized PA auction output, see issue #825 here; and on implementing an additional Ad-Slot Size signal, see issue #869 here (accessed on 22 April 2024).

[45] See 'Instream video ad in a Protected Audience sequential auction setup' demo here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
	We welcome further feedback from market participants on this use case, including on whether other Privacy Sandbox tools (e.g. Shared Storage) offer options to deliver the necessary signals.	
Google intends to deprecate event level reporting for PA auctions, no earlier than 2026. Once event-level reporting has been deprecated, the Private Aggregation API will become the only reporting mechanism available.	Google aims to prevent the use of event-level reporting for discovering the IG of individual visitors to the publisher's site, aligning with the privacy objectives of Fenced Frames. As the Private Aggregation API will become the only reporting mechanism within the PA API, the IG will be passed solely through "generateBid" and to "reportWin" functions. Our understanding is that this could reduce the information available to ad techs and could have an impact on their ability to optimise their bidding strategy. We are keen to hear further detail on the specific impacts and proposals for design changes.	Google has said that it anticipates collaborating with the ecosystem to enable the necessary event-level reporting without compromising user privacy. Recognising concerns about the impact on ad techs' bidding strategy optimisation, Google foresees the availability of a private machine learning training model based on TEEs well ahead of the removal of the current event-level reporting. We are continuing to monitor developments.
PA auction design shifts data flows that were previously server to server onto the device. This raises concerns about transparency, and contractual issues (e.g. as ad techs have no contractual relationship with Google).	We recognise that Privacy Sandbox changes, including restrictions on access to information that is currently available, can impact ad tech business practices. We are working to identify these issues, including possible solutions.	Google's reply to the IAB Tech Lab's Fit Gap Analysis refers to the concern that ad techs using the Privacy Sandbox tools will not have a contractual relationship with Google,[46] as these tools are inherent to the browser and developers independently determine their usage.
Concerns about the requirement to adopt TEEs to operate PA's server-side elements, such as the Bidding and Auctions Services and the Key/Value Server.	We discuss concerns relating to TEEs below. Google has indicated that some off-device services will be an optional extra for market participants who want to develop larger, more	Since the last publication, we are aware of increased concerns regarding uncertain TEE requirements and the unavailability of Bidding and Auction services beyond the origin trial.

[46] See the 'Data Guarantees' heading in Google's response to the IAB Tech Lab's report here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
	sophisticated models, allowing stakeholders to choose components aligning with their objectives. We are working with Google to explore the flexibility of server-to-server architecture and its impact on market participants.	Google continues to emphasise on-device functionality will suffice for ad techs to conduct PA auctions, and that off-device Bidding and Auction services will be optional. This is supported by ongoing improvements in latency,[47] with forthcoming updates providing greater clarity on Bidding and Auction services costs and the outline of the baseline system,[48] as well as strategies for scaling up traffic Bidding and Auction services beyond the origin trial.[49] We have also heard concerns that Google's characterisation of server-side elements as 'optional' is misleading as, in practice, most ad techs will need access to real time information from Key/Value servers. Google states that running Key/Value servers in TEEs will be required no sooner than Q3 2025 and that Google will provide at least 12 months' notice before the TEE requirement becomes mandatory. We await the results of the testing period and encourage additional stakeholder feedback.
PA lacks adequate authentication to verify contextual responses, K/V server-originated responses, or bid submissions.		Stakeholders have raised concerns that PA is insufficiently robust in terms of validating the authenticity of contextual responses, responses from a key-value server or bid submission. For example, stakeholders claim to have devised effective attacks against PA. These concerns have been raised with Google and we await its response.

35. Our concerns under **D&I D – User Experience** relate to the default enrolment into PA and the information notice for PA being shown once, immediately after

[47] See the 'Improve Protected Audience API auction latency' page here (accessed on 22 April 2024).
[48] See the 'Bidding and Auction Costs' presentation here (accessed on 22 April 2024).
[49] See 'roadmap' within the Fledge GitHub repository here (accessed on 22 April 2024).

the Topics API dialogue box. We are continuing to engage with Google on resolving these concerns and asking it to conduct further user research and testing, to ensure adequate user comprehension of the API including its distinction from the Topics API and the purpose of PA IGs, ease of accessing the relevant user controls and enabling users to revisit their PA preferences.

Summary

36. Google needs to resolve our concerns for PA API and our current view is that this should involve taking the following steps:

(a) Enhance Chrome UX to ensure disclosure of data processing activities conducted by site owners and all advertising partners when delegating permissions for IG creation to third-party partners or combining third-party data.

(b) Develop a robust governance and monitoring framework to ensure the timely delivery of scheduled privacy measures, particularly PETs, fraud detection protocols, and up to and including revocation of API access, to ensure that where abuses of the API are identified, Google responds appropriately.

(c) Address the issues relating to GAM’s approach to PA, including by ensuring that it does not distort competition in digital advertising between Google and other market participants, in a way that could reinforce its existing market position.

(d) In particular, resolve concerns related to use of a third-party (i.e. other than GAM) ad server to run the top-level PA auction with GAM participating as a buyer in the PA component auction. Additionally, reflect the need for publishers to have the same reporting visibility over component auctions as GAM.

(e) Resolve ad format concerns, specifically the use of video and native ads in Fenced Frames. Our understanding is that these formats are particularly important to ad revenue and that they are currently unsupported with Fenced Frames.

(f) Continue dealing with stakeholders' suggestions and providing support in developing solutions, where possible, regarding IGs, on-device latency, and server-to-server architecture.

Measuring digital ads

Attribution Reporting API

Overview

37. The Attribution Reporting API (**ARA**) aims to allow ad techs to measure conversions without third-party cookies. A conversion occurs when the user takes an action (e.g. creating an account or making a purchase) after clicking on or viewing an ad.[50] Measuring conversions is necessary for several of ad tech's key functions, including budgeting, campaign reporting, optimising bidding strategies, and pricing ad inventory.

38. ARA supports two forms of reporting:

    (a) Event-level reporting. Event-level reports provide information about a specific ad event (like click or view). The browser stores information about ad events and conversions on-device and sends a report to the ad tech if a conversion attribution occurs. Chrome adds delay and noise to the reports. The length of the delay is dependent on the ad tech's configuration, with a minimum 1-hour report window limit. Delay and noise are intended to protect user privacy by preventing ad techs from using event-level reports to track users across sites.[51]

    (b) Summary or aggregate reporting. Summary reports capture information about attributed conversions in a similar way as event level reports. The ad tech must first specify which ad event and/or conversion dimensions they would like to report on. When a conversion is attributed, Chrome encrypts the ad event and conversion information and sends it to the ad tech, with a random delay between 0 to 10 minutes or with no delay if the ad tech opts in to instant reports. For instant reports there are additional null reports introduced. The ad tech can batch these encrypted reports together and send to their aggregation service, a specialised server running in a TEE on the public cloud. The aggregation service aggregates the batched reports and adds privacy protections like noise. The ad tech can then retrieve summary reports from the aggregation service.[52]

[50] See Google Developer Blog on ARA here (accessed on 22 April 2024).
[51] ARA currently supports up to eight conversion categories for event-level reporting. See Google Developer Blog on event-level reports here (accessed on 22 April 2024).
[52] An overview of Aggregation Service for the Attribution Reporting API can be found on GitHub here (accessed on 22 April 2024).

39. Chrome recommends ad techs to use summary and event level reports together, as they provide complementary information. Google Ads has published a technical explainer on how it is using ARA to measure conversions.[53]

Potential concerns

40. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

Potential concerns	**Provisional CMA views based on ICO's preliminary assessment**
Key controls, such as epsilon values and API rate limits, have not been tested.	We understand that key controls (e.g. rate limits, epsilon values, reporting delays etc applied to both event and summary reports) are set initially as placeholders/'strawmen' during testing. For example, for summary reports, parties running aggregation services can use an epsilon value up to 64 while ARA is adopted through third-party cookie deprecation – with an expectation that an appropriate range will be identified in due course. The ICO is concerned that key controls and parameters for the ARA have not been effectively tested to establish the optimum balance between utility and privacy. There is also a concern that Google will not be able to gather useful feedback from ARA customers as API callers are likely to have a vested interest in preserving maximum utility. Effective testing is for Google to define, but Google must justify why 64 is appropriate or test to find the appropriate number. Google has said that key privacy parameters are still under review as parties continue to test and experiment with ARA. Google is exploring how governance for internal decision making will improve transparency and strengthen guardrails. To support ecosystem testing efforts, Google has provided a number of tools for testing, such as Simulation Library[54] and Noise Lab[55] and will also give ad techs enough time to test before any changes are made. We await Google's response on its governance process.
Any measurement product that permits events to be connected to an individual will always present a cross-site tracking risk.	We understand that, for event level reports, a key product requirement is an advertiser's ability to learn that a particular ad displayed to an individual resulted in a conversion, and for these signals to inform/train machine learning models. Accordingly, Google has provided sufficient space in the maximum value for the source_event_id (64 bits) to allow an ad shown to an individual on a publisher site to be mapped to any relevant granular information available to publishers or partners. This ID can then be associated with limited conversion data.

[53] See Google Ads Developer Blog on 'Optimally configure the Attribution Reporting API for ad measurement' here (accessed on 22 April 2024).
[54] See Simulation Library repository on GitHub here (accessed on 24 April 2024).
[55] To access the Noise Lab, see here (accessed on 24 April 2024).

Potential concerns	Provisional CMA views based on ICO’s preliminary assessment
	Google has acknowledged that, by necessity (i.e. model training), the design of event level reports links limited conversion data back to a specific individual and event on a publisher site. While Google has applied a range of controls to make reidentification harder (e.g. limiting the information joined to between 1 and 3 bits (conversion data) and applying event-level (i.e. not user level) differential privacy), Google has also acknowledged that the granularity of data required for model training ultimately limits the application of certain controls (e.g. at a certain point, a lower epsilon would undercut the bidding model use case). As a result, Google has acknowledged that misuse of the API can result in reidentification. We understand it is Google’s view that this risk is acceptable as the ARA significantly reduces both the permissiveness and quantity of cross-site tracking currently enabled via third-party cookie-delivered measurement products while delivering a vital ad use case. Additionally, Google expects that the API will be mainly used by well-intentioned advertisers (agreed to via the Privacy Sandbox attestation process), further reducing the risk. Based on the ICO’s preliminary assessment, we view it as probable that a proportion of API callers will use cross-site information derived from event level reports for purposes beyond ad measurement and reporting. For organisations deviating from Google’s intended use case, after consulting with the ICO, we view it as likely that alignment to transparency and lawfulness principles in the Applicable Data Protection Legislation will be particularly impacted. In response, Google has expressed its dedication to the long-term goal of reducing the likelihood of successful abuses of the API. However, its immediate goal is to help the ecosystem transition away from third-party cookie-enabled products that enable far more pervasive tracking. We understand that Google does not intend to transition to aggregate-only reporting. Accordingly, we have asked Google to explain what governance and monitoring can be implemented to ensure that, where identified, Google responds appropriately to abuse of the API.
Navigation tracking will undermine key ARA limits placed on click events.	We understand that, across the Privacy Sandbox tools, no controls are in place to explicitly prevent organisations using link decoration/navigation tracking to undermine limits applied to ARA. As a result, for click events, it is possible for an ad tech to join a user’s identity cross-site via a navigation event. This undermines the 3-bit limit applied to navigation event trigger data. In response, Google has pointed to a range of anti-covert tracking (ACT) efforts that strive to make covert tracking more challenging. We await further details to understand how these controls resolve this concern.
Documentation, guidance and wider public-facing information relating to ARA do not make clear the	The ICO noted a concern with Google that a range of public-facing Google-produced documentation may have created ambiguity regarding the application of PECR. As regards ARA (and also applicable to wider Privacy Sandbox tools), the ICO’s position,

Potential concerns	Provisional CMA views based on ICO's preliminary assessment
requirement to consider the collection of consent required by PECR.	which we share, is that the storage and access of information for non-essential purposes requires consent. In response to this concern, Google is updating the EU Consent Policy FAQ and the Privacy Sandbox Privacy-related Compliance FAQ. We await to receive these updates.

41. Based on stakeholder feedback and our own analysis of the API, we have considered the following potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns identified based on further submissions from Google and other market participants since our last report was published in January 2024. New concerns raised by stakeholders during the reporting period are included at the end of the table.

Potential concerns	CMA views in January 2024 report	Updated CMA views
ARA does not support some types of attribution that are currently available with third-party cookies, for example multi-touch attribution.	It is clear that Google's ARA will not provide the same functionality as third-party cookies, given the desire to limit the amount of personal information shared. We consider that the changes Google has made to ARA following stakeholder feedback should increase its utility overall, including the move from fixed to flexible event reporting windows.	Stakeholders have expressed further concerns around Google's approach to multi-touch attribution, arguing that 'single touch' attribution is likely to advantage Google. For example, a current user journey may involve seeing an ad several times on different properties (e.g. a publisher site, their social media feed, etc) before the user takes an action. Users may also act on their intent to convert by searching for the advertised product. Stakeholders are concerned that Google is likely to be the 'last touch' and therefore capture more of the value from conversions than other market participants. We have shared this feedback with Google and await its response.
Coarser measurement may make it harder for publishers to value their ad inventory.	See above	Stakeholders continue to express concerns that reduced access to real-time, cross-site data could make it more challenging to value ad inventory. Although we anticipate that the results from the period of Chrome-facilitated testing will give us greater insight into the magnitude and direction of any impact on publishers and advertisers, given the desire to limit the amount of personal information shared, it is unrealistic to

Potential concerns	CMA views in January 2024 report	Updated CMA views
		expect Google's ARA to provide the same functionality as third-party cookies.
The proposed '20 event per aggregatable report' limit appears arbitrary and undermines ARA's utility.	Many of the Privacy Sandbox APIs require Google to define parameters. Our current view is that a '20 event' per aggregatable report limit is reasonable, given that attempting to measure small numbers of events via aggregate reports is unlikely to be useful. Google has published detailed guidance on tuning ARA, information on working with noise and details of how Google Ads uses ARA.[56] Our current view is that this information should allow market participants to use ARA effectively.	Stakeholders continue to express concerns about the values of parameters that Google has defined. Our January 2024 report recognised that the Privacy Sandbox design requires Google to define some parameters and our view remains that the report limit is likely to allow market participants to use ARA effectively.
Advertisers are currently able to adjust their spending on ad campaigns in real time. ARA imposes reporting delays and could lead to wasted spend that could otherwise have been reallocated.	We understand that ad techs can tune ARA to prioritise different types of reporting, including the move from fixed to flexible event reporting windows. We are keen to understand whether ARA can provide reporting that minimises delay for ad spend optimisation use cases. We welcome further feedback from market participants based on their experiments during the Chrome-facilitated testing period.	The move to flexible event reporting windows has been reflected in the technical specification[57] and also in an explainer update.[58] Our discussions with Google on this point are ongoing. Further, we have received feedback that there are missing fields in the flexible reporting events, namely currency and orderID. We have shared this feedback with Google and await its response.
ARA degrades open display measurement compared with measurement capabilities on O&O ad inventory.	More sophisticated attribution may be possible on O&O inventory, for example where the ad tech has access to first party data. The Commitments impose restrictions on Google's use for first-party data (specifically Chrome browsing history and Google Analytics) for measurement on Google O&O inventory. We are considering whether further restrictions on Google's use of first-party data are necessary.	Stakeholders continue to express concerns that measurement using ARA will be less effective than measurement on O&O inventory. We have previously stated that we are conscious of the risk that ad spend could move away from open display and into O&O inventory depending on the overall impact of the Privacy Sandbox changes.[59] Our discussions with Google on further first-party data restrictions are ongoing.

[56] See Google Ads Developer Blog on optimally configuring ARA here and the Google Developer Blog on the ARA and Noise Lab here (accessed on 22 April 2024).
[57] See the technical specification on the Attribution Reporting API repository GitHub here (accessed on 24 April 2024).
[58] See the Flexible Event-Level Configurations explainer on the Attribution Reporting API repository on GitHub here (accessed on 24 April 2024).
[59] See paragraph 27 of the CMA's Q4 2023 update report (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
Market participants will be dependent on Google's APIs for ad measurement in future, which raises concerns about the ability to audit and verify results.	Ad verification currently relies on auditing of log-level reporting data, which will not be available under ARA. Google needs to explain how it sees ad verification use cases being addressed under the Privacy Sandbox.	Our discussions with Google on ad verification use cases are ongoing. We have clarified that we are keen to understand the differences between common approaches to ad verification using third-party cookies and the approaches available using ARA. We have previously stated that we do not expect the Privacy Sandbox to provide identical functionality of third-party cookies. We have also raised stakeholder concerns that Google is not bound by contract to ensure verifiable server-to-server communication. There does not seem to be a comparable feature within the Privacy Sandbox tools more broadly to verify that Google is the other party to the data exchange. In addition, the party relying on the Privacy Sandbox tools does not know how the data provided will be processed and has no way of verifying that the expected processing occurred. This can have consequences for commercial viability and commercial contracts. We await Google's response this point.
Google's proposed approach to attribution differs from the approach taken by other browsers, which means that there may be limited interoperability of ARA with other solutions.	We remain concerned that lack of interoperability could harm competition by creating additional cost and complexity for businesses seeking to measure digital ads. Google needs to explain how it will continue its efforts to enhance greater interoperability of approaches to attribution and reporting over time.	We are aware that Microsoft has proposed implementing 'ARA with modifications for better parity with CPA billing' in Edge.[60] We remain keen to understand implications for interoperability and efforts to improve interoperability of approaches to attribution and reporting. We await Google's response on this point.
Google limiting the number of different attributions per	We are concerned about Google limiting the number of different attributions per advertiser to eight conversion types, which may be	Google has introduced custom trigger data, allowing ad techs to configure trigger data values and/or

[60] See the 'API difference highlights' explainer on the Privacy Preserving Ads repository on GitHub here (accessed on 24 April 2024)43.

Potential concerns	CMA views in January 2024 report	Updated CMA views
advertiser to eight conversion types, potentially harming advertisers who have more than eight types.	harming advertisers who have more than eight types. Currently, ARA limits 'trigger data' to 3 bits and this only allows eight distinct conversion types. Phase 2: Full Flexible Event-Level[61] would appear to indicate future support for up to 32 values; however there is currently no timeframe or deadline for this. The solution suggested within ARA for attributing to multiple domains is currently restricted to three domains[62] (which may be insufficient) and requires the advertiser to register these domains in the 'click' event (which would add overhead).	cardinality.[63] The trigger data supports 32 bits. ARA adds noise depending on the number of distinct trigger values, e.g. limiting the number of distinct trigger values with reduce noise and vice versa.[64] We understand that discussions within Google on ARA supporting multiple reporting domains for conversions is ongoing.[65] In the absence of further stakeholder feedback, it is likely that the change to configurable trigger data will resolve the concern about limiting tigger data to 3 bits.
The lack of and need for a transaction ID where the data passes from the buy side to the sell side, enabling the two to connect.	We are aware of stakeholder requests for Google to provide a transaction ID to support attribution reporting.[66] Our current view is to agree with Google that this could undermine the intended privacy model for ARA.	Our view remains unchanged.
The need to seek explicit feedback from advertisers concerning modification to their commercial contracts given the changes to aggregation and attribution.	Stakeholders have expressed concerns that Google needs to seek explicit feedback from advertisers concerning modification to their commercial contracts given the changes to aggregation and attribution, specifically whether advertisers are willing to be billed on the basis of noisy or aggregate reporting. We continue to welcome feedback from market participants, particularly from advertisers on this point.	We understand that a small portion of the ecosystem relies on attribution data for billing, whether that is Cost Per Action (CPA) or Cost Per Mille (CPM) and has raised concerns regarding the impact of noise and delay on billing. Google is responding to these concerns on GitHub and welcomes additional feedback from interested stakeholders.[67]

[61] An overview of Phase 2: Full Flexible Event-Level reporting can be found on GitHub here (accessed on 22 April 2024).

[62] See issue #1048 on the Attribution Reporting API repository on GitHub here (accessed on 22 April 2024).

[63] See the Flexible Event-Level Configurations explainer in the Attribution Reporting API repository on GitHub here (accessed on 24 April 2024).

[64] See 'Data Limits and Noise' in the Event explainer in the Attribution Reporting API repository on GitHub here (accessed on 22 April 2024)

[65] See the minutes of the regular ARA stakeholder meeting on 5 February 2024 here (accessed on 22 April 2024).

[66] See issue #15 on the Attribution Reporting API repository on GitHub here (accessed on 22 April 2024).

[67] See Issues on the Attribution Reporting API repository on GitHub here (accessed on 24 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
	We recognise that Privacy Sandbox represents a significant change for the ecosystem and reiterate that we do not expect Privacy Sandbox to deliver identical functionality to the technologies (like third-party cookies) that it intends to replace. We also recognise that Privacy Sandbox may have business impacts (e.g. changes to business practices).	
Stakeholders have expressed concern that the lack of a key discovery mechanism in ARA would make aggregated reports unsuitable for their use cases.	N/A	In June 2023, Google proposed adding key discovery functionality to ARA and said that it intended to publish a tool to help ad techs explore the impact of threshold selection on the precision/recall trade-off. We are not aware of the timelines for shipping this proposal. We have raised this concern with Google and await its response.
Stakeholders have expressed concern that adding noise to reports will have a disproportionate impact on smaller ad techs.	N/A	We understand this concern to focus on access to reliable signals for smaller vs larger market participants. Stakeholders have noted that the noise added to reports can be disproportionately limiting for smaller ad techs who are likely to reach the 20-event threshold more slowly and may not be able to rely on aggregate reports as much as larger ad techs. However, Google clarified that there is no enforced minimum number of conversion events per report. The limit of minimum 20 events per aggregatable report does not exist. We welcome further feedback from market participants, including on their experience of using the tools that Google has provided to help ad techs work with noise.
Stakeholders have expressed concern that the current ARA setup does not support manual campaign optimisation.	N/A	Stakeholders have expressed concerns that some ad techs want to manually optimise campaigns based on granular reporting. Google has discussed this scenario with ad techs and proposed approaches to using ARA to support manual campaign optimisation. Google's view is that ARA allows for ad tech customisation and flexibility to solve a range of ad tech use cases. For example, Google suggested using different flexible event-level configurations and, using

Potential concerns	CMA views in January 2024 report	Updated CMA views
		event-level reports with summary reports to reduce the impact of noise and to meet stakeholders' manual and automatic optimisation needs.

42. As regards the application of **D&I D – User experience**, similar to the position for PA API, our concerns stem from the default enrolment into ARA, the sequencing of the PA API and ARA information notice after the Topics dialogue box potentially leading to misperceptions about their association, and the accessibility of the ARA settings page. We are continuing to engage with Google on these, and other UX concerns.

Summary

43. Google needs to resolve our concerns for ARA, and it has agreed to take the following steps:

(a) Develop a robust governance and monitoring framework to ensure that ARA processes the minimum amount of data necessary to achieve its purpose and that where abuses of the API are identified, Google responds appropriately.

(b) Provide further details on proposed ACT measures that strive to make covert tracking more challenging.

(c) Update the general Privacy Sandbox developer compliance guidance on the requirement for API callers to obtain user consent.

44. In addition to these steps, our current view is that Google should:

(a) Secure greater interoperability and/or standardisation of approaches to attribution reporting. These currently appear fragmented with other available solutions including Mozilla/Meta's Interoperable Private Attribution and Safari's Private Click Attribution. The lack of interoperability could harm competition by creating additional cost and complexity for businesses seeking to measure digital ads.

(b) Explain how, in Google's view, ad verification use cases will be addressed under the Privacy Sandbox, including ARA.

(c) Seek explicit feedback from advertisers on the impact of changes, particularly concerning modification to their commercial contracts given the changes to aggregation and attribution.

Trusted Execution Environments

Overview

45. Google introduced Trusted Execution Environments (**TEEs**) to support use-cases where off-device processing is required while preserving the privacy of user data. Google has control of the Chrome environment where it can determine the security and privacy characteristics of the browser. However, there are no such built-in controls outside the browser, which necessitates TEE-based solutions for device to server interactions that extend the functionality of Privacy Sandbox APIs.

46. TEEs are secure server configurations that are primarily secured through appropriate hardware environments (served by the cloud providers – see below). In addition, in a Privacy Sandbox context, code images and scripts are developed and maintained by Google and further secured by an attestation mechanism that ensures the TEEs have not been modified by third parties.

47. Aggregation Service in a TEE is required for use of the ARA Aggregate API and the Private Aggregation API. However, debug reports allow for the use of Aggregation Services outside of a TEE, and ahead of third-party cookie deprecation most users have debug reports. There are also TEEs for different contexts, such as the Key/Value and Bidding and Auction Servers for PA. Google has updated the TEE explainer[68] to provide more detail on timeline and feature availability. Stakeholders continue to express concern about on-device performance, meaning that off-device components (e.g. the Bidding and Auction services for PA API) will not, in practice, be optional. We are monitoring this issue and welcome further feedback from market participants, in particular based on their experiences during the Chrome-facilitated experiments period.

Potential concerns

48. After consulting with the ICO, we are concerned that in the absence of TEEs and other features at the point of third-party cookie deprecation, API callers will be able to join user activity across the sites they visit (see **D&I A – Privacy outcomes** table in the PA API section above). We await to receive

[68] For more detail, see the TEE explainer here (accessed on 22 April 2024).[69] See Bidding and Auction Cost explainer here and Aggregation guidance here (accessed on 22 April 2024).

further details from Google on how its proposed governance framework will address this concern.

49. Based on stakeholder feedback and our own analysis of the API, we have considered the following potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns identified based on further submissions from Google and other market participants since our last report was published in January 2024. New concerns raised by stakeholders during the reporting period are included at the end of the table.

Potential concerns	**CMA views in January 2024 report**	**Updated CMA views**
Cost and complexity of adopting TEEs. We have heard concerns from ad tech stakeholders about the significant financial and staffing resources required to adopt and maintain TEEs.	Google has published certain explainers to address this concern.[69] We expect that it will publish further information (e.g. a cost explainer for K/V) to help ad techs estimate the costs associated with adopting TEEs. We recognise that some of these costs will vary, for example depending on specific deals with cloud providers that an ad tech can negotiate.	Google has confirmed that the K/V cost explainer will be published in H1 2024 to supplement previous B&A self-assessment guidance and that it will continue to proactively seek feedback from expected users of K/V regarding cost considerations. We encourage stakeholders to provide us with any further material feedback on cost concerns where they are able to, recognising that cost targets can be sensitive business information. We understand that there is a risk the cost and complexity of adopting TEEs could be greater to ad techs outside of Google's ecosystem, reliant on Google Cloud Platform (GCP) services. We are exploring the impact of this on ad techs and would welcome stakeholder feedback on non-negligible cost concerns.
Google currently only supports two public cloud providers, Amazon Web Services (AWS) and Google Cloud Platform (GCP).	Google has committed to support other public cloud providers, based on feedback from the ecosystem. Google has stated that it will use ad tech feedback on which cloud services should be supported as a key prioritisation criterion. Although we agree this is a sensible route forward, we recommend that Google provide timelines for ensuring that cloud providers, and any others	Google has now proposed criteria that additional compute environments offered by public Cloud Service Providers (CSPs) must satisfy in order to be eligible for processing user data generated by Privacy Sandbox APIs. We note that this means the environment must be secure, private, isolated, remotely attestable and the CSP must provide an attestation report. Google will validate that the CSP and the remote

[69] See Bidding and Auction Cost explainer here and Aggregation guidance here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
	as the market develops, are supported within appropriate timeframes. At the very least, Google needs to provide objective criteria for new cloud providers. Competition in the cloud infrastructure level is subject to a separate, ongoing market investigation by the CMA.[70]	attestations are trustworthy, by ensuring compliance with recognised industry standards on cloud security. In particular ISO 27001, ISO 27017 and ISO 27018, and certification from cloud security industry bodies, i.e. Level 2 in Cloud Security Alliance's STAR program. Google has now published finalised guidance and specification criteria for onboarding new cloud providers.[71] In addition, Google expects to publish a technical explainer on its approach for supporting new CSPs before third-party cookie deprecation, and to be ready to add potentially eligible cloud providers in 2025. We invite feedback from stakeholders on these measures, particularly on the prospect that some of the discussions on the review process are likely to be private to prevent disclosure of confidential information by CSPs and to avoid disclosing internal security practices. Furthermore, we understand that Google does not have plans to onboard alternative public cloud providers ahead of third-party cookie deprecation. We would like to invite feedback on the fact that the earliest approval for alternative public cloud providers is likely to be in 2025.
Google has limited support to public cloud, meaning that ad techs cannot run TEEs on their private cloud infrastructure.	Google has said that deploying TEEs on private cloud environments presents significant challenges. We note the strong ecosystem interest in private cloud (e.g. the issue was raised in Google's Q2 2023 and Q1 2023 feedback reports). We have raised the issue with Google and are seeking further clarity on the specific security challenges.	We understand that Google plans to continue exploring TEE technologies to be able to expand the choices available to ad techs, while meeting security requirements, and will take into consideration the types of solutions available as they make decisions about TEE requirements. Google is exploring options for supporting TEEs outside of public cloud but is unable to confirm whether and when support for TEE solutions outside of public clouds will be available in production. Google has proposed publishing further details on its technical

[70] See CMA, Cloud services market investigation.

[71] See GitHub explainer here (accessed on 24 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
		approach to private cloud TEEs, to gather further ecosystem feedback ahead of third-party cookie deprecation. We encourage stakeholders to provide feedback. Our concerns remain about the impact on publishers and advertisers, in particular the cost of TEE adoption plus the sunk costs of investment in private cloud infrastructure.
Self-preferencing risk associated with running TEEs on GCP.	We are aware of stakeholder proposals for an entirely open-source solution, including an open-source TEE, that is inspectable and transparent. We will need to consider this as part of a range of solutions to mitigate against the self-preferencing risk.	Discussions with Google are ongoing on this issue.
Performance degradation and scalability	N/A	We have received feedback from stakeholders stating that adopting public cloud for TEEs can have performance implications, for example having to use cloud components in the hot path of an auction is not as performant or reliable as tuned, on-premises hardware. We have also heard scalability concerns on TEEs being rolled out and scaled reliably to users, especially as the TEE system has never operated at the proposed scale. Stakeholders have asked for a six-month extension to the timetable given these concerns. Some stakeholders have also said that not having a Bidding and Auction service available at third-party cookie deprecation would lead to a significant degradation in performance given limited browser-side resources.[72] We have relayed these concerns to Google and await its response.
Timings	N/A	Stakeholders have said that Google's recently proposed solutions cannot be tested in the timeframes available due to the preparatory steps that market

[72] For more details, please see "Concerns about the requirement to adopt TEEs to operate PA's server-side elements, such as the Bidding and Auctions Services and the Key/Value Server" under the PA Services Concerns heading above.

Potential concerns	CMA views in January 2024 report	Updated CMA views
		participants would need to undertake prior to testing e.g. it could take up to 12 months to get regulatory approval with data protection/privacy regulators to use one of Google's suggested workarounds with data storage. We understand that given typical customer journeys extend across devices, it may have been critical for some market participants that testing of ARA occurred holistically once Android support for the ARA was made available. Android Privacy Sandbox ARA was available for testing on production devices starting in February 2023. App-to-web attribution across Chrome and Android was available for testing on production devices starting in May 2023. We await Google's response to these concerns.
Chrome restricting scope for innovation through its implementation of TEE services	N/A	Stakeholders have expressed concerns that Chrome is currently requiring the Google implementation of TEE services for on-device auctions. Stakeholders have said that rather than coupling to Google's own implementation, Chrome should specify the behaviours that a satisfactory implementation of a Trusted Signals Server, Aggregation Server, and any other required non-browser components, must meet. This would allow for innovation within acceptable privacy boundaries. Google has noted in its Q1 2024 progress report that to allow for others to run their own code in TEEs, Privacy Sandbox will need to review the code (and any changes) to confirm it does meet the privacy guarantees. Google welcomes feedback on what benefits this would provide which are not currently possible. Additionally, we have recently heard a new concern that Google's control over the design of TEEs might allow it to limit the ability of competitors to provide alternative functionalities and differentiate their services. For example, through control of the design of Bidding and Auction service TEEs, Google might be able to stifle

Potential concerns	CMA views in January 2024 report	Updated CMA views
		its competitors' innovations in machine learning models. Google has responded that it may limit functionality in order to maintain security and privacy, e.g. adding noise to data, or disallowing raw user data outside of a TEE. When the design limits functionality, the same limitations apply to Google Ads. We recognise that Google still has discretion on defining the margin of flexibility provided to ad techs to implement their functionality to differentiate their services. We welcome feedback on this point, in addition to any concerns on Bidding and Auction service governance.
Governance arrangements for coordinators.	Supporting alternative providers also requires Google to onboard coordinators for the Aggregation Service on that platform. We are concerned that delays in onboarding coordinators could have a negative impact on market participants, for example giving them less time to test their implementations and provide feedback.	We understand that Google has made efforts to mitigate any risk that the timeline for onboarding third-party coordinators could negatively impact the ability of market participants to provide feedback by allowing testing of new clouds before third-party coordinators are onboarded. We also understand that Google believes the operational difference between (a) Google acting as both coordinators and (b) Google and a third party acting as coordinators does not materially impact testing. Google has confirmed to us that Accenture is now operating as a third-party coordinator for Aggregation Service on AWS, and that it will have onboarded a third-party coordinator for GCP ahead of third-party cookie deprecation. We note that Google's selection criteria for third-party coordinators include a commitment to act as a trusted neutral party and responsibly manage the privacy and security of the system. This includes low reliance on the partnership as a source of revenue, and an agreement to make a published statement about their role as a coordinator; and technical expertise with cloud infrastructure and the ability to meet operational requirements. We invite further feedback from ad techs on this point. In addition, we have asked Google to specify what controls will be put in

Potential concerns	CMA views in January 2024 report	Updated CMA views
		place to ensure that Google does not influence the second coordinator. Google has said it has several safeguards that mitigate the concern that Google can influence the second coordinator. These include requiring the second coordinator to meet policies to maintain integrity of the system and not act in a way that undermines its security. Accenture has attested to acting in the above manner in a public statement[73] for Aggregation Services on AWS, and Google has given us assurances that the second prospective coordinator will make similar statements when they start operating as coordinator. Google will employ similar controls to meet security best practices, including limiting access to restricted information, and documenting when any access occurred. Our discussions with Google are ongoing on the question of monitoring of and appeal mechanisms for coordinators. We have also asked Google if there are any plans or considerations to remove Google as a coordinator, before or soon after third-party cookie deprecation. However, there are no plans at this stage to remove Google from being a coordinator, based on ensuring operational success, developing and adding new capabilities to the coordinator services and for security value. However, Google is open to re-evaluating this, including based on ecosystem feedback. We welcome feedback on this point. Stakeholders have also expressed concern that wording in the coordinator service reliability guarantees, specifically the phrase that Google does not 'make any specific promises about the coordinator service, any related service, report, feature or functionality, their reliability, availability, or ability to meet your

[73] See Accenture's public statement here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
		needs' protects Google without offering similar protection for market participants building on Privacy Sandbox tools. We have flagged this concern to Google.

50. We are only considering the application of **D&I D – User experience** for user-facing APIs and so have not reviewed TEEs under this criterion.

Summary

51. Google needs to resolve our concerns for TEEs and our current view is that this should involve taking the following steps:

(a) Provide ongoing public updates on the estimated costs of deployment and testing related to the TEEs for ARA and PA. This may include Google's offer to publish a statement outlining its technical approach to private cloud TEEs and asking for further stakeholder feedback on costs before third-party cookie deprecation.

(b) Respond to our concern that Google Ads might benefit versus competing ad techs from cost and latency efficiencies derived from using a cloud provider also owned by Google (i.e. GCP).

(c) Provide further information on the governance of the third-party coordinators, specifically the monitoring of, and appeal mechanisms for, coordinators.

(d) Clarify whether there will be a point at which the Coordinator Service will have warranty language that protects both advertisers and ad tech partners that are being asked to use Privacy Sandbox tools for billing purposes.

Strengthening cross-site boundaries

Related Website Sets

Overview

52. Related Website Sets (**RWS**) is a carve-out to third-party cookie deprecation, intended to mitigate site breakages. RWS allows a set of domains to be declared as belonging to the same party. Google has said that RWS is not designed for ads use cases, but that there is no prohibition from using RWS for ads purposes so long as that use complies with data protection laws.

When one site embeds another site and both are in the same RWS, Chrome will allow the embedded site to access its own cookies, which in the absence of RWS would be blocked as being third-party cookies; therefore, tracking across the domains within a RWS will be possible. RWS consists of a 'set primary' domain and 'set member' domains.[74]

53. Site owners declare related domains using one of three Google-defined subsets. The subsets are based on use cases, reflecting the purpose of the relationship between the set primary and the set member:

(a) Country code top level domains (ccTLDs): For example, google.fr is a ccTLD for Google in France. The 'ccTLD' subset can contain an unlimited number of domains meeting the formation criteria. In practice, the number of domains is limited to 255, the current number of ICANN ccTLDs.[75]

(b) Service domains: For example, domains used to isolate sensitive functions (such as supporting authentication flow) from user-facing domains. 'Service domains' are domains that provide key infrastructure for a service. The 'service' subset can contain an unlimited number of domains meeting the formation criteria.

54. 'Associated' domains: Google uses the example of maintaining user journeys across distinct brand websites. RWS could enable those companies to share cross-site data between those domains, if the set formation criteria were met. RWS will automatically grant cross-site access to the first five domains listed.

55. RWS relies on the Storage Access API to facilitate cross-site access for domains in the 'associated' set.[76] The Storage Access API is subject to technical controls that Google has said will discourage the use of the 'associated' subdomain for ads use cases.

56. The list of subsets may evolve. Google has told us that examples of declarations may help Chrome and the broader web ecosystem identify additional use case patterns to possibly create new subsets or new APIs. Google lists set formation requirements by subset on the RWS GitHub

[74] The RWS Submission Guidelines can be found on GitHub here (accessed on 22 April 2024).
[75] The ICANNwiki 'Country code top level domain' can be found here (accessed on 22 April 2024).
[76] An overview of how RWS uses the Storage Access API can be found on GitHub here (accessed on 22 April 2024).

repository.[77] Google applies technical validation to RWS submissions. There is currently no validation other than the technical checks.

Potential concerns

57. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

Potential concerns	Provisional CMA views based on ICO's preliminary assessment
The purposes for sets are not clearly recorded by set owners.	When submitting a set, we understand that set owners must provide a description of the cross-site processing purposes for the service and associated sets. Additionally, for associated sets, the RWS submitter must explain how/why users would expect the set domains to be affiliated. From the currently submitted sets, we observe that the free text field available to submitters is often completed with limited accuracy and/or for purposes that may be considered out of scope of the proposal.[78] Based on this information and the ICO's preliminary assessment, we are concerned that service and associated sets may be utilised for purposes other than those specified by Google in the set formation requirements. Additionally, we are concerned that inaccurately recorded purposes for cross-site data sharing undermines transparency for users visiting websites belonging to a set. In response, Google is considering the addition of structured fields (e.g. an enumerated list of 'common' rationales for set inclusion) to improve the consistency and accuracy of information submitted by set owners. This would also include a free text field. We await the proposed update to the submission process. However, outside of adding specificity to the submission process, Google has said that it will not actively limit how set owners choose to utilise the service or associated sets. Outside of the technical limitations, there are currently no restrictions in place regarding the purposes of RWS. We understand Google views the technical constraints of the API suitable to limit harmful misuse of the API. We await these potential updates and will reflect further together with the ICO as we continue our analysis.
The purpose for the set members sharing cross-site data is not clearly made available to the user.	We understand that the Chrome Settings UI does not provide information to explain why certain websites have grouped themselves in a set to share cross-site data. While this information may be available on RWS GitHub documentation, it is highly unlikely that most users will ever visit this repository.

[77] An overview of set formation requirements can be found on GitHub here (accessed on 22 April 2024).
[78] See currently submitted sets on GitHub here (accessed on 22 April 2024).

Potential concerns	Provisional CMA views based on ICO's preliminary assessment
	Together with the ICO, we consider that, in a post-third-party cookie deprecation landscape, it is additionally important to highlight where data is being shared cross-site. As a result, we are concerned that the Chrome UI does not explain to users the purpose of data sharing between set members. We consider that, currently, users will have insufficient clarity about the processing occurring within service and associated sets particularly. In response, Google has agreed to improve transparency in the Chrome UI. Further, based on the proposed changes to set submissions outlined above, Google is also exploring how structured data from set submission may be presented to users in the Chrome UI. We await Google's updates to the Chrome UI.
If misuse of RWS is observed on a large scale it will not be actively addressed.	We are concerned that RWS (in particular the service and associated sets) will be used for purposes beyond user-facing purposes/user experience. Based on the ICO's preliminary assessment, we are concerned that cross-site data sharing, within the bounds of RWS, involves a risk to replicate a range of data privacy concerns the ICO identified in its 2019 Report and 2021 Opinion. Given this, we are concerned that Google has no process or governance in place to address these risks if they materialise. Initially, we had believed that RWS was a temporary solution to assist websites with user experience breakages during the third-party cookie deprecation transition. Google has clarified that there is currently no intent to phase-out RWS. We understand Google views the technical limits (e.g. 5+1 TLDs in an associated set) placed on RWS are sufficient to limit the scope of misuse of the API. Google has said that more stringent controls on the use of RWS should not be imposed as this would necessitate a more centralised role for Chrome (contracts, enforcement, etc) that would raise concerns from third parties using RWS. Further, Google has said that sites using RWS must still comply with their own data protection obligations. Google intends to update its approach to governance for the Privacy Sandbox as a whole. We await further information to understand if improvements in this area might resolve our concerns.

58. Based on stakeholder feedback and our own analysis of the API, we have considered the following potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns identified based on further submissions from Google and other market participants since our last report was published in January 2024.

Potential concerns	CMA views in January 2024 report	Updated CMA views
Google discretion in merging RWS declarations into the canonical list.	Although only a handful of submissions have been made to date, it is clear a level of human intervention is still required in some cases. This will become a more urgent issue with scale as more submissions are made. We are concerned that this introduces the possibility of arbitrary discretion and would like Google to expand the governance framework to include a means for submitters to appeal if they disagree with a decision made by a human during the process. We have raised specific stakeholder feedback with Google.[79]	We shared stakeholder feedback around Google's discretion in approving requests to merge new RWS declarations into the canonical list with Google. Google published a response on GitHub in March 2024. Google's response clarifies the reasons that the specific pull request was rejected and notes that it intends 'to phase out human involvement and rely entirely on automated checks'.[80] We believe that moving to automated checks, as part of a broader governance process, is likely to resolve this concern.
Lack of clarity around the definition of 'ownership'.	We have considered stakeholder feedback around issues relating to ownership and data controllership within RWS. We recognise Google's desire to implement clear, automatable validation checks that effectively mitigate abuse. Automating checks also reduces Google's discretion, therefore reducing the risk that Google will govern RWS in ways that risk distorting competition. Google has implemented a /.well-known/ metadata requirement that essentially defines 'ownership' as administrative access to the set member domains. Developers place a copy of the RWS declaration in the /.well-known/ folder on each set member domain. This demonstrates that they have access to modify files on each domain in the set and prevents domains from being added to the set without their agreement. This removes some of the complexity in defining either corporate ownership or data controllership. We agree with Google's approach to technical validation based on access to a site's /.well-known/ directory.	We maintain our view that Google's approach to validating common administrative access to domains is appropriate.
RWS limits automatic cross-site data sharing to the first five	We believe that limiting auto-granted cross-site access to the first five domains in the 'associated' subset can reduce the risk of abuse when	We have discussed the five-domain limit further with Google. We note that the proposal evolved over time, Google took and considered feedback

[79] For example, see Movement for an Open Web's blog on RWS here (accessed on 22 April 2024).
[80] See Pull Request #148 on the Related Website Sets repository on GitHub here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
domains in the 'associated' subset.	compared to third-party cookies. We acknowledge stakeholder feedback that it may be possible to combine data from more than five domains in a manner that complies with data protection law. Google arrived at the five-domain limit after consultation with the ecosystem and undertaking user research and analysis. We expect Google to provide further evidence in support of this finding.	on larger and smaller numbers before settling on five. Google provided us with user research suggesting that a relatively small number of associated domains (fewer than 10) can aid user understanding. There are significant caveats around the research, so we do not consider it conclusive. Google also explained its desire to broadly align with the approaches that other browsers use when dealing with site breakages due to cookie deprecation. Stakeholders continue to express the view that limiting auto-granted access to five domains is 'insufficient' for their intended use cases, with some suggesting that RWS should include a feature to allow domain owners to share RWS data with a third party. We believe that this could undermine RWS. Despite stakeholder concerns, we are satisfied that Google's decision-making process in setting the auto-grant limit at five associated domains was sufficiently robust. Changes to the limit or attempts to abuse RWS should be managed within the Privacy Sandbox governance process that Google will set out.
Prompting flow can be disruptive and undermine user experience.	We consider that this strikes an acceptable balance between utility and privacy. RWS is primarily aimed at preventing site-breakages post third-party cookie deprecation. Prompting for additional cross-site data sharing requests by sites and services enables user choice and intervention to prevent breakage where access to wider cross-site data sharing beyond the limits imposed by RWS is required.	We maintain our view that the prompting flow strikes an acceptable balance between privacy and utility when used to mitigate the risk of site breakage.
Restrictions on the ability to combine data across sites disproportionately affects sites without access to logged-in users (e.g. news). Sites with a large	RWS, and Privacy Sandbox as a whole, will limit site owners' ability to share cross site data between 'associated' domains and this limitation may affect publishers' ability to build first party audience data. Some types of sites, specifically those with a high proportion of logged in users, may be less affected as they will have the option to combine data	We are considering whether further restrictions on Google's use of Google first-party data regarding user activity on sites other than those of the relevant publisher and advertiser are needed. Our discussions with Google are ongoing.

Potential concerns	CMA views in January 2024 report	Updated CMA views
proportion of logged-in users (e.g. Google) are less affected by the restrictions.	on logged in users on the server side. We are continuing to discuss the implications of this with Google. Paragraph 27 of the Commitments includes specific provisions on Google's use of Google First-Party Personal Data and Personal Data regarding user activity on sites other than those of the relevant publisher and advertiser to target and measure ads.	

59. As regards the application of **D&I D – User experience**, we note certain positive UX implementations Google is planning to introduce including structured rationale for set inclusions in RWS submissions and information provision to enhance user understanding of how RWS works and the underlying user benefits. However, we remain concerned that the RWS user flow may not be intuitive enough, and that users may not be sufficiently enabled to identify sites belonging to the same set and comprehend how their data is collected and shared across RWS member domains. We are continuing to engage with Google, which is also conducting further user research to resolve our concerns.

Summary

60. Google needs to resolve our concerns for RWS, and it has agreed to take the following steps:

(a) Consider the addition of a structured field to set inclusions in RWS submissions to allow for more concise characterisation of common purposes for set membership.

(b) Improve transparency in Chrome's UI by exploring how the structured data from set submissions may be presented to users.

61. In addition to these steps, our current view is that Google should:

(a) Improve RWS governance, including by defining and implementing clear policies relating to the Chrome team's role in defining the use case-based subsets, the set formation criteria, and the currently undefined process for managing disagreements between the decision maker and RWS submitter on whether a submission meets the criteria. Address feedback on user control and user experience.

Federated Credential Management

Overview

62. Federated Credential Management (**FedCM**) is intended to support federated identity on the web following third-party cookie deprecation, allowing users to choose which account to use to log in to a website via a dialog in the browser. Google has said that identity federation has played a central role in raising the bar for authentication on the web compared to per-site usernames and password in terms of trustworthiness, ease-of-use, and security.[81]

63. Federated identity solutions currently rely on technologies such as iframes, redirects and cookies – which provide vectors for user tracking across the web, and would be restricted by Google's Privacy Sandbox changes. Google has proposed FedCM as a privacy-preserving solution to enable relying parties (RPs) to provide users with a choice of identity providers (IdPs) for sign-in and authentication.

64. We are aware that both Mozilla and Apple are considering implementation of a variation of FedCM tools in their browsers, and that standardisation discussions are likely to continue in the newly chartered W3C Federated Identity Working Group.[82]

Potential concerns

65. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

Potential concerns	**Provisional CMA views based on ICO's preliminary assessment**
Websites will use the client_metadata_endpoint and dialogs to obtain invalid consent.	We understand that a website (RPs) can optionally use the client metadata endpoint to return the site's privacy policy and/or terms of service and display this, hyperlinked, in the Chrome-provided sign-in dialog. Under the Applicable Data Protection Legislation, valid consent for processing personal data must be freely given, specific, informed and unambiguous.[83] Based on the ICO's preliminary assessment, we are concerned that websites (RPs) may rely on the sign-in dialog and linked policies to obtain a user's consent as the lawful

[81] See Google Developer Blog on FedCM here (accessed on 22 April 2024).

[82] For more information on the Federated Identity Working Group see here (accessed on 22 April 2024).

[83] Article 4(11), Article 6(1)(a) and Article 7 GDPR. For more information on valid consent, see the ICO's website here (accessed on 22 April 2024).

Potential concerns	Provisional CMA views based on ICO's preliminary assessment
	basis of processing. Google is planning to update its developer guidance to make clear that presenting this information in the dialog does not constitute consent. We remain concerned that a significant portion of sites will use the Chrome FedCM dialog and client metadata endpoint to attempt to obtain an invalid consent for purposes beyond authentication. We are continuing our discussions with Google on this point.

66. Based on stakeholder feedback and our own analysis of the API, we have considered the following potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns identified based on further submissions from Google and other market participants since our last report was published in January 2024. New concerns raised by stakeholders during the reporting period are included at the end of the table.

Potential concerns	CMA views in January 2024 report	Updated CMA views
FedCM might be implemented in a way which negatively impacts competition between IdPs, including Google's own 'sign in with Google', through technical complexity of implementation.	We are working with Google and stakeholders to understand further the impact of technical complexity on IdPs which compete with Google.	Although Google has told us that it disagrees that competition between IdPs is relevant for the purpose of assessing the impact of FedCM on competition in digital advertising or publishers and advertisers, it has clarified that any technical complexity in the implementation of FedCM for IdPs is because it prioritised user usability over ease of deployment when designing the API. Google has said that it has also sought to minimise technical complexity where possible e.g. using existing IdP JavaScript SDK libraries that many IdPs already provide, and that most RPs auto-load into their websites. Furthermore, Google has informed us that it is developing features to increase user choice of IdP. For example, with Multi-IdP API, it is exploring ways to support multiple IdPs to coexist cooperatively in the FedCM account chooser.[84] We would encourage it to continue these efforts. In the absence of any further stakeholder feedback, and based on

[84] See issue #319 on the FedCM repository on GitHub here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
		the information currently available, we do not consider that any technical complexity for IdPs in implementing FedCM will have a negative impact on competition between IdPs, including Google's own service, but we will continue to monitor developments.
Google might unfairly benefit from greater use of federated ID within advertising solutions, as cross-domain signals are reduced.	Although we do not view support for a use case in which Google has an interest to be, in itself, an act of self-preferencing, we are keen to understand this dynamic further. We would be concerned if Google implemented FedCM in such a way which benefited its own IdP and will continue to monitor this risk.	Google has told us that, although it can envisage possible downstream advertising use cases based on signed-in users to various websites and platforms, FedCM is not intended to support advertising use cases, and has not been designed with advertising use cases in mind. We have asked Google to confirm that it does not have any plans to use personal data derived from its own IdP, Google Sign-In, on third-party sites for the targeting or measurement of digital advertising. We look forward to receiving Google's response on this before coming to a view in relation to this potential concern.
FedCM might disintermediate publishers, restricting their ability to track users on their property.	We consider this risk to be low given that it is the publishers' choice whether to support federated login as opposed to managing user sign-in themselves. However, we invite views from publishers to understand if this is an outstanding concern.	Stakeholder have raised concerns that FedCM could restrict publishers' access to user email addresses, which can be used in cross-site identity resolution. Based on the information currently available, we do not consider that this represents an outstanding concern.
FedCM might not support the broadest range of features, limiting its effectiveness.	We are encouraged by engagement on GitHub with respect to additional use cases and will continue to monitor the situation.	Google has told us that the initial design of FedCM was focused on consumer federated identity use cases, and that it is aware of API details which need to be improved to support wider use cases. In particular, Google has told us that its original intention was for enterprise identity use cases to rely on existing Chrome enterprise policies. However, it has now heard from enterprise identity vendors that would prefer API-based solutions. Google has told us this is an area which it is actively investigating. Google has informed us of further feedback it has received about the lack of cross-browser support for FedCM.

Potential concerns	CMA views in January 2024 report	Updated CMA views
		We are aware that Google is working to enable cross-browser support by collaborating on developing FedCM through the W3C Federated Identity Community Group and W3C Federated Identity Working Group. Google has said that alternatives, such as Storage Access API and Cookie Access Heuristics, allow log-in use cases to be addressed cross-browser in interoperable ways. We have been made aware of recent stakeholder activity on GitHub raising further use cases requests related to FedCM. We will continue to monitor the situation and encourage interested parties to continue to engage on GitHub.
It may not be feasible for industry to adopt FedCM ahead of third-party cookie deprecation.	N/A	A stakeholder raised the point that high migration efforts and lack of cross-browser standardisation meant FedCM might not be a feasible short-term solution at third-party cookie deprecation. In response, Google has told us that it believes FedCM should be relatively easy to implement but that it will continue to promote awareness and adoption of FedCM, including by smaller IdPs. It also said it hopes that the recently launched W3C Federated Identity Working Group will continue to drive cross-browser support of federated identity solutions, and act as a resource for developers to raise questions and provide feedback. We would invite further views from stakeholders related to this potential concern.

67. As regards the application of **D&I D – User experience**, there are concerns as to whether the user will receive sufficient transparency with respect to how their data will be used for advertising purposes. Google has said that FedCM allows IdPs to include links to the RP’s Terms of Service and Privacy Policy on sign-in prompts. However, we remain concerned about the likelihood of users accessing the links and their ability to make informed decisions. Google has also told us that it is looking into introducing a new ‘button flow’ feature which would allow users to deliberately launch the sign-in screen, even if there are settings enabled which normally block such prompts. We are

continuing to discuss this and other changes to the FedCM user experience with Google to ensure users can make effective choices.

Summary

68. Google needs to resolve our concerns for FedCM and has agreed to take the following steps:

(a) Update its developer guidance to clarify that websites must not rely on the client_metadata_endpoint and Chrome FedCM dialogs as valid consent.

69. In addition to these steps, our current view is that Google should:

(a) Consider and respond with additional solutions that will further discourage the use of the FedCM dialog box to obtain consent for purposes beyond authentication.

(b) Confirm that it does not have any plans to use personal data derived from its own IdP or Google sign-in on third-party sites for the targeting or measurement of digital advertising.

(c) Continue to work closely with industry to support adoption ahead of third-party cookie deprecation, and eventually cross-browser standardisation.

Shared Storage API

Overview

70. The Shared Storage API is a general purpose API that primarily supports two use cases: (i) URL selection (including event level reporting to be deprecated from 2026 onwards); and (ii) output for Private Aggregation API. It provides a generic storage facility for cross-site data to meet legitimate use-cases that were previously facilitated by cross-site cookies.

71. The API can be written to at any time into a shared data storage mechanism; however reads are restricted by ’output gates’, operation within secure worklets (to prevent data exfiltration) and privacy-preserving mechanisms.

72. The first gate is the content Selection output gate. This includes functionality for creative rotation of ads, A/B testing, and a limited ability to provide trust signals (although Google have made clear this only supports, not supplants, Private State Tokens for this particular use case), among other functions. The second gate is the Private Aggregation output gate, which sends reports to be aggregated and includes functionality for unique reach.

Potential concerns

73. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

Potential concerns	**Provisional CMA views based on ICO's preliminary assessment**
At third-party cookie deprecation, Shared Storage API will be deployed without a number of key technical privacy controls.	A range of planned PETs will not be implemented by Google until at least 2026. These include: Fenced Frames; a replacement for event level reporting and/or the enforcement of the Private Aggregation API for measurement of the Select URL gate. We are concerned that the absence of these features will allow API callers to join user activity across sites. Prior to the implementation of expected mitigations, Google has implemented additional per-page entropy budget for the Select URL gate. Based on the ICO's preliminary assessment, we view them as only partially effective. Google is exploring possible monitoring of these controls to assess effectiveness against misuse. The ICO has told us that without these PET controls, the privacy-guarantees are significantly undermined for the Select URL Gate, and that the Shared Storage API may not mitigate key issues the ICO identified in the 2019 Report and 2021 Opinion. We are working with the ICO and Google to understand further details on Google's proposed governance approach, and this will include understanding if alternative assurances can be provided ahead of 2026.
Future 'gates' may be added to the Shared Storage API, and this may change the risk profile of the API and potentially wider Sandbox Proposals.	We understand that, in the future, additional output gates may be added to the Shared Storage API (e.g. in addition to the Select URL and Aggregate Reporting gates). We are concerned that new products/features added to the proposal will introduce additional risk to users that cannot be evaluated at the time of writing. Google has said that its intent is to add meaningful functionality without undermining privacy limitations of this and other Privacy Sandbox APIs. Google is considering how a decision-making process might be established to govern the addition of new use cases to the Shared Storage API. We await further information from Google and will consider this as part of our wider work looking at governance and future decision-making.
Key controls, such as epsilon values and rate limits, have not been tested.	For the Private Aggregation API, as with the ARA API, we understand that key controls (e.g. epsilon values and contribution budgets) have been initially set as placeholders/'strawmen' during testing and adoption of the API. We are concerned that key controls and parameters for the Private Aggregation API have not been effectively tested to establish the optimum balance between utility and privacy. There is also a concern that Google will not be able to gather useful feedback from Private Aggregation 'customers' as API callers are likely to have a

Potential concerns	Provisional CMA views based on ICO's preliminary assessment
	vested interest in preserving maximum utility. Effective testing is for Google to define. Google has said that the current epsilon parameter can be revisited over time as technical improvements are made to the aggregation service. Google is exploring how they will work with customers to test and migrate to new epsilon values over time.

74. Based on stakeholder feedback and our own analysis of the API, we have considered the potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**.

75. The CMA does not currently have any specific or immediate major concerns for this API, especially as it is primarily used to support or extend other Privacy Sandbox APIs or as a general use API. Given its supporting role, however, future governance and monitoring will be important.

76. As regards the application of **D&I D – User experience**, the ICO has expressed concern that the use cases fulfilled by the Shared Storage API are not clearly presented to the user. Google has accepted this and has agreed to refresh the UI. We await more information on this.

Summary

77. Google needs to resolve our concerns for Shared Storage API, and it has agreed to take the following steps:

(a) Provide more information on governance and decision-making processes and ensure these are adequate.

(b) Reconsider and update the UI.

(c) Consider how it will work with customers to test and possibly migrate to new epsilon values over time.

Cookies Having Independent Partitioned State

Overview

78. Cookies Having Independent Partitioned State (**CHIPS**) is intended to support the embedding of third-party services within webpages after third-party cookie

deprecation, without re-enabling cross-site tracking.[85] It enables developers to read and write cookies from cross-site contexts, such as iframes, in a strictly partitioned manner such that a cookie may only be accessed within the context of the top-level site where it was set.[86] Third parties who set partitioned cookies on separate webpages are not able to join up this information.

79. Google has said that CHIPS is necessary to support users' expectations of businesses on today's Internet and to facilitate website functionality such as:

(a) Third-party embedded services including chat, maps, and payments;

(b) Third-party Content Delivery Networks servicing access-controlled content which must be authorised by the first-party site; and

(c) Embedded ads relying on per site frequency capping or user preferences.

80. Other browsers have considered measures to address these use cases. Firefox's solution involves partitioning all third-party cookies by default, while Safari previously attempted to partition based on heuristics before instead blocking all third-party cookies.

81. CHIPS takes a different approach and requires developers to explicitly opt-in, which Google has said will reduce confusion and unexpected bugs. CHIPS is being discussed in W3C's Privacy Community Group and appears to be moving towards cross-browser support, with outstanding discussion relating to performance and memory rather than security or privacy concerns.[87]

Potential concerns

82. The ICO has not raised any concerns under **D&I A – Privacy outcomes** for CHIPS.

83. We have considered the following potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns

[85] An overview of the CHIPS proposal can be found here (accessed on 22 April 2024).

[86] Google provides the following illustrative example: 'For instance, when chatvendor.com is embedded on site A.com, it could request a "Partitioned" cookie to be set. Later, when chatvendor.com is loaded on site B.com, it cannot access the cookie and associated data set by it when it was previously loaded on A.com. chatvendor.com cannot join cookies that it sets across A.com and B.com to track users across the web, but chatvendor.com's key functionality of knowing who a user is across successive visits to a specific top-level site is still possible – without A.com or B.com having to trust chatvendor.com more than they do today'.

[87] See Chips repository on GitHub here (accessed on 22 April 2024).

identified based on further submissions from Google and other market participants since our last report was published in January 2024. New concerns raised by stakeholders during the reporting period are included at the end of the table.

Potential concerns	**CMA views in January 2024 report**	**Updated CMA views**
The partitioning of cookies by domain may reduce the ability of ad techs to compete on the targeting and measurement of advertising based on cross-domain tracking.	We accept that a reduction in cross-domain tracking is necessary to achieve the privacy benefits of third-party cookie deprecation. We will consider this balance as part of our overall assessment of Google's proposals.	We have not received any further feedback related to this potential concern following our January report. As previously noted, we accept that a reduction in cross-domain tracking is necessary to achieve the privacy benefits of third-party cookie deprecation. We will consider this balance as part of our overall assessment of Google's proposals.
CHIPS might be implemented in such a way which does not sufficiently enable advertising use cases.	We would like to understand further the extent to which CHIPs preserves existing advertising use cases.	Google has told us that CHIPS is not intended for ads use cases. We agree with Google's assessment in this case. CHIPS is one of several Privacy Sandbox APIs that is aimed at addressing non advertising use-cases that will be impacted by third party cookie deprecation such as sign-on systems.
The partitioning of cookies by domain may reduce the effectiveness of tools for the targeting and measurement of advertising based on cross-domain tracking.	We accept that a reduction in cross-domain tracking is necessary to achieve the privacy benefits of third-party cookie deprecation. We will consider this balance as part of our overall assessment of Google's proposals.	We have not received any further feedback related to this potential concern following our January report. As previously noted, we accept that a reduction in cross-domain tracking is necessary to achieve the privacy benefits of third-party cookie deprecation. We will consider this balance as part of our overall assessment of Google's proposals.
CHIPS might be implemented with insufficient memory to enable the third-party services required by, in particular, small publishers.	Google continues to make best efforts to ensure CHIPS is implemented with sufficient memory to support the greatest range of use cases. We are also pleased to see Google's engagement with other browsers, and willingness to make changes in order to progress CHIPS towards standardisation.	Our view remains unchanged.
CHIPS may impact the ability of publishers to offer SSO sign-in services based on authenticated embeds.	We note Google's intent to support authenticated embed use cases through Storage Access API with user prompts and continue to monitor. We would also like to understand the extent to which FedCM mitigates this concern by enabling SSO sign-in use cases.	Google has since implemented a fix for this in Storage Access API. We welcome further feedback on the extent to which this fix resolves stakeholder concerns.

Potential concerns	CMA views in January 2024 report	Updated CMA views
Implementation of both ‘normal’ cookies and CHIPS partitioned cookies for SSO during the transition period will create significant overheads for market participants.	N/A	This will be an ongoing concern for CHIPS and other APIs where old and new methods are operating in parallel. We welcome feedback from stakeholders on the impact of this issue. We have asked Google to consider ways it can mitigate these transition costs.
Even where Storage Access API is modified to resolve issues in CHIPS, there is not yet a consistent cross-browser implementation of Storage Access API so this will increase costs for market participants.	N/A	Google has told us that it is making progress with standardising both Storage Access API and CHIPS across browsers. Mozilla is implementing CHIPS and Google is currently in discussion with Webkit (required for all iOS browser implementations) regarding CHIPS implementation. Mozilla have shipped a modified specification of the newly specified Storage Access API that reduces implementation differences.

84. As regards **D&I D - User experience**, we have concerns around the user controls for CHIPS and first-party cookies not being distinct from each other. Google in response has said that distinct controls could lead to significant breakage risk, user confusion and lack of meaningful privacy improvement. We are continuing to engage with Google to ensure adequate user controls for CHIPS.

Summary

85. Google needs to resolve our concerns for CHIPS and our current view is that this should involve taking the following steps:

(a) Ensure that the ability of publishers to offer single sign-in services via authenticated embeds is preserved, especially during the transition period where stakeholders (including and especially non-ad tech stakeholders) may experience significant overheads in maintaining support for both old and new methods.

(b) Ensure that CHIPS is implemented with sufficient memory to enable third-party applications relied upon by publishers.

(c) Help mitigate costs for stakeholders who have to maintain parallel stacks in the lead up to third-party cookie deprecation.

(d) Work towards a consistent cross-browser implementation of Storage Access API where it affects CHIPS users.

Fenced Frames

Overview

86. Fenced Frames aims to enforce a boundary between a webpage and any cross-site content it embeds, such that user data cannot be joined up between the two sites. Under Google's PA proposal, Chrome renders the winning ad in a Fenced Frame. The requirement to render winning ads within Fenced Frames will be enforced no sooner than 2026.[88]

87. Google is continuing to make gradual progress in enabling various Fenced Frames solutions, illustrated by the increased GitHub explainer updates from October 2023. Fenced Frames does not support the same use cases as iframes currently. For example, PA supports video rendering using a mechanism that relies on iframes, and Google has not yet designed a solution that is compatible with Fenced Frames, which could significantly impact advertisers' revenue.

Potential concerns

88. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

Potential concerns	**Provisional CMA views based on ICO's preliminary assessment**
Outstanding cross-site tracking risks remain unmitigated.	We note that the Fenced Frames proposal currently maintains a range of unmitigated cross-site tracking risks.[89] The ICO's 2021 Opinion sets out its expectation that proposals must address existing risks, as well as considering any new risks that are introduced and how these will be mitigated before any processing takes place in order to comply with Applicable Data Protection Legislation.

[88] The timelines of pending PA API capabilities can be found here (accessed on 22 April 2024).

[89] See the Fenced Frames Explainer here (accessed on 22 April 2024).

	Once we receive further updates on how Google is planning to address these risks, we will consider whether our concerns have been resolved.

89. Based on stakeholder feedback and our own analysis of the API, we have considered the following potential concerns under **D&I B – Digital advertising** and **D&I C –** Impact **on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns identified based on further submissions from Google and other market participants since our last report was published in January 2024.

Potential concerns	**CMA views in January 2024 report**	**Updated CMA views**
Fenced Frames does not currently support use cases such as native and video advertising, which may impact the ability of publishers to effectively monetise their content.	Google should implement changes to enable these key use cases before requiring ads to render in Fenced Frames.	See PA API section above.
Fenced Frames does not sufficiently support brand safety.	N/A	A stakeholder raised a concern that, by restricting information about page context, Fenced Frames does not sufficiently enable advertisers to ensure brand safety. Google has said in response that advertisers can ensure brand safety within Fenced Frames by analysing the page URL during the contextual auction, and preparing perBuyerSignals which can be used to filter out ads which do not meet brand safety standards. We welcome further feedback from stakeholders on this concern.

Potential concerns	CMA views in January 2024 report	Updated CMA views
Fenced Frames does not sufficiently support expandable ads use cases.	N/A	A stakeholder raised a concern that Fenced Frames does not sufficiently enable advertisers to display expandable ads. Google has confirmed that expandable ads use cases are not intended to be supported. According to Google, a key privacy goal of Fenced Frames is that the surrounding web page cannot learn what ad is being rendered, which would be necessary in order to support expandable ads. We welcome further feedback from stakeholders on this concern.

90. Currently, we do not have any outstanding concerns in relation to the application of **D&I D – User experience**.

Summary

91. Google needs to resolve our concerns for Fenced Frames and our current view is that this could involve taking the following steps:

(a) Provide further assurances on how it will mitigate cross-site tracking risks within Fenced Frames.

(b) Continue to engage with industry on the design of Fenced Frames, including by not enforcing its requirement until major ad formats are supported.

Fighting spam and fraud on the web

Private State Tokens

Overview

92. Private State Tokens (**PST**) enables trust signals to be transmitted between websites to determine whether a user is trustworthy or engaged in spam or fraud without allowing the user's identity to be discovered across sites. Instead, the PST aims to enable sites to collaborate in segmenting users into 'trusted' and 'untrusted' categories. To do so, a website that has already established a user's trustworthiness would be able to issue that user's

browser with PSTs.[90] These tokens could then be redeemed on other websites establishing trust without identifying the user or providing information on the origin of the token. The tokens themselves will allow for limited information to be communicated.

93. As part of the registration process for becoming a PST issuer, issuer websites need to declare the intended purpose of the tokens. By design, it is not possible to easily determine the purpose of a token. Therefore, while Google may be able to infer some misuse of PST tokens over time, it is not easily detectable.

Potential concerns

94. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

Potential concerns	**Provisional CMA views based on ICO's preliminary assessment**
PST can be used for purposes wider than anti-fraud or in ways that are unfair to the user.	We understand that PST allows token issuers to assign a user one of six values when issuing tokens that may be based on, potentially, non-transparent issuer-defined metrics. Based on this understanding and the ICO's preliminary assessment, we are concerned that: • Tokens may be used to assign values to users for purposes other than anti-fraud/security etc. • Tokens may intentionally or unintentionally influence a user's browsing experience in a way which is unfair. We understand that the PST enrolment process only conducts technical checks and does not review the purpose and means of processing undertaken by the issuer. Google has said that with expected key rotation, in practice, an issuer will not be able to use all six metadata values simultaneously. Additionally, as sites are limited to two issuers only, it is Google's view that sites will not want to 'waste' a limited anti-fraud capability on a relatively poor cross-site tracking tool. Further, Google believes that improvements to the issuer declaration process (see below) can assist with preventing misuse of PST. Google has agreed to make it clearer that PSTs are 'not intended to convey arbitrary cross-site information'.[91] We discussed with Google the possibility of removing token issuers if clear misuse was identified. On this final point, we await further detail on Google's wider approach to governance.

[90] This website is known as the 'issuer'. Any website can issue PSTs.

[91] See the Private State Token API Explainer here (accessed on 22 April 2024).

The purposes of tokens are not made sufficiently clear by issuers.	As regards the transparency of PST for users, we observe: • Registered PST issuers are recorded publicly in a JSON file stored in the PST GitHub.[92] • Each issuer's application may also be viewed in the GitHub issues where it was submitted. Purposes for PST use are declared in a free text field and are not validated. • In the Chrome UI, information regarding PST is exposed via a setting called 'Auto-verify', but with no information linking to the third parties providing the services or their purposes for processing. • Chrome is reliant on site owners using third party issuer services to provide relevant information to consumers and maintain relevant data protection compliance. From the observations above, we are concerned individuals will not be able to clearly understand all use cases PST may address now and in the future. Google has agreed to include the purposes from the issuer application directly in the JSON file and is exploring updating the open text field to a defined list. Additionally, Google has agreed to increase visibility of the guidance for the use of PST in developer documentation. Also, Google is considering updates to the PST ('Auto-verify') Chrome UI to make clearer to users the purposes of processing and the roles third parties are likely to undertake.

95. Based on stakeholder feedback and our own analysis of the API, we have considered the following potential concerns under **D&I B – Digital advertising and D&I C – Impact on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns identified based on further submissions from Google and other market participants since our last report was published in January 2024.

Potential concerns	**CMA views in January 2024 report**	**Updated CMA views**
PST could centralise Google's power by requiring sites to rely on Google to determine whether a user should be trusted.	While any entity can become a PST issuer, we believe it is conceivable that the main issuers will be well-known sites that most people visit. Given that Google owns several domains that are among the most visited sites, it is in a strong position to become a prominent and trusted issuer that is relied on by many sites.	Google has told us that it does not currently envisage issuing/using PSTs. Our understanding is that the use of PSTs is optional and that anti-fraud organisations can rely on other signals besides PSTs. However, we have received further concerns from stakeholders regarding the risk to competition of Google becoming a dominant issuer of PST tokens. Given the above, we have evaluated two possible solutions to this concern.

[92] See the Private State Tokens issuers recorded here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
		One of the options we considered was for Google to formally agree not to enter the market for PSTs in future. Alternatively, we suggested that the design of PSTs could be modified to introduce a limit on the number of partner websites that can redeem tokens from an issuer, to reduce the risk of issuer dominance. After careful consideration and discussions with Google, we came to the view that these potential solutions would not be appropriate given the limited evidence that this concern would lead to a material impact on competition in the ad tech market. Google has reassured us that the use of PSTs issued by Google will not be required, and that redeemers will be able to consume PSTs issued by a third-party other than Google. Moreover, Google has said that the largest proportion of adoption and interest in becoming PST issuers has come from small and midsize businesses. Furthermore, it is unlikely that any one issuer would be relied on by many sites. Google has said that this is because anti-fraud use-cases span a wide range of threats, so different verticals would likely have their own issuers.
Google could abuse its position as a dominant PST issuer.	To mitigate the risk to competition of Google becoming a dominant issuer of PST tokens, we recommend that Google provide policy or technical safeguards that would prevent it from abusing its position. This could be enforced through the registration and governance mechanisms that have yet to be clarified in the PST proposal. We would particularly welcome governance policies that specify why certain issuers might be disallowed from issuing PST tokens.	Google informed us that it is working to define objective criteria on how PSTs can be used, and the circumstances in which an issuer would be removed for violating those criteria. Google envisages publishing this guidance ahead of third-party cookie deprecation.
There will not be enough choice of PST issuers.	Our understanding is that Google has already provided demos and guides to help with setting up and running an issuer, but this does not guarantee that there will be enough competition and enough choice of issuers that are broadly trusted. To obtain greater assurance on this, Google could provide a target for how many PST issuers are expected to exist (and be	Google has told us that it is actively seeking to encourage adoption and increase the number of PST issuers. Google also considers it likely that the use of PST for anti-fraud use cases will span a wide range of threats, so there would be a variety of issuers that specialise in different verticals.

Potential concerns	CMA views in January 2024 report	Updated CMA views
	actively used to redeem tokens) by the time third-party cookies are deprecated.	We have not received further feedback from stakeholders on this point. We will continue to monitor developments.

96. As regards the application of **D&I D – User experience**, our understanding is that PST is enabled by default (except for those who had previously blocked third-party cookies), although users can opt-out or otherwise negate the functioning of PSTs using an ‘Auto-verify’ feature in Chrome. As mentioned in the **D&I A – Privacy outcomes** section above, given that PST currently permits a non-exhaustive range of use cases, we are concerned that market participants may use PST data for purposes besides verification. We consider this to be problematic, as users will not be made aware of the other purposes for which their data may be used. In response to our concerns, Google is exploring ways to ensure better transparency of how PSTs may be used and to prevent misuse of PSTs. We are continuing to engage with Google on this and other concerns relating to user experience, including around PST user controls.

Summary

97. Google needs to resolve our concerns for PST, and it has agreed to take the following steps:

(a) Provide clear registration and compliance guidance for PST issuers in published guidance. The guidance will specify that PSTs should not be used for purposes other than anti-fraud and Google is exploring a mechanism for users to report complaints about potential misuse.

(b) Improve transparency for users on the purpose of PSTs by including this information in the issuer application and increasing the visibility of relevant guidance.

(c) Update the PST (‘Auto-verify’) Chrome user interface to make clearer to users the purpose of processing and third-party roles.

Limiting covert tracking

Bounce Tracking Mitigations

Overview

98. Bounce Tracking Mitigations (**BTM**) is intended to address cases where sites use a 'stateful bounce' to identify users across different sites. A 'stateful bounce' allows sites to replicate the cross-site tracking functionality of third-party cookies. For example, the user navigates to Site A, Site A redirects the user to Site B, Site B accesses state (e.g. sets a cookie, accesses local storage, and so on) and redirects the user again either back to Site A or to another site.

99. These redirects can happen quickly, and users may not be aware of them. Google's implementation of BTM relies on user interaction. If the user has interacted with the site that they are redirected to (Site B in our example above) within the last 45 days, the 'stateful bounce' will be allowed, otherwise the state (e.g. the cookie set by Site B in our example) will be deleted.

100. Google has identified some use cases that rely on stateful bounces that will continue to work because they involve user interaction. These use cases include: (i) federated authentication, (ii) single sign on; and (iii) payments.[93] Google has invited specific feedback on whether user interaction is the most appropriate signal to indicate that the stateful bounce is part of a use case that should be supported under BTM.[94]

Potential concerns

101. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

Potential concerns	**Provisional CMA views based on ICO's preliminary assessment**
Sites frequently visited by users will still be able to use bounce tracking.	We are concerned that large sites, that may retain a large percentage of a population group as monthly active users, would still be able to undertake effective bounce tracking. We are currently discussing this with Google and we will provide an update in the next quarterly report.

[93] An overview of out-of-scope use cases can be found here (accessed on 22 April 2024).

[94] See issue #24 on the Navigation-based Tracking Mitigations repository on GitHub here (accessed on 22 April 2024).

102. Based on stakeholder feedback and our own analysis of the API, we have considered the following potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns identified based on further submissions from Google and other market participants since our last report was published in January 2024. New concerns raised by stakeholders during the reporting period are included at the end of the table.

Potential concerns	**CMA views in January 2024 report**	**Updated CMA views**
There is a risk that the current implementation of BTM will disadvantage competitors that rely on legitimate use of browser storage.	Our understanding is that the user interaction requirements of BTM may undermine the ability of competitors and other stakeholders in the Privacy Enhancing Technology (PET) market to use redirect flows for legitimate purposes. Google's response to this issue [95] recommends using additional consent flows or the Storage Access API. However, we were informed by stakeholders that these options would add an unacceptable level of user friction that would break their use case. We are continuing to discuss with Google how these concerns may be resolved. This includes exploring an alternative implementation of BTM that could use list-based approaches to identify trackers, or adapting the Shared Storage API in a way that would allow legitimate use of browser storage by PETs.	Stakeholders have reiterated their concern that Google is placing disproportionate user interaction requirements on alternative solutions beyond what is required by data protection law. Specific stakeholder proposals for resolving the issue have included an 'allow list' approach, where Google would be required to facilitate access to bounce tracking and unpartitioned client-side storage for alternative solutions whose cross-site data processing has been accredited by an independent external auditor. We are discussing the feasibility of this proposal and alternative approaches with Google.
Sites that are regularly visited by users (i.e. more than once every 45 days) will still be able to use bounce tracking.	We are concerned that Google would be able to circumvent the protections provided by BTM because of the large volume of user interactions that Google sites receive. This could give Google an advantage over competitors that have smaller audiences. We have asked Google to confirm that it will not use bounce tracking outside of their accepted use cases (e.g. login and payments).	We are currently discussing this concern with Google, and we will provide an update in the next quarterly report.

[95] See issue #64 on the Navigation-based Tracking Mitigations repository on GitHub here (accessed on 22 April 2024).

Potential concerns	CMA views in January 2024 report	Updated CMA views
There is a risk that BTM will reduce competitors' ability to use link decoration.	We have received concerns that Google's implementation of BTM tampers with URL strings. Our understanding is that link decoration is not affected in the current implementation of BTM or other Privacy Sandbox proposals.	Our views remain unchanged. However, as noted in the D&I A section for ARA, our understanding is that link decoration currently allows ad techs to join a user's identity across sites via navigation events. Google has pointed to a range of anti-covert tracking (ACT) efforts that strive to make covert tracking more challenging. We will review our position in response to any further details or controls that may be shared by Google in response to the concern around navigation tracking.
There was insufficient industry consultation before the release of BTM.	Industry stakeholders have had the opportunity to comment on Google's BTM proposal since it was announced publicly in September 2022. Possible avenues for stakeholder engagement include the corresponding GitHub repository[96] and relevant W3C groups.	Our views remain unchanged.
BTM currently has a bug that causes it to delete Privacy Sandbox API storage.	N/A	Google has told us that it has identified cases where BTM cleared storage related to Privacy Sandbox APIs, and that this primarily affects ad techs using their own domains for click tracking and API calls. Google estimates that the current impact of this bug is minimal, affecting less than 1% of users in the Mode-B experiment. Google has disabled BTM in Mode B Chrome-facilitated testing experiment traffic until a fix is confirmed.

103. As regards the application of **D&I D – User experience**, we consider that Google has taken adequate precautions to ensure that BTM does not adversely affect user experience. Such precautions include periodic reviews and deletion of stored data only if the user has not interacted with a site in 45 days, as well as a 1-hour grace period that allows the user to complete their interaction before the site host's storage is deleted. These precautions help to minimise the impact of BTM on legitimate use cases such as payment flows.

[96] See the Navigation-based Tracking repository on GitHub here (accessed on 22 April 2024).

104. We will continue to monitor how BTM impacts user experience in technologies that currently rely on redirection and browser storage for legitimate use cases (e.g. PETs and authentication).

105. Although BTM will not be enforced until after third-party cookie deprecation, BTM is currently available for testing/use by anyone who has already blocked third-party cookies. This gives stakeholders and users an opportunity to monitor and feedback on the impact of BTM on user experience before it becomes fully operational.

Summary

106. Google needs to resolve our concerns for BTM, and our current view is that this should involve taking the following steps:

(a) Resolve concerns related to the disproportionate consent requirements imposed by BTM on alternative solutions, potentially making it harder for competitors to use redirect flows for legitimate use cases.

(b) Confirm that the current BTM implementation would not allow sites with a large first party presence (like Google's sites) to use bounce tracking. We are waiting for Google's confirmation on this point.

User-Agent Client Hints/User-Agent Reduction, IP Protection, DNS-over-HTTPS, Storage Partitioning and Network Partitioning

Overview

107. The purpose of **User-Agent Client Hints** (**UA-CH**), which follows from **User-Agent Reduction** (**UAR**), is to limit passive fingerprinting of users, limiting the amount of information the browser automatically delivers about the user to the web server it interacts with through the User-Agent String. The User-Agent String is transmitted as a request header in every HTTP exchange between client and server. The process is generally opaque to users. UA-CH therefore enforces a model whereby the server must actively request identifying details about the client that could be used for fingerprinting (e.g. device model) rather than passively receive them.

108. **DNS-over-HTTPS** is a protocol that encrypts the interactions between client (browser) and Domain Name System (DNS) provider to enable further privacy protection for browsing habits, preventing surveillance of sites requested/visited. DNS-over-HTTPS also prevents active attacks that attempt to divert browser-traffic to malicious servers (a common attack in public wi-fi settings such as cafes and airports, including for phishing purposes). As a

further security measure, DNS-over-HTTPS traffic can also be mixed with other HTTPS traffic on the same connection.

109. **IP Protection** is a proposed privacy feature in Chrome that aims to avoid sharing a user's real IP address with eligible third parties. Under the current proposal, a privacy proxy will be used to anonymise eligible users' IP addresses.[97] Google will use two proxies where the first is run by Google and the second by an external content delivery network (CDN). Google's aim is to (i) stop a destination website from seeing a user's original IP address and (ii) prevent any single proxy from seeing both the user's original IP address and traffic content.

110. **Storage Partitioning** isolates some web platform APIs used for storage or communication if used by an embedded service on the site, i.e. in the third-party context.

111. A browser's network resources, such as connections, DNS cache, and alternative service data are generally shared globally. **Network State Partitioning** will partition much of this state to prevent these resources from being shared across first-party contexts. To do this, each request will have an additional 'network partition key' that must match in order for resources to be reused.

Potential concerns

- *User-Agent Client Hints/User-Agent Reduction*

112. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

Potential concerns	Provisional CMA views based on ICO's preliminary assessment
'Critical Hints' is likely to be used for non-compliant fingerprinting.	The key difference between the User-Agent String and UA-CH is that UA-CH changes the model of receiving information from passive to active. Rather than a site passively receiving all the available information for requests, UA-CH requires the site to make active requests for the hints it needs, in such a way that a browser may observe such calls and intervene, depending on site permission policies. In theory, this should be beneficial for user privacy, as the amount of information made available by default has been reduced.

[97] An overview of the IP Protection proposal can be found here (accessed on 22 April 2024).

	The ICO has told us that this proposal has limited effectiveness as a stand-alone anti-fingerprinting tool and would ideally work alongside other Privacy Sandbox proposals. The ICO considers that the effectiveness of this proposal has been undermined by the deprecation of the Privacy Budget proposal and the limited scope of the IP Protection proposal. We await more information from Google to better understand the future intent for this API given the demise of Privacy Budget.

113. Based on stakeholder feedback and our own analysis of the API, we have considered the potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**.

114. Although we do not currently have concerns about UA-CH/UAR, we are keen to ensure that Google does not remove or limit access to critical hints in the future. A stakeholder has drawn our attention to a research paper[98] published last year that studied the use of UA-CH on thousands of websites. The paper notes that Google accounted for both the overwhelming majority of 'critical hint' requests (high entropy, potentially identifying) and exfiltration of this data to external servers. We are awaiting comment from Google.

115. We have also asked Google to clarify its normative language in the UA-CH developer documentation giving the directive that sites 'should not' make heavy use of critical hint requests as this implies Google may impose some restriction in the future. Given the evidence above that Google is currently the primary consumer (and exfiltrator) of critical hint data we want to emphasise the importance of not restricting this capacity for other market participants.

116. We are only considering the application of **D&I D – User experience** where we are looking at a user-facing API and so have not reviewed UA-CH under this criterion.

- *IP Protection*

117. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we also include our provisional views on each of the concerns identified.

Potential concerns	**Provisional CMA views based on ICO's preliminary assessment**

[98] See Senol and Acar (2023) here (accessed on 22 April 2024).

Users must sign into their Google account to benefit from IP Protection.	We understand that the IP Protection proposal is still under development. If Google requires users to be signed-in to a Google Account to authenticate and thereby limit fraudulent behaviour, we are concerned that users will not be able to benefit from this Privacy Sandbox proposal without agreeing to wider terms and conditions associated with signing into a Google Account. This limits the overall benefit of the proposal.
The proposal requires Google to take account of: • defining and monitoring tracking activity; • authenticating users; • contracting a Content Delivery Network (CDN); and • managing and updating a block list.	Together with the ICO, we require further information to inform our view in four areas: monitoring tracking activity; the authentication of users; the relationship with the CDN; and the management of a block list.

118. As regards IP Protection, based on stakeholder feedback and our own analysis of the API, we have considered the following potential concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**. In the table below, we also include our updated views on each of the concerns identified based on further submissions from Google and other market participants since our last report was published in January 2024.

Potential concerns	CMA views in January 2024 report	Updated CMA views
Google may continue to benefit from user activity data while limiting competitors' access to the same data.	We may suggest that Google removes itself from the first 'hop' and use a second independent third-party instead. We will also need to understand whether data collected through sign-ins can be used in Google advertising and whether requiring user sign-in for IP Protection could be replaced by alternative means for user authentication.	Given the underlying technologies and design for IP Protection in its current state, we do not consider that there would be significant benefit in compelling Google to relinquish the first hop, especially as the design now requires a Google login to activate IP Protection. Furthermore, the requirement for a Google login will inevitably reduce uptake and, therefore, further reduce the overall footprint of IP Protection, mitigating both utility concerns (fewer Chrome browsers will engage IP Protection) and specific privacy concerns regarding an associated Google login. The design – if implemented as stated – will prevent Google from benefiting from the login requirement and their administration of the first hop and given IP Protection will not be fully deployed until well after third-party cookie deprecation, this primarily becomes a future governance issue.

Potential concerns	CMA views in January 2024 report	Updated CMA views
		However, we would welcome further consideration from both Google and the wider ecosystem of alternatives (for anti-abuse purposes) to the Google login requirement as the design continues to evolve in future.
Google's ability to control the inclusion of ad tech rivals on this list could advantage its ad tech services, especially if they are not subject to the same restrictions in the future.	Google will need to provide further detail on the governance process. We may suggest that independent third-party governance be required to ensure fairness and transparency.	We welcome further clarity from Google regarding future governance arrangements – especially regarding the final form, or source, of the tracker list.
Competition between providers of VPN services may be foreclosed.	This is beyond the scope of the Commitments but an issue that we will consider where appropriate.	Our view remains unchanged.
Publishers and advertisers that rely on IP addresses for geographically targeting and personalising content will be forced to offer a worse service.	The provisions for GeoIP within IP Protection proposals will allow ad tech and publishers to continue to optimise content to approximate geographic location. As with the Topics API, there may be no 'right' level of granularity for all market participants. We will need to consider loss of precision in targeting against privacy benefits.	Coarse GeoIP data will serve most use cases and, in any event, will only apply to those trackers on the final tracker list, in third party contexts and will only be functional for signed in users.
Publishers and advertisers may be less able to effectively identify fraudulent activity.	We will need further specifications from Google on how block lists or other options will be applied.	For other use cases such as anti-fraud or anti-spam, Google is offering other APIs such as PST and Shared Storage (SelectURL can be used to indicate trust level for the client, for example).
Google may provide insufficient notice for ad techs to implement alternative solutions with their publishers and test and comment back on proposals.	We will need Google to clarify and seek feedback on sufficient notice to be provided to ad techs to implement alternative solutions with their publishers and test and comment back on proposals.	A stakeholder has asked that Google provide a minimum notice period of 12 months to implement alternative solutions. We have not received feedback from Google on this specific suggestion.

119. As regards the application of **D&I D – User experience**, as the IP Protection proposal develops further, we will keep the relevant user experience under review to ensure users have adequate choice and control.

- *DNS-over-HTTPS, Storage Partitioning and Network Partitioning*

120. **DNS-over-HTTPS**, **Storage Partitioning** and **Network Partitioning** are closely aligned with implementations by other browsers with the common aim of improving online privacy. The ICO has not raised any concerns. At present, we do not have any concerns under any of the D&I Criteria regarding these APIs.

121. Furthermore, DNS-over-HTTPS will be removed from the list of proposals we are monitoring as it is not Privacy Sandbox specific. However, Google will keep us updated of any substantive design changes.

Summary

122. Google needs to resolve our concerns for UA-CH/UAR and IP Protection and our current view is that this could involve taking the following steps:

(a) As regards **UA-CH/UAR:**

(i) Provide more information to better understand what limits are placed on access to critical hints.

(ii) Provide assurances that it will not further remove or limit access to critical hints in the future, especially in light of the findings of the research paper presented above.

(b) As regards **IP Protection**:

(i) Ensure an adequate governance process to ensure fairness and transparency.

(ii) Provide specifications on how block lists or other options will be applied.

(iii) Need for sufficient notice to be provided to ad techs to implement alternative solutions with their publishers and test and comment back on proposals.

(iv) Provide more information on how the IP Protection proposals would affect user experience.

(v) Provide more information on monitoring tracking activity; the authentication of users; the relationship with the CDN; and the management of a block list.

Other updates covering the reporting period

Update on testing and trialling

123. Google launched in January 2024 a combined end-to-end experiment utilising 1% of traffic for which Chrome disabled third-party cookies as part of its Mode B testing initiative. Using Mode B traffic will ensure that third-party cookies are not used in auctions intended for testing the Privacy Sandbox tools. This test will seek to estimate the potential direction and scale of impacts on Google and the advertisers and publishers who rely on its advertising services.

124. Our wider evidence base will also include testing results from third-party market participants. We have engaged with a wide variety of market participants who have begun or submitted plans to run tests of the Privacy Sandbox tools during Q1 and Q2 2024.

125. As mentioned in our last update report, our assessment will not consider these testing results in isolation but alongside a wider evidence base. This will include evidence gathered from across the industry on how the Privacy Sandbox tools might affect their business operations. We are also asking third party testers to submit a range of quantitative and qualitative information with their results and will continue to engage with market participants on their testing plans.

126. We encourage market participants to conduct tests in line with our guidance.[99] The testing period will run to the end of Q2 (during which third party testers can submit results to the CMA).

127. One point that has been brought to our attention is that not all experimental traffic which DSPs are receiving from SSPs is labelled. Some DSPs have submitted that the share of experimental impressions which are unlabelled may be different across treatment and control groups. We encourage DSPs to assess whether this issue is affecting their experiments and to consider potential mitigations available within their experimental designs.

[99] See CMA's Guidance to third parties on testing dated 29 June 2023 and Additional CMA guidance to third parties on testing dated 26 October 2023.

128. For those ready, results can be submitted to privacysandbox@cma.gov.uk.

Actions and conclusions of the Monitoring Trustee

129. The Monitoring Trustee has not informed the CMA of any instances of Google being non-compliant with its obligations under the relevant paragraphs of the Commitments.

130. Although the Monitoring Trustee's quarterly report represents a snapshot in time, Google is subject to continuous monitoring for the duration of the Commitments. Therefore, monitoring activities may be reported on as in progress or otherwise in the process of discussion, negotiation, investigation, or consideration, with a future road map of monitoring work at any given time.

131. During the reporting period, the Monitoring Trustee has overseen Google's activities relating to paragraphs 25-27, 30-31, and 33 of the Commitments. These activities are largely a continuation of, and build upon, the work undertaken in the previous periods, including:

(a) Developing a deeper understanding of Google's internal data control systems in order to robustly test Google's proposals to address its commitments on Chrome browsing history, Google Analytics data, and ad inventory on websites not owned and operated by Google. These commitments only apply after Chrome ends support for third-party cookies, but we are working to ensure that these controls are fully implemented well in advance of third-party cookie deprecation. In the current reporting period, there was a particular technical focus on anti-abuse activities, as well as identified paragraph 26 data use instances.

(b) Continuing to review compliance artifacts around internal decision-making processes (e.g. logs and records) to test whether Google's internal processes are being followed in practice.

(c) Reviewing Google's proposals for new technologies and the risk that these could self-preference Google through their design, development or implementation. This has included scrutinising Google's Key Design Decisions to test their compliance with Section H of the Commitments. Select examples for the reporting period include engagement with Google regarding developments around Related Website Sets, trusted services within the PA API and ARA, and Bidding and Auction Services within the PA API.

(d) Engagement with Google regarding the API user attestation and enrolment process.

(e) Working to develop potential approaches and structures to support ongoing monitoring and compliance following third-party cookie deprecation.

132. As explained below, the Monitoring Trustee has been working closely with the Technical Expert, as well as with the CMA. Submissions (or extracts of submissions) from stakeholders which are relevant to multiple elements of the compliance regime are frequently shared between the CMA, Monitoring Trustee, and Technical Expert to ensure that they are fully addressed.

Technical Expert

133. As mentioned in previous update reports, the Technical Expert aims to support the Monitoring Trustee by providing the following skills which are vital for effective monitoring of the Commitments:

(a) Analysing Google's data access and flows;

(b) Analysing technical access controls and security; and

(c) Providing general ad tech expertise and advice.

134. We have also continued our direct dialogue with the Technical Expert. Discussions have focused primarily on market trends and issues concerning the design and implementation of Google's Privacy Sandbox proposals. We have taken account of views and comments from the Technical Expert in our ongoing discussions with Google on the design and proposed implementation of the Privacy Sandbox tools and in identifying the remaining potential concerns described in the section above.

Engagement with market participants

135. We are continuing to engage with market participants in the wider online advertising ecosystem to ensure that we become aware of, and understand, concerns about the Privacy Sandbox tools and their impact.

136. Our own stakeholder engagement is not intended as a substitute for market participants' direct interactions with Google, and we would encourage participants to raise substantive concerns through existing channels including W3C. Google is required under the Commitments to respond to reasonable views and suggestions, as summarised in Google's quarterly report which is published alongside this document. It is important that Google responds substantively to feedback, and we will highlight to Google where we do not consider that it has provided an adequate response and ensure that it does so.

137. Since the publication of the CMA's last report, in Q4 2023, our engagement has had a particular focus on encouraging and guiding industry testing, following the publication in October 2023 of our additional guidance note[100] to market participants considering testing.

138. We asked interested stakeholders their views on the issues set out in the last quarterly report. In total we heard from 25 stakeholders. Concerns raised through responses from these stakeholders were largely in areas that we were already aware of, but there were some new issues identified. Concerns raised throughout the stakeholder engagement process have been raised with Google in a confidential manner, and directly informed our role overseeing the design and implementation of its proposals.

139. Details of the concerns raised by market participants related to the specific APIs have been included in the relevant sections above. Other concerns raised have included the following:

Use of data

140. **Market participants have suggested that Google should clarify (a) the scope of data that will not be used, and (b) how and where this data is not going to be used, with respect to each of paragraphs 25, 26 and 27 of the Commitments.** We are aware that there are questions and concerns around Google's use of data. We have passed these comments to Google, and we are considering these as part of our work on first-party data. Google has said that it agrees that the scope of the data commitments is important and that it is engaging with the Monitoring Trustee and us with respect to the data covered by these commitments, and the technical mechanisms to ensure that, after Chrome ends support for third-party cookies, data will only be used in line with the requirements of the Commitments.

141. **The Chrome browser has access to many different types of data. Market participants have suggested that it would be helpful to have more clarity over:**

(a) **What Google means by 'browsing history…' as there is a commitment not to use personal data of this kind for targeting advertising. Clarifications would include the usage of browsing history tied to an authenticated Chrome user's account, the usage of**

[100] See CMA's Additional CMA guidance to third parties on testing dated 26 October 2023.

URL and content data, activity within sites, and any location tied to that history.

(b) **How and where data can move in Google pipelines to understand both the direct and indirect ways targeted advertising can or cannot benefit. For example, if Google were to draw inferences from its Chrome and Account Data for non-advertising purposes, and that then fed into targeting or other predictive models for advertising, this would negate some of the value of the Commitment.**

(c) As above, we have raised this with Google. Google has said that it has set up internal controls to guarantee that browsing history data cannot be used in contravention of the Commitments, directly and indirectly, for ads targeting and measurement purposes.

(d) **Google as an entity should be prevented from using a broader set of data than just browsing history, even if that is broadly defined, for targeting advertising purposes on their open web integrations. If Google is able to use account data, search history, YouTube history, Gmail etc, for targeted advertising across the web and are only restricted on URL usage from a browser bar, that will not be a meaningful restriction.**

(e) Google notes that under paragraph 27 of the Commitments, after Chrome ends support for third-party cookie, Google will not be allowed to use its first-party data to track users to target or measure ads shown on third-party websites across the web. However, Google is not prohibited from using its first-party data, except personal data from Chrome browsing history and from Google Analytics that customers have not shared or exported to other services for advertising purposes, for the targeting and measurement of ads shown on its O&O properties.

Timing

142. **Market participants have raised concerns over the lack of clarity on timelines for third-party cookie deprecation, and some have suggested that the Privacy Sandbox will not be in a position to be switched on in 2024. Market participants also raised concerns over the process for how cookies will be phased out, including that Google does not set out how third-party cookie deprecation will be scaled from 1% to 100%. They also note that a faster phaseout could have a greater revenue impact on smaller ad techs which may struggle to properly train machine learning models until third-party cookie deprecation extends beyond 1% and are**

more likely to need time to coordinate with others in the industry as compared to vertically integrated players like Google.

143. We have shared these concerns with Google. Given the time needed to resolve outstanding issues and take account of testing results, Google has said that it will not complete third-party cookie deprecation by the end of this year. Subject to resolving our remaining competition concerns, Google is now aiming to proceed with third-party cookie deprecation starting in early 2025. Under the Commitments, it is for Google to decide when the Standstill Period is triggered.

Fees

144. **Market participants have made the following comments about potential fees:**

145. **What fees (if any) will Google charge in connection with the Privacy Sandbox tools, including but not limited to fees associated with: (a) API access, (b) registration fees, (c) data fees, and/or (d) licensing fees? If Google does charge fees, what criteria is Google willing to commit to or at least share publicly with respect to making such determinations? How much prior advance warning will Google provide to the marketplace regarding any fees?**

146. We agree it is important that Google clarifies whether there will be any charges in relation to the Privacy Sandbox, and to provide transparency. We have raised this with Google.

Other

147. **Market participants have suggested that PETs such as Privacy Sandbox are seeming to go beyond basic legal requirements which set new ways of operating for the industry.**

148. We understand this to mean going beyond basic legal requirements relating to data protection. This is a concern we have heard before. Although Google is a company that can make its own decisions including how it approaches data protection, under the Commitments, Google is required to consider the D&I Criteria in designing, implementing and evaluating the Privacy Sandbox proposals. The D&I Criteria include impact on privacy outcomes and compliance with data protection principles, but it is one of five criteria, and other factors that will need to be considered include impact on competition in digital advertising, and impact on publishers and advertisers.

149. Google has said that while it has sought to ensure that the Privacy Sandbox APIs enable compliance with applicable legislation and has engaged with the ICO and us in their development, it does not consider the basic legal requirements to be a cap on what it can offer to the industry and to users. It is seeking to improve Chrome users' privacy while providing effective alternatives to third-party cookies, which in some circumstances includes improvements to user privacy beyond what may be legally required of Google or those using the technologies.

150. **Market participants have suggested that companies are concerned over the lack of viable alternatives to the Privacy Sandbox.** As mentioned in the competition concerns section of the report, we appreciate that Google's market position allows it to have a significant impact on the viability of alternative technologies that may compete with the Privacy Sandbox tools following the removal of third-party cookies, so we are continuing to engage with Google on this issue.

151. **Market participants have suggested that a lack of interoperability means publishers will need to adjust their content to suit the unique framework and technical requirements of each platform on which it is distributed.** As noted in this report, Google is required to consider the D&I Criteria in designing, implementing and evaluating the Privacy Sandbox proposals. D&I C looks at the impact on publishers and advertisers. We have shared this concern with Google.

152. **Market participants have suggested that input received by the CMA and Google until now has largely come from outcome-based performance vendors, and so the use case for self-service DSPs is not being considered. In their view, this means it is degraded at best which could lead advertisers to move spend to platforms where granular reporting is available post third-party cookies, such as Google O&O inventory**. We appreciate the need for a wide range of use cases to be considered and raised this concern with Google. Google has said that there are multiple self-service DSPs who regularly provide public feedback on the APIs and that Chrome is actively engaging on typical self-service DSP topics like video and third-party ad servers.

153. **Market participants have requested that Google retains dynamic link decoration following third-party cookie deprecation.** This is not in scope of Google's Commitments and our assessment, but we have raised this comment with Google.

154. **Market participants have suggested that third-party cookie deprecation on mobile devices should not happen before full interoperability**

between web and app is achieved. We have raised this comment with Google. In response, Google has agreed that it is desirable to support app and web interoperability and noted that it has launched cross app and web attribution measurement and is exploring web-to-app targeting solutions.

155. However, Google has said that it is not planning to delay third-party cookie deprecation on mobile web, and it does not have a goal of 100% coverage at the end of third-party cookie deprecation. Rather, it expects compatibility on Android for cross app and web measurement to be reasonably high at third-party cookie deprecation and to increase over time as users update their phones.

156. **Market participants have suggested that Google should make its guidance on experimentation clearer to support stakeholders with testing. In their view, developer guidelines do not have clear instructions on how testing would be performed at scale for reliable A/B testing.**

157. Testing is an important part of the process to inform decisions around the Privacy Sandbox. We have published guidance for ad techs, publishers, ad advertisers on how they can test the APIs in a way that would contribute to our assessment of the Privacy Sandbox tools, which we recommend stakeholders consult in the first instance in case of doubts about testing.[101] We appreciate the work stakeholders are doing to provide test results. We are aware that some stakeholders have had questions about experimentation and wanted more clarity on the guidance. We consider this to be important and have raised this with Google.

158. **In addition, several stakeholders have alleged specific breaches of Google's Commitments:**

(a) It has been alleged that Google is in breach of the Commitments in particular section D (Transparency and consultation with third parties) and Section H (Non-discrimination). It has been claimed that Google is self-preferencing its advertising products and services, and using competitively sensitive information provided by an ad tech provider or publisher to Chrome for a purpose other than that for which it was provided.

[101] See footnote 99.

(b) While we do not consider that there has been any ‘breach’ of provisions in sections D and H of the Commitments, we have raised the substance of the concerns with Google under paragraph 17.a.ii. of the Commitments, where appropriate.

(c) It has been alleged that, in relation to the classification based on host names under Topics API, Google impairs its rivals’ ability to monetise their ad inventory in competition with Google’s O&O ad inventory. It has been alleged that, if Google’s designs restrict rivals from interoperating and competing with its ad systems offered to rival media owners to monetise their ad inventory or common advertiser prospects for such digital advertising solutions, the combination of this interference with the impaired effectiveness of Google’s proprietary API ad systems violates both the spirit and the letter of Google’s commitments, particularly paragraph 30.

159. While we do not consider that there has been any ‘breach’ of provisions in the Commitments, including paragraph 30, we have raised the substance of the concerns with Google under paragraph 17.a.ii. of the Commitments, where appropriate.

160. In relation to ARA, it has been alleged that by reducing to 3 bit storage and adding ‘fake data’ of the results rivals’ systems receive, Google’s design only degrades rivals’ ad solutions but not the optimisation of matching paid content across its O&O properties’ ad inventory. It has been alleged that this would shift spend from across the open web towards the largest online publishers—such as Google’s O&O properties – and that this ‘discriminatory design’ would seem to violate both the spirit and the letter of Google’s commitments, particularly paragraph 30.

161. As regards to the alleged violation of paragraph 30 of the Commitments, it is not clear to us how such a violation arises where the functionality available to Google through the ARA is the same as for third parties.

162. A further submission put forward information on alleged preferential treatment of Google [via Chromium], which it has been claimed is in breach of the Commitments.

163. We have already raised the substance of these concerns with Google under paragraph 17.a.ii. of the Commitments, where appropriate.

IAB Tech Lab – Privacy Sandbox Fit Gap Analysis for Digital Advertising

164. The report from IAB Tech Lab's Privacy Sandbox taskforce provides useful insights. Google has published its own response to the report.[102]

165. Within the report, IAB Tech Lab raises a number of concerns regarding the different aspects of the Privacy Sandbox. Several stakeholders reiterated concerns raised by IAB Tech Lab in responses made to our last quarterly report. There are certain concerns raised, such as around governance, that we are actively considering and are currently in communication with Google about.

166. In Google's response to the IAB Tech Lab report, it notes that it largely focused on the technical assessment, and that it plans to engage the ecosystem and update its public FAQs in relation to other questions and concerns raised, such as around fragmented documentation, commercial requirements, third-party audits, industry accreditation, scalability, transparency and future governance. We consider that clarity over these questions is important. We welcome Google's plan to update its public information and have followed up with Google to understand its progress on this.

167. Google has said that it has provided updates on several of these areas. It has addressed:

(a) Fragmented documentation by updating the navigation of the developer pages of the Privacy Sandbox to be use case focused, using similar categorisations to the IAB Tech Lab in its recent Privacy Sandbox Task Force report.[103] Google plans to use this use case-based approach to documentation going forward.

(b) Commercial requirements under the 'Data Guarantees' section of the above Google response to the IAB report,[104] and some Google Ads products have shared their approaches as set out in the FAQ for Ad Manager and Privacy Sandbox.[105]

[102] See Google's response to the IAB Tech Lab's report here (accessed on 22 April 2024).

[103] See the developer pages of the Privacy Sandbox here (accessed on 22 April 2024)

[104] See the 'Data Guarantees' heading in Google's response to the IAB Tech Lab's report here (accessed on 22 April 2024).

[105] See the FAQ for Ad Manager and Privacy Sandbox here (accessed 22 April 2024).

(c) Third-party audits under the ‘Algorithm Integrity Guarantee’ section of the above Google response to the IAB report.[106]

(d) Regarding accreditation Google would expect those bodies to continue accrediting products, including their use of technologies, rather than the technologies by themselves.

(e) Regarding scalability, Google has said that it continues to be open to data from developers that demonstrates issues.

(f) Regarding transparency and governance, Google has said that it continues developing in the open on GitHub and at forums like W3C while engaging with the CMA under the Commitments.

Stakeholder engagement

168. Our focus for stakeholder engagement over the next quarter will be on guiding ongoing industry testing of the Privacy Sandbox APIs and working with Google to resolve outstanding concerns.

169. Given the global nature of Google’s developments, we welcome feedback from organisations both within and outside the UK.

Engagement with the ICO and international authorities

170. We have continued to work together closely with the ICO in implementing the Commitments. The ICO’s role has included:

(a) Participating in discussions with us and Google on the development of the Privacy Sandbox tools, analysing data protection impacts with a specific emphasis on user controls and assessing compliance with data protection legislation;

(b) Engaging directly with Google on these issues by holding separate meetings which we have also attended;

(c) Continuing to work with us on plans for the wider assessment of the Privacy Sandbox tools, including assessing privacy impacts; and

[106] See the ‘Algorithm Integrity Guarantee’ Google’s response to the IAB Tech Lab’s report here (accessed on 22 April 2024).

(d) Engaging with market participants on proposed alternative technologies to third-party cookies and similar advertising technologies.

171. We have also continued to engage with our international counterparts and data protection authorities on the implementation of the Commitments in an effort to identify any issues of common concern and ensure consistency of approach.

Next steps

172. Over the next three months, we will focus on working with Google to resolve the concerns we have identified in this report ahead of the Standstill Period.

173. We are planning to publish our next update report and Google's progress report in July 2024.

Contact details

174. We would welcome views from interested parties on this report, as well as on any other relevant publications (e.g. Google's own quarterly report). The relevant contact details are:

CMA: privacysandbox@cma.gov.uk; adam.gayton@cma.gov.uk; angela.nissyrios@cma.gov.uk; and chris.jenkins@cma.gov.uk.

Monitoring Trustee (including communications for the Technical Expert): trustee.services@ing.com; matthew.hancox@ing.com; and david.verroken@ing.com.

Google: Feedback - Chrome Developers.

Annex 1 – current proposals in the Privacy Sandbox

1. At the time of publication, the list of proposals in the Privacy Sandbox include the following arranged by use case:

Use Case: Showing relevant content and ads

2. Currently, third-party cookies 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.

3. Google has developed two proposals to enable ads targeting and retargeting respectively without third-party cross-site tracking.

   (a) Topics

   (b) Protected Audience

Use Case: Measuring digital ads

4. Cross-site tracking may also be 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.

5. Google has developed the following measurement and reporting tool that does not rely on third-party cookies:

   (a) Attribution Reporting

Use Case: Strengthen cross-site privacy boundaries

6. Google has developed a proposal for companies to declare relationships among sites, so that browsers allow limited third-party cookies access for specific non-ads purposes such as facilitating a user-journey across several sites:

   (a) Related Website Sets

7. Another tool allows users to log into particular sites without sharing their personal information with those sites:

   (a) Federated Credential Management

8. A range of other boundary APIs have been developed:

   (a) Related Website Sets

   (b) Shared Storage

   (c) CHIPS

   (d) Fenced Frames

Use Case: Fighting spam and fraud on the web

9. 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.

10. Google has developed a new API to enable trust in a user’s authenticity to be conveyed from one context to another, to help sites combat spam and fraud, without passive tracking:

   (a) Private State Tokens

Use Case: Limiting covert tracking

11. Other 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. A further example is the IP address, which is useful for detecting fraud and the geographical tailoring of content.

   Google has developed a range of proposals aimed at limiting covert tracking without breaking currently supported use cases:

   (a) Bounce Tracking Mitigations

   (b) User Agent Reduction (including User-Agent Client Hints)

   (c) Storage Partitioning

(d) Network State Partitioning

(e) IP Protection (previously Gnatcatcher)

Annex 2 – context and framework of our assessment

12. We have summarised below the framework for our assessment as set out in Google's Commitments.

The Commitments framework

13. The Purpose of the Commitments is to address the competition concerns we identified during our Competition Act 1998 (**CA98**) investigation, namely that, without sufficient regulatory scrutiny and oversight, the Privacy Sandbox proposals could: [107]

    (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 O&O ad inventory; and

    (c) allow Google to deny Chrome web users substantial choice in terms of whether and how their Personal Data is used for the purpose of targeting or measurement and delivering advertising to them.

14. The Commitments state that Google will design, implement and evaluate the Privacy Sandbox proposals by taking into account the following factors (the D&I Criteria), which will inform the answer to the question of whether or not the Purpose of the Commitments, as defined above, has been achieved. The D&I Criteria are:[108]

    (a) impact on privacy outcomes and compliance with data protection principles as set out in the Applicable Data Protection Legislation (**D&I A – Privacy outcomes**);

    (b) impact on competition in digital advertising and in particular the risk of distortion to competition between Google and other market participants (**D&I B – Digital advertising**);

[107] See paragraph 7 of the Commitments.

[108] See paragraph 8 of the Commitments.

(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&I C – Impact on publishers and advertisers**);

(d) impact on user experience, including the relevance of advertising, transparency over how Personal Data is used for advertising purposes, and user control (**D&I D – User experience**); and

(e) technical feasibility, complexity and cost involved in Google designing, developing and implementing the Privacy Sandbox (**D&I E – Technical feasibility for Google**).

15. Under the Commitments, Google will work with us without delay to seek to resolve concerns raised and address comments we made with a view to achieving the Purpose of the Commitments.[109] Google will inform us of how it has responded to those comments. In practice, this means that Google will take action or provide the CMA with assurances on the actions it will take (or refrain from) to resolve any remaining concerns.

16. In the event that we cannot reach mutual agreement or resolve concerns within 20 working days of written notice by the CMA (unless extended by mutual consent), we may take action, including by reopening the CA98 case.[110] We have not served any such notice to date.

17. The Commitments also require that 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 such removal.[111] 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.

18. During the Standstill Period, we may notify Google that competition law concerns remain such that the Purpose of the Commitments will not be achieved.[112] Google will work with us 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 us of how it

[109] See paragraph 17.a.ii of the Commitments.

[110] Pursuant and subject to the provisions of section 31B(4) CA98. See paragraph 17.a.iii of the Commitments.

[111] See paragraph 19 of the Commitments.

[112] See paragraph 21 of the Commitments.

has responded to those comments. In practice, this means that Google will take action or provide the CMA with assurances on the actions it will take (or refrain from) to resolve any remaining concerns.

19. As part of the Commitments to the CMA, we will monitor Google's compliance with those assurances following deprecation of third-party cookies.

20. If Google fails to comply with the Commitments, including any of the assurances provided to us, the CMA may continue its investigation under section 31B(4)(b) CA98 or apply to the court for an order under section 31E CA98. In the event of a material change of circumstances, the CMA also may continue its investigation under section 31B(4)(a) CA98. Where the CMA continues an investigation under section 31B(4) CA98, the CMA's powers to impose interim measures and/or to make an infringement decision become available to the CMA again.

21. Accordingly, if Google fails to respond to our concerns or does not provide the required assurances, we could oppose the removal of third-party cookies – in which case we would expect to continue (reopen) the CA98 investigation if Google stated that it would push ahead with third-party cookie deprecation.

Proposed approach during the Standstill Period

22. Once Google triggers the Standstill Period, we expect to assess the evidence from the testing and trialling results, along with our own analysis of the potential impact of the Privacy Sandbox changes, informed by stakeholder responses.

23. In making this assessment, we recognise that the Privacy Sandbox represents a significant change for the entire ad tech ecosystem, and that the ecosystem will experience significant impacts – for example, impacts on revenue, on the cost of advertising, or on business practices due to changes in measurement and reporting. We expect the Chrome-facilitated testing period (which will run from Q1 to Q2 2024) to provide data on the direction (i.e. positive or negative) and potentially the scale of impacts on publishers and advertisers in particular.

24. We will consider any impacts (e.g. revenue loss) in the overall context of the Privacy Sandbox changes, including the potential to deliver benefits to consumers. The Commitments do not require that there be no loss of revenue to publishers and advertisers from the deprecation of third-party cookies and their replacement with the Privacy Sandbox tools. However, the Commitments require that Privacy Sandbox is implemented in a way which does not infringe competition law and minimises the impact on revenue to the extent possible,

while also considering privacy impacts and the legitimate aim of compliance with data protection principles as set out in the Applicable Data Protection Legislation through reducing cross-site tracking.

25. The scale and direction of impacts on the ecosystem could change over time, as ad techs optimise their systems, retrain machine learning models using signals from Privacy Sandbox APIs and new Privacy Sandbox functionality becomes available. Our stakeholder engagement on specific challenges, like latency concerns around Protected Audience auctions on-device, suggests that some stakeholders are optimistic that they can iteratively improve over time. Our assessment will consider the scale and direction of impacts alongside any evidence on potential improvements (or degradations) that might occur.

26. Similarly, some existing ad tech business models will be disrupted where they currently rely on cross-site tracking technologies, including third-party cookies. The purpose of the Commitments is not to support specific business models. In assessing the Privacy Sandbox changes our focus will be on the likely impacts for competition and consumers overall.

Engagement with the ICO

27. To support and inform the CMA's assessment, the ICO has focused on **D&I A – Privacy outcomes** and, where relevant, **D&I D – User experience**. These criteria, together with the ICO's direct scrutiny of Google's compliance with data protection principles as set out in the Applicable Data Protection Legislation, provide the mechanism by which the ICO is examining the APIs, supporting our analysis to determine whether the Privacy Sandbox delivers positive privacy outcomes and choice for individuals.

28. In our Commitments Decision, we cited the ICO's Opinion on data protection and privacy expectations for online advertising proposals dated 25 November 2021[113] as a resource that provides additional regulatory clarity on the data protection expectations that online advertising proposals should meet. Accordingly, when assessing **D&I A – Privacy outcomes** and **D&I D – User experience**, the ICO has drawn upon its 2021 Opinion, particularly section 5 which sets out the Commissioner's expectations. These principles and recommendations for ad tech market participants developing new solutions provide a framework to ensure that the interests, rights and freedoms of

[113] See the 2021 Opinion.

individuals are respected.[114] This framework is rooted in the Applicable Data Protection Legislation.[115] These principles and recommendations remain applicable and in the context of the Commitments the ICO has used them to consider Google's Privacy Sandbox proposals.

29. As well as considering future developments, the ICO's 2021 Opinion also built on the ICO's update report into ad tech and real time bidding dated 20 June 2019 (together, the **2019 and 2021 Publications**).[116] Both in its 2019 and 2021 Publications, the ICO sets out expectations that the ad tech industry addresses a range of issues. [117] As stated at the time, these data protection issues relate to several types of harm that organisation needed to consider as part of a risk-based approach to data protection. The ICO's expectations have not changed: where new online advertising products are proposed, they must address the issues it identified in the 2019 and 2021 Publications and mitigate any new or different risks and harms they involve in order to comply with data protection principles and the UK data protection law. In summary, when considering the Privacy Sandbox against D&I A and D, its previous work and identified systemic issues have been front of mind for the ICO.

30. Coming to a position on how effectively Google has taken into account **D&I A – Privacy outcomes** requires the ICO to sets out a view on the impact of the Privacy Sandbox on privacy outcomes.

31. The ICO's position on possible privacy benefits is, again, informed by its assessment of the compliance with Applicable Data Protection Legislation using the approach set out in its 2019 and 2021 Publications. The ICO's 2021 Opinion, in particular, sets out the requirements for the industry to address a range of data protection concerns that it continues to observe after identifying them in the ICO's 2019 Report.[118] As stated at the time, the ICO sets out expectations that 'new proposals for enabling online advertising must address the issues and harms highlighted [in the 2019 Report]'. [119] The ICO's evaluation of the Privacy Sandbox tools, and their possible benefits, is based

[114] See paragraphs 43-46 of the 2021 Opinion.

[115] See page 2 of the Commitments. 'Applicable Data Protection Legislation' is defined to mean all applicable data protection and privacy legislation in force in the UK, including the Data Protection Act 2018, the UK General Data Protection Regulation (**GDPR**) (and regulations made thereunder) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**).

[116] See the 2019 Report.

[117] See paragraphs 16-17 of the 2021 Opinion.

[118] See page 16 of the 2021 Opinion.

[119] See page 19 of the 2021 Opinion.

on the risk and likelihood of these previously identified concerns being replicated in a post-Sandbox ecosystem.

32. As set out in the ICO's 2021 Opinion, the ICO has noted that both PECR and data protection law are technology neutral. [120] It continues to be the ICO's view that concerns highlighted in its 2021 Opinion were predominantly the result of industry practices and not the underlying technologies. [121] Accordingly, where the ICO has identified a possible concern, its current view is also informed by the risk and likelihood of misuse by third parties using the Privacy Sandbox tools based on information available and its historic observations about potential data protection law non-compliance issues in the ad tech ecosystem.

33. Under the Applicable Data Protection Legislation, the principle of accountability ensures that those responsible for the processing of personal data are able to demonstrate how they are complying with their obligations. Taking a data protection by design approach to governance and accountability at the outset will assist Google and the parties using the Privacy Sandbox APIs to comply with their data protection obligations more easily and to demonstrate this to data subjects and regulators.

[120] See page 20 of the 2021 Opinion.

[121] While maintaining its position regarding technology neutrality, it is also the ICO's view that the characteristics of a technology can contribute towards the ease by which websites and third parties are able to comply with data protection legislation.