CMA update report on implementation of the Privacy Sandbox commitments

November 2024

CONTENTS

Summary

1. This report sets out the CMA's current assessment of the issues we have identified in our previous update reports, including the April 2024 report, concerning Google's proposed Privacy Sandbox tools (see **Appendix 1**). Our analysis is based on the framework for assessment set out in the Commitments that the CMA accepted from Google in February 2022.

2. Since we published our quarterly report in April 2024, Google announced[1] that instead of deprecating (or removing) third-party cookies, it plans to give users a choice on whether to allow or limit third-party cookies. While we were considering Google's revised approach to the Privacy Sandbox, we did not publish our last quarterly update report. We invited views on Google's revised approach and provide a summary of the views we received in the sections below. Our view is that the current Commitments need to be updated to reflect Google's revised approach. We are discussing with Google the implications of the revised approach for our competition concerns, and the changes that are required to address them.

3. In the interim, this report sets out progress that has been made in resolving our issues relating to the individual Privacy Sandbox tools and our current views based on the existing Commitments framework. Google has an ongoing obligation not to design or implement the new Privacy Sandbox tools in a way which discriminates in favour of its advertising businesses.

4. In the sections below, we outline Google's responses to the concerns we identified in our previous reports and the steps it has taken to resolve issues. We also include feedback received from market participants on these points. This report incorporates feedback from the Information Commissioner's Office (**ICO**) on the privacy and data protection impacts of the Privacy Sandbox. The ICO has been closely involved in this process, given that the aim is to ensure that both competition and privacy are protected.

5. Many issues identified about the Privacy Sandbox tools in our previous reports are resolved in a number of areas. Resolved issues, and issues that fall outside the scope of the CMA's investigation, are included in **Appendix 2**. Other issues highlighted in the sections below may be resolved through Google's proposed improvements to its governance framework, once finalised and provided it is implemented effectively. The key elements of the proposed governance framework are set out in paragraph 14 of this report.

---

[1] The Privacy Sandbox Blog, 'A New Path for Privacy on the Web', 22 July 2024 (accessed on 10 November 2024).

6. In some areas, there continues to be a risk that parties and Google may use the Privacy Sandbox tools in a way that is not in compliance with Applicable Data Protection Legislation leading to ongoing risks for privacy outcomes. In most cases concerning compliance with this legislation, the responsibility lies with the parties using the Privacy Sandbox tools. Resolving these risks of noncompliance by parties through technical changes to the Privacy Sandbox tools has had to be balanced against the potential for distortions to competition arising from Google's plans with respect to the availability of third-party cookies in the Chrome browser.

7. The ICO will monitor how the industry responds to Google's revised approach to Privacy Sandbox and retains its independence to take regulatory action against all parties where non-compliance is identified, including by Google and organisations that use the Privacy Sandbox tools.[2]

8. Based on the available evidence, we consider that in the period since our last update report (1 April 2024 to 30 September 2024), Google has complied with the existing Commitments.[3] 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 concerns relating to the development and implementation of the Privacy Sandbox tools.

[2] See ICO statement in response to Google announcing it will no longer block third party cookies in Chrome (Accessed on 10 November 2024).
[3] During the reporting period, the Monitoring Trustee has overseen Google's activities relating to paragraphs 25-27, 30-31, and 33 of the Commitments. The Monitoring Trustee has not informed the CMA of any instances of Google being non-compliant with its obligations under those paragraphs of the Commitments. We have also continued our direct dialogue with the Technical Expert.

Context and framework of our assessment

9. This document sets out our current assessment of the proposed Privacy Sandbox changes, updating the assessment we published in April 2024. The framework for our assessment is based on the Development and Implementation (**D&I**) criteria set out in the existing Commitments.[4]

10. Google's proposal to replace third-party cookie deprecation with a new user choice experience is likely to change the scale of the impact on the ad tech ecosystem in relation to the issues we describe in this report, because third-party cookies will continue to be available for some users depending on their choice. However, for the proportion of traffic where third-party cookies are unavailable, the Privacy Sandbox tools will remain important for the ad tech ecosystem to target and measure advertising.

11. We have consulted the ICO on aspects of the Privacy Sandbox relating to privacy and data protection.[5] The ICO has continued to share its feedback on elements of the Privacy Sandbox with respect to the impact of proposals on privacy outcomes and compliance with data protection principles as set out in Applicable Data Protection Legislation. The issues listed in the section below include the ICO's input primarily in relation to D&I A (privacy impacts) and D&I D (user experience) of the existing Commitments. Where the ICO has identified a possible issue with Google's current proposals, its view is also informed by the risk and likelihood of misuse (ie using the Privacy Sandbox tools in ways that create risks for privacy outcomes and compliance with data protection principles as set out in Applicable Data Protection Legislation) by parties, such as publishers, advertisers and ad techs.[6]

12. Our assessment of the individual Privacy Sandbox tools highlights several areas where we consider issues to be resolved while noting that the risk of misuse by parties may persist.[7] In most cases, we consider that the primary responsibility for mitigating these risks rests with the parties using the Privacy Sandbox tools.

Google's proposed governance framework for the Privacy Sandbox tools

13. In previous reports, we have set out our view that Google's discretion over how the Privacy Sandbox works, develops over time and the conditions for

---

[4] See the Commitments, paragraph 8.
[5] See the Commitments, paragraph 18.
[6] For more information on the ICO's approach to reviewing the Privacy Sandbox tools, see the CMA's Q1 2024 update report, Annex 2, paragraph 32.
[7] Issues we consider to be resolved have been included in Appendix 2 of this report.

using the Privacy Sandbox (eg requiring attestations) could create a risk of self-preferencing or the perception of self-preferencing.[8] To mitigate this risk, Google has put in place a framework governing the development and implementation of the Privacy Sandbox. We are working with Google and the ICO as Google continues to develop proposed improvements to its governance framework.

14. At the time of this report, the proposed improvements to the governance framework includes the following elements:

(a) **Introducing a formal consultation period for strategic decisions (being decisions relating to roadmap changes for a specific Privacy Sandbox tool, with a significant privacy or utility impact and which will be deployed in general availability)**. The formal consultation will include Google providing details on the proposed decision, an assessment of the impact on the D&I criteria in the applicable Commitments, a defined period for market participants to provide feedback (the current proposal is three weeks) and a published record of the decision including a summary of feedback and other input. This formal consultation process would operate in addition to existing 'development in the open' practices (eg engaging with stakeholders via GitHub issues), and to existing reporting on key decisions to the Monitoring Trustee.

(b) **Introducing an externally managed appeals process to which parties can appeal certain operational decisions, ie binary decisions which Google makes based on pre-defined criteria, that are addressed specifically to their business**. Examples of operational decisions of this type could include decisions to reject a developer's Related Website Sets (**RWS**) set declaration in the canonical RWS list and decisions relating to attestation and enrolment. We consider that an external appeals process could mitigate risks arising from Google's decision-making power.

(c) **Codifying privacy and utility principles, expanding on the D&I criteria**. Google proposes to add detail to clarify its approach to assessing each of the D&I criteria. We consider that codifying privacy and utility principles would be helpful in balancing privacy and utility considerations, including in the context of the formal consultation process described in (a) above. However, a Google-led codification of these principles could create risks of self-preferencing or the perception of self-preferencing (eg giving Google significant leeway in interpreting the D&I criteria), and we are working with Google to avoid such risks as it drafts these principles.

---

[8] See the CMA's Q1 2024 update report, paragraph 14(b).

(d) **Introducing a new annual reporting mechanism to the CMA and the ICO on risks to privacy from cross-site tracking under the Privacy Sandbox in Chrome**. Our understanding is that this reporting will include, where available, feedback from stakeholders (eg privacy regulators, data subjects, researchers) and technical metrics, where possible, providing insight on how the ad tech ecosystem is using the Privacy Sandbox tools. Google proposes that this cross-site tracking risk report could feed into its decisions on design changes, where relevant to mitigate risks.

15. As we explain in more detail in the section below and **Appendix 2**, our view is that Google's proposed governance framework could resolve a range of outstanding issues once finalised and provided it is implemented effectively. Until Google has done so, these issues will remain unresolved.

Potential concerns and current views on the individual Privacy Sandbox tools

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

17. We outline the concerns we have identified for each of the tools and APIs based on the Commitments framework (**D&I A – Privacy outcomes**, **D&I B – Digital advertising**, **D&I C – Impact on publishers and advertisers** and **D&I D – User experience**). The sections below include outstanding issues, with resolved issues listed in **Appendix 2**.

Showing relevant content and ads

Topics API

Overview

18. The Topics API is intended to enable interest-based targeting.[9] 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.[10]

[9] For an overview of the Topics proposal, see 'Topics' on The Privacy Sandbox (accessed on 10 November 2024).
[10] For the Topics taxonomy, see the 'Topics' repository on GitHub (accessed on 10 November 2024).

Human curation is intended to ensure that topics are interpretable, for example 'Arts & Entertainment', and that sensitive topics are excluded.

19. The on-device classifier uses the site's hostname, including subdomains. For example, sport.site.com may be classified under 'sport' but site.com/sport will only have the topics allocated to site.com. Google has published further details on the classifier model and the 'override list' which includes manual classifications for the top 50,000 domains.[11]

20. 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.[12]

Assessment

21. 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 assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
Google does not provide sufficient clarity to individuals regarding how their data is used by the Topics API.	See D&I D below	See D&I D below
The enrolment process does not effectively segregate API callers where multiple registrations are made for a single entity.	No reporting within this reporting period.	Key controls and privacy boundaries within the Topics API proposal rely on the effective segregation of API callers (ie parties using the API) enabled via the wider Privacy Sandbox enrolment process (equivalent boundaries

[11] See Chrome Developer guidance, 'The classifier model', 25 January 2022 (accessed 10 November 2024).
[12] See Chrome Developer Blog on 'Enhancements to the Topics API', 8 November 2023 (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
		are similarly maintained by the enrolment process in wider APIs such as ARA, PA API and Shared Storage API; however, for brevity a single issue is recorded here against Topics API). Given the central importance of these boundaries, if API callers are not effectively segregated, there is a risk of cooperation that can subvert the purposes and privacy controls of the APIs. Currently, we understand that Google's enrolment process allows multiple enrolments from a single entity (where, for example, sufficiently separate products may have a legitimate reason to independently access an API). We observe that Google acknowledges this risk and requires entities to undertake an additional review via a Multi Enrolment Request Process. This process, we understand, is designed to ensure that multiple enrolments from the same entity are justified and, therefore, help maintain key API controls (for example, in the case of Topics API, this would help maintain reidentification risk controls that limit the total amount of topics revealed to a single entity for each three-week epoch period). Based on discussions with Google and review of the published list of enrolments, we are concerned that segregation of enrolments is not sufficiently robust to deliver the reduction in risk anticipated where API callers' cooperation could subvert the purposes of the APIs. We have raised this concern with Google and are awaiting further details of the proposed governance process to understand how this risk might be monitored.

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
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'.[13] The taxonomy is a key variable when assessing privacy risk associated with the Topics API. 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.	Our discussions with Google on governance confirm that significant changes to the taxonomy, that would impact privacy or utility, would be subject to the formal consultation period described in paragraph 14 on governance above. Therefore, subject to the governance framework working effectively, this issue could be resolved. The formal consultation process could provide assurance that the D&I criteria, including impacts on privacy, will be considered if any future changes are made to the Topics API taxonomy.

22. 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

[13] See the 2021 Opinion, page 44.

table below, we also include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024.

Potential concerns	**The CMA's views in the April 2024 report**	**The CMA's assessment**
Google will be less reliant on the Topics API than other market participants, given its access to first-party data.	Sections G and H of the Commitments already impose some 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.	We are continuing to discuss this issue with Google.
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.	Stakeholders have expressed concerns that low user consent rates on the Topics API may affect its utility and result in adverse impacts on publisher revenue. We recognise that Google needs to request user consent for the Topics API to operate. We have engaged with Google about the user choice and controls for the Topics API to ensure that users can make effective choices. We anticipate that the Chrome-facilitated testing period in early 2024 will provide further information about Topics availability.	Google has informed us that it designed the Topics API user experience (UX) to provide transparent information about the processing which occurs when the API is switched on, and to enable users to make an informed and freely given choice as to whether to consent. Recently, Google announced the release of additional controls for the Topics API, giving users greater control over which topics are associated with them. Our discussions with Google regarding UX are ongoing. Provided that Google is taking appropriate steps to enable users to make effective choices when interacting with the Topics API (described in more detail under D&I D below), then we consider this issue could be resolved. Regarding the risk that low consent rates may adversely affect publisher revenue, we consider that some of the impact can be alleviated using additional signals such as the context of a page.
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	Our discussions with Google on governance confirm that significant changes to the taxonomy, that would impact

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	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. 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 Google's governance proposal will consider whether it will adequately mitigate the risks to user privacy that may occur as a result of changes to 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.	privacy or utility, would be subject to the formal consultation period described in paragraph 14 on governance above. The formal consultation process outlined by the framework provides assurance that Google will consider stakeholder feedback and balance the range of D&I criteria in decisions relating to the taxonomy. Therefore, subject to the governance framework working effectively, and Google seeking to make this type of change, this issue could be resolved.
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 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	As above, subject to the governance framework working effectively, this issue could be resolved. Moreover, Google's decision to implement its revised approach to Privacy Sandbox means that there will be a proportion of traffic choosing to retain third-party cookies. This may have implications for ad techs, who can continue to rely on third-party cookies to leverage their first-party data.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	A assessment of the Topics API above, any utility-focussed changes to the taxonomy will need to be accompanied by compensating privacy controls.	
Topics API will be difficult to test until it is stable and fully implemented in Chrome.	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.	Our view is that Google's governance framework described in paragraph 14 above, if applied effectively, could resolve stakeholder concerns around changes to the Topics taxonomy. Google intends to continue to develop Privacy Sandbox in a collaborative manner (eg with public discussions and using the Blink dev mailing list) and proposes to implement a formal consultation period for major changes that significantly impact privacy or utility. Google has confirmed that changes of this type to the Topics taxonomy would be subject to formal consultation under the proposed governance framework.
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.[14] 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 continuing to discuss this issue with Google.

[14] See Google's Q4 2022 progress report, page 34 (accessed on 10 November 2024).

23. We have consulted with the ICO regarding the application of **D&I D – User experience** and set out our assessment in the table below. The CMA's assessment below includes the ICO's feedback.

Potential concerns	**The CMA's assessment including the ICO's feedback**
Google does not provide sufficient clarity to individuals regarding how their data is used by the Topics API.	We raised a concern that the Topics API consent user interface (UI) 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 (eg as determined by API callers). To address this issue, Google 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. Furthermore, in May 2024, Google provided an update on changes it is making to its Privacy Sandbox Privacy-related Compliance FAQs. Relevant to addressing the CMA's concern, these updates provide guidance to API callers regarding their requirement to clearly communicate how data processed via the Topics API will be used, with particular reference to purposes beyond ad-related purposes. In this reporting period, together with the ICO we continued to engage with Google to provide feedback on the Topics consent UI. Google has developed updated screens in response to the feedback. Before rolling out these changes, Google shared the results of an online UX study, which showed a significant improvement in overall comprehension rates among users exposed to the updated screens compared to the current screen designs. While user comprehension was observed to be low for a minority of questions used to test users, the overall comprehension scores show users making informed choices about the Topics API, based on Google's opinion on how Topics data is supposed to be used. One remaining issue is that Google does not plan to add all the information which was featured in the updated Topics consent UI to its Privacy Guide for users. This missing information would help users to make informed decisions regarding their privacy once their initial interaction with the consent interface is complete. We recommend that Google also adds to the Privacy Guide the detail in the Topics API consent UI. If Google implements this change, this issue could be resolved.
Aspects of the Topics settings page design and consent interface may make it more difficult for individuals to make informed decisions about the collection and use of their personal data.	Informed by the ICO-CMA joint paper on Harmful Design in Digital Markets,[15] we expressed concerns that aspects of the Topics settings page and user consent interface could make it harder for individuals to make informed choices in line with their preferences on the collection and use of their data. We have engaged with Google on a range of points relating to this issue. As an example, we have asked Google to include additional information in the consent UI to clarify how users' personal data may be used via the Topics API. In recent UX testing, Google tested updated language in the Topics API screen that provides a clearer indication that other sites make use of the data provided by the user's browser via the Topics API. The text changes resulted in improved overall comprehension relative to the preceding version of the screen. Also, we engaged with Google regarding the positive framing used in the Topics consent UI. It has been our shared view with the ICO that such framing

[15] See the ICO-CMA joint paper on Harmful Design in Digital Markets (accessed on 10 November 2024).

Potential concerns	The CMA's assessment including the ICO's feedback
	may influence Chrome users to overestimate the privacy-protective properties of Topics API. While Google has made improvements in this area, for example by removing the text 'We're launching new privacy features that give you more choice over the ads you see', positive framing remains in the headline of the updated version of the user consent interface ('Turn on an ad privacy feature'). We recommend that Google replaces this framing with more neutral language to enable users to make informed choices in line with their preferences. Our concern regarding the use of positive framing to inform users about the Topics API is also relevant to the Chrome Privacy Guide. Google has shared a preview of the addition of explicit controls for the Topics API to the Chrome Privacy Guide, which will help users to control their Topics settings. While we welcome the addition, we have previously highlighted that stating to users that the Topics API is 'protecting your browsing history and identity' can be misleading, as the API shares insights derived from browsing history with parties. We recommend that Google changes this wording wherever it appears, including the initial Topics API consent UI, to resolve this issue. We also have a remaining concern with the absence of information that may be needed for users to make informed decisions about the Topics API. We have previously told Google that it should be made clear to users that it is exclusively the topics stored in Chrome that are auto-deleted after 4 weeks, while API callers have the ability to store them for longer. This is currently not mentioned in the initial Topics API consent UI, the Chrome Privacy Guide or the Topics settings page. Given the issues remaining which risk users being unable to make informed choices regarding the permissions they set for Topics API, we consider it key that Google address the recommendations outlined above prior to considering the issue resolved.
Users may have limited awareness of their Topics API settings in Chrome (and pathways to change them) after receiving a single exposure to the Topics API prompt during the roll-out of third-party cookie deprecation.	We expressed concerns that there may be a negative impact on users' ability to control their privacy settings in the medium and long term as a result of only receiving a single exposure to the Topics API consent dialogue box. It is our view that a single exposure will reduce the likelihood of users re-engaging with these settings in the future. In response to this issue, Google has said that multiple exposures to the prompt would go against its general principle of limiting the number of re-notifications used on Chrome. This argument is informed by Google's research, which suggests that a higher volume of notifications results in users being more likely to ignore notifications. Google also reported UX research findings in which participants who viewed the API screens had higher levels of perceived autonomy compared to those in a neutral control condition. We acknowledge the need to balance the use of any re-notifications with avoidance of inundating users with information. Google has shared previews of explicit Topics API controls being included in the Privacy Guide as a mitigation to our concern and these controls should provide users with the ability to change their settings at any time. In response to these actions by Google, we consider this issue resolved. However, we have additional points to flag. As discussed in the first row above, the Privacy Guide preview contains less information than the updated Topics consent UI screens. We recommend that Google also include the extra information present in the consent screens in the Privacy Guide to resolve this issue. The change would benefit users.

Potential concerns	The CMA's assessment including the ICO's feedback
	We also suggest that Google explores ways of signposting the pathway through which users can change their Topics settings. This will help users be more aware of (and better able to control) their settings and counteract the issue of non-repeat prompting.

Protected Audience API

Overview

24. The Protected Audience (**PA**) API (formerly known as FLEDGE) is primarily intended to support remarketing and other custom audience use cases.[16] Remarketing is the practice of serving targeted ads to individuals based on their activity on an advertiser's website. PA API 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. PA API has several components, intended to work together to facilitate privacy preserving remarketing. Google has published a timeline showing the status of each component.[17] The timeline is high level, indicating the quarter in which Google expects the feature to be available.

Assessment

25. 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 assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
At third-party cookie deprecation, PA API 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	Google recognises current gaps in the PA API privacy protections. The published roadmap includes action to address some of the issues we identified in April 2024 (eg a timeline to move to TEEs for

[16] For more information on PA API and how it works see Chrome Developer Blog, 'Protected Audience API', 27 January 2022 (accessed on 10 November 2024).
[17] See Chrome Developer Blog, 'Status of pending Protected Audience API capabilities', 9 February 2023 (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	(TEEs)[18] 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 API 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 API 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 that planned controls will be delivered as currently outlined in the product roadmap.	off-device elements of the PA API). Our understanding is that the formal consultation process described in paragraph 14 in the governance section would apply to changes to this roadmap (eg a decision to implement the TEE requirement or Fenced Frames). Under the governance framework, the proposed annual reporting on cross-site tracking risks on Privacy Sandbox in Chrome provides a formal mechanism for Google to collate information on these risks and use that information to inform decisions on changes to the PA API. Subject to this governance framework working effectively, this has the potential to manage the risk of PA API being deployed without a number of key technical privacy controls in place. Particularly while key controls are missing, ad techs using the PA API are responsible for their data protection compliance. The ICO retains its independence to take regulatory action where non-compliance is identified.
Third-party/cross-site data will be combined with first-party data in the PA API IG.	We understand that k-anonymity controls (previously in place to prevent	Google's EU user consent policy states that '[w]hen using Privacy Sandbox APIs, (topics,

[18] 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, 'Aggregation Service', 29 November 2022 (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	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 API. 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 • excessive profiling will occur that exceeds the API's remarketing use case. Google has acknowledged that it is possible to leverage third-party data in PA API'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	protected audience and attribution reporting), you may be using personal data for ads personalisation and/or accessing local storage. The EU user consent policy requires you to obtain valid user consent for these actions in the same way as you rely on consent today for ads personalisation and the use of non-essential local storage to the extent legally required'.[19] Google has an opportunity to surface information about how IGs may be used via the 'first time notice' for the PA API in Chrome. In April 2024, Google updated the 'first time notice' to clarify that ad techs may combine IG data with other information they already hold. Google intends to continue to iterate on this prompt, considering results from UX research on user comprehension. Also, sites have the responsibility to surface information to users to comply with the Applicable Data Protection Legislation where they are using the API and increased responsibility where third party data is included. Sites seeking to create IGs that leverage cross-site data must describe this processing to users when seeking consent to store IG data via their privacy notice. Ad techs using IGs, including those seeking to combine first and third-party data, are responsible for their data protection compliance. The ICO retains its independence to take regulatory action where non-compliance is identified.

[19] See Google, 'Help with the EU user consent policy', 31 October 2019 (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	API 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 API UX to understand if this concern is resolved.	Google's decision to relax *k*-anonymity requirements removes a technical barrier to ad techs using IGs for microtargeting. Our understanding is that Google decided to relax *k*-anonymity requirements to help improve latency in PA API.[20] This is a reasonable balance between technical restrictions to improve privacy and improve PA API's effectiveness, noting that microtargeting risk can be addressed through data protection requirements on parties using the API. The ICO's 2021 Opinion on Data protection and privacy expectations for online advertising proposals[21] highlighted the potential harm of extensive processing about people's behaviour, preferences and attitudes and the need for organisations to address this risk. As mentioned above, ad techs using the API are responsible for complying the Applicable Data Protection Legislation and will be exposed to risk where this is not managed appropriately.
The delegation of 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	In early April 2024, Google proposed updates to the PA API 'first time notice' that a user will see. These updates aimed to clarify that first party sites might work with advertising partners when using the API and may combine this data with other information they already know. Google is also planning to test user comprehension of the updated 'first time notice'. Google states that comparable points of clarification are being explored in relevant PA API Chrome settings pages.

[20] See the CMA's Q3 2023 update report, paragraph 51.
[21] See the 2021 Opinion.

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	to resolve these concerns, including undertaking further user research.	Additionally, Google is updating its Privacy Sandbox Privacy-related Compliance FAQs to highlight transparency and fairness requirements for API callers - particularly when using Privacy Sandbox products that use personal data in ways that may not always be understood by users. The above updates on both the PA API's UX and relevant privacy FAQs could resolve this issue. Any privacy and data protection risks that may persist depend on how and whether sites inform users that embedded parties may create IGs, as opposed to conduct taken directly by Google.
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-	Our understanding is that Google intends to implement a phased timeline to transition default site permissions from 'allow all' to 'block all'. We await publication of the timeline for the transition for this issue to be resolved. To enhance transparency and provide greater control over data processing, the ICO recommends site owners regularly review their use of cookies and similar technologies, in line with the ICO PECR guidance.[22]

[22] For further details see the ICO's 'How do we comply with the cookie rules?' guidance (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	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.	
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, the ICO has expressed the concern 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	Our discussions with Google on governance confirm that changes to the PA API would be subject to the formal consultation process as described in paragraph 14 on governance above, if the change significantly altered privacy or utility properties of the API. Changes below the significance threshold may be captured by Google's reporting to the Monitoring Trustee and reporting to the ICO and the CMA on cross-site tracking risks on Privacy Sandbox in Chrome. We consider this issue could be resolved, subject to the governance framework working effectively. Under the envisaged consultation process, Google will consider stakeholder feedback and balance the range of D&I criteria in decisions relating to the PA API.

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	ensure privacy is correctly balanced against utility and the immediate priority of adoption. We await Google's updated approach to governance.	
That additional cross-site data that exceeds the original scope of the proposal is processed in PA API without sufficient transparency.	No update provided in this reporting period.	In September 2024, Google announced an update to PA API that will allow auctions to use signals relating to user views and clicks within advertiser bidding models. We understand that Google introduced the 'clickiness' feature following feedback from the ad ecosystem. We understand that this new feature allows view and click events to be registered alongside similar source events recorded by the ARA. As with the removal of k-anonymity restrictions on IGs (that allows third party data outside of the first party site to be processed in the auction), the introduction of this feature deviates from the original scope of the proposal that sought to limit cross-site tracking. With the introduction of the 'clickiness' feature, user browsing activity relating to views and clicks across multiple sites is now processed in the PA API auction. Google has sought to minimise the risk of introducing further cross-site data into the API by: limiting click and view data to total count; adding an unspecified amount of noise; only allowing access to the signal inside the auction environment; and applying the same planned controls to post-auction reporting. Alongside the update to the API, Google has proposed updates to the PA API UX to inform users that additional cross-site signals are used in the API. However, Google only

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
		mentions click data and not views. We have requested that Google accurately informs users of the cross-site information available to advertisers in PA API. We recommend that Google update the language to make it clear to users that sites can find out what ads users click on, and view, on other sites. Addressing this issue can resolve transparency concerns in this area.

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 assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024.

27. Stakeholders have used the Chrome-facilitated testing period to identify changes that they believe could improve PA API utility. Some (eg Criteo) have published those proposals, including explanations of why and how they believe the changes could be implemented.[23] We want to ensure that the Privacy Sandbox develops in ways that continue to take the D&I criteria into account and meet Google's obligations (eg non-discrimination) in the Commitments. Our current view is that Google's governance framework could provide an appropriate framework for decision-making with respect to stakeholder-requested changes. However, Google is not required to wait until the future governance process is in place to consider feature requests. The process that Google has run to date (ie discussions with the CMA, the ICO and the Monitoring Trustee where the proposed changes could raise issues under the Commitments) can be applied to these requests.

PA API Concerns

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
GAM will not participate in PA API component auctions	Our understanding of the current approach is that GAM	Stakeholders continue to request support in

[23] See 'Google's Privacy Sandbox: The Path Forward for Viability', 27 June 2024 (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
unless it is the top-level PA API seller. This means that publishers have to use GAM in order to access AdX demand.	will only participate in PA API component auctions where GAM also run the top-level PA API auction. We are exploring whether parties other than the publisher ad server should be able to run the top-level PA API auction. Our current understanding is that some ad server functionality (eg pacing) may not be available unless the ad server runs the top-level PA API auction. 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 API 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 API auction.[24] We are continuing to discuss these concerns with Google. This is a high priority area for us to resolve.	implementing Prebid's solution,[25] highlighting its configurability advantages over GAM's implementation. We are continuing to discuss this issue with Google.
PA API 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 component auction winners.	PA API 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 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	We are continuing to discuss this issue with Google.

[24] See Issues #10690 and #9481 on the 'Prebid' repository on GitHub (accessed on 10 November 2024).
[25] For more details, see Prebid's 'top level PAAPI module' (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	component sellers the publisher may select. Google has provided 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 API auctions. We encourage the ecosystem to provide feedback on Google's proposed design.[26]	
Information on PA API component auction winners will be visible to GAM, raising concerns about unequal access to information.	Our current understanding is that each PA API 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. Based on its commitments to the French Competition Authority on the online advertising case,[27] 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' (eg for computation of the Minimum Bid to Win). We are currently discussing with Google whether GAM has access to information that is not shared with the publisher.	We are continuing to discuss this issue with Google.

[26] See Issue #957 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[27] See Decision 21-D-11 regarding practices implemented in the online advertising sector, 7 June 2021 (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
GAM proposes to use machine learning to decide whether to trigger a PA API 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 API auction. Our understanding is that the option is for publishers to either opt-in or out of the machine learning trigger. 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 API auction, and access to the information necessary to decide whether to trigger that auction.	Since the publication of our last report, GAM has launched a control mechanism, 'Allow testing on all inventory with non-Google sellers'[28], which allows publishers to override the GAM decision on whether to run a PA auction in response to an ad request. The framing of this option suggests that it is intended for testing, not as a long-term solution. We take note of this update and are continuing to discuss this issue with Google.

PA API Services Concerns

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
Latency for on-device auctions. Testing suggests that PA API auctions may be slower, either due to device constraints (eg processing power available), auction design (eg waiting for information on the winning contextual bid before completing the PA auction) or network requests (eg 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 API. The design changes add controls for sellers, allowing sellers to set limits on the time and resources buyers can consume.[29] The guidance includes recommended best	In addition to Google's research on the impact of ad rendering time on viewability and impressions,[31] several stakeholders have published data on latency (eg Wirtualna Polska, RTB House, and Criteo).[32] We have also discussed unpublished (at the time of writing) findings with other stakeholders whose results are similar. Some stakeholders described their approaches to attempt to

[28] See 'Allow testing on all inventory with non-Google sellers' in Google Ad Manager Help (accessed on 10 November 2024).
[29] See 'Performance of Protected Audience Auctions' in Google's Q3 2023 feedback report (accessed on 10 November 2024).
[31] See 'Fast ads matter', 29 October 2019 (accessed on 10 November 2024).
[32] See 'Protected Audience API test on Wirtulana Polska Media Inventory', 25 March 2024; 'FLEDGE on-device auctions end-to-end latency', 17 June 2024; and 'Privacy Sandbox Testing Results Show Shortfalls to Meet CMA Requirements', 27 June 2024 (all accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	practice for buyers and sellers.[30] We are monitoring latency issues closely, recognising that high latency can lead to unsold ad inventory and negatively impact UX. 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.	mitigate latency by, for example, reducing the size of the bidding logic to reduce on-device computation requirements. Since the publication of our last report, Google has published details on B&A services with 'mixed mode' to support the usage of B&A.[33] Our understanding is that this will address some of the latency concerns. Google reiterates that on-device serves as an effective alternative to B&A and continues to propose solutions aimed at improving parallelisation,[34] which would require changes to how GAM implements PA API as well as introducing timeouts. Google also highlights that by enhancing features within the PA API, such as 'clickiness' data, and by transitioning to the revised approach to the Privacy Sandbox, ad tech companies can regain additional revenue, outweighing the associated costs of latency.[35] To resolve this issue, Google should continue implementing improvements to optimise latency and continue to provide guidelines outlining best practices for ad tech use cases (balancing data enrichment and latency). Any associated impact on performance (such as unsold inventory) should also be addressed through the proposed governance framework.
Concerns about the requirement to adopt TEEs to	We are aware of increased concerns regarding uncertain	Our views remain unchanged. Ad techs have expressed

[30] See Chrome Developer Blog, 'Improve Protected Audience API auction latency', 27 June 2022 (accessed on 10 November 2024).
[33] See 'Protected Audience Mixed Mode Auctions' on GitHub (accessed on 10 November 2024).
[34] See Issue #851 on the 'FLEDGE' repository on GitHub (accessed on 10 November 2024).
[35] See 'What is Google Ad Manager's plan regarding any added latency from the Protected Audience API?' (accessed 10 November 2024); 'Privacy-Enhanced versus Traditional Retargeting: Ad Effectiveness in an Industry-Wide Field Experiment' 30 September 2024 (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
operate PA API's server-side elements, such as the Bidding and Auction (B&A) Services and the Key/Value Server.	TEE requirements and the unavailability of Bidding and Auction services beyond the origin trial. 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. This is supported by ongoing improvements in latency,[36] with forthcoming updates providing greater clarity on B&A services' costs and the outline of the baseline system,[37] as well as strategies for scaling up traffic B&A services beyond the origin trial.[38] Google also emphasised that some off-device services will be an optional extra for market participants who want to develop larger, more sophisticated models, allowing stakeholders to choose components aligning with their objectives. Concerns have been raised 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. We are working with Google to explore the flexibility of server-	concern that latency could increase once PA API operations transition to TEEs, particularly when production-level traffic becomes available for B&A servers and the Key/Value TEE becomes mandatory. Subsequently stakeholders will be required to adopt TEEs and other optional features[39] to maintain competitiveness, rather than develop larger models, given the direct impact of auction duration on ad rendering times.[40] We encourage stakeholders to publish testing results once testing becomes available. We continue to monitor developments regarding the TEE requirements and server architecture costs, design and timeline,[41] as outlined further in the TEE section below.

[36] See Chrome Developer Blog, 'Improve Protected Audience API auction latency', 27 June 2022 (accessed on 10 November 2024).
[37] See 'Bidding and Auction Costs' on the 'Protected Auction Services Discussion' repository on GitHub (accessed on 10 November 2024).
[38] See 'roadmap' within 'Bidding and Auction services' on the 'Protected Auction Services Docs' repository on GitHub (accessed on 10 November 2024).
[39] For example, see 'Sharding via Key/value Server' on the 'Protected Auction Key Value Service' repository on GitHub (accessed on 17 July); and see Issue #1140 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[40] See KV lookup latency under 'API Usage' within Google's Q1 2024 feedback report; and see 'InterestGroupBuyers as promise' within Issue #1093 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[41] See Google's 'Timeline for availability of Bidding and Auction services' (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	to-server architecture and await the results of the testing period.	
Google intends to deprecate event level reporting for PA API 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. 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.	Our views remain unchanged. We recognise the importance of stakeholders optimising their bidding strategies based on reporting from PA API auctions once event level reporting is deprecated. Google reiterates that event level reporting will be supported until at least 2026.[42] We are aware of several stakeholder requests to expand reporting. Google is engaging with these proposals, for example it seeks feedback on an alternative version of the 'global click and display counters' request. We encourage stakeholders to continue to provide feedback directly to Google on its alternative.[43] We are also aware of stakeholders' requests to provide more detailed debugging and monitoring tools with real-time event-level data samples.[44] Our current view is that the governance framework, if applied effectively, could provide a mechanism for decision-making on these ongoing issues, including through formal stakeholder consultation and consideration of the D&I criteria.

28. We have consulted with the ICO regarding the application of **D&I D – User experience** and set out our assessment in the table below. The CMA's assessment below includes the ICO's feedback.

[42] See Google's 'Status of pending Protected Audience API capabilities' (accessed on 10 November 2024).
[43] For more information, see 'New field addition to modelingSignals that can only encode display and click information' in Google's Q1 2024 feedback report; and Google's alternative proposal in Issue #957 on the 'PA API' repository on GitHub (accessed 10 November 2024).
[44] See Issue #632 on the 'PA API' repository on GitHub (accessed on 10 November 2024); and see 'Real-time monitoring API' (accessed 10 November 2024).

Potential concerns	The CMA's assessment including the ICO's feedback
The sequencing of the initial Topics, and combined PA API and ARA prompts makes it unclear or unintuitive for users that these are three different APIs.	The close sequencing of the prompts for Topics, PA API and ARA is impacting user comprehension. Google's UX research shows that users struggle to identify that the initial prompts for Topics, PA API and ARA are providing information about three different APIs. Particularly in relation to the PA API and ARA, our view is that the highlighting of the 'Got it' button on the prompt nudges users to dismiss the notice without reading or comprehending the information presented. This view is informed by the ICO-CMA joint paper on Harmful Design in Digital Markets which describes a 'harmful nudge' as 'when a firm makes it easy [for] users to make inadvertent or ill-considered decisions'. In response to this research finding and our concern, Google conducted further testing of user comprehension of the discrete nature of the APIs using an updated set of Topics and combined PA API and ARA prompts, with the latter prompt having undergone a restructuring to draw a clearer distinction between PA API (described as 'site-suggested ads') and ARA (described as 'ad measurement'). To note, this issue is also applicable to ARA. For brevity, it has not been repeated in the ARA section of this report. The new UX research conducted by Google shows that average clarity ratings for the updated API screens were significantly greater than the midpoint of the scale in response to the question 'how clear is it to you that the two screens above describe three ad privacy features'. While we welcome this research, we would have more confidence in the results if users were asked a question that did not state the number of APIs. We recommend that Google avoids such leading questions in future, to increase the robustness of its research results. In the UX research, both the current and revised versions of the PA API/ARA prompt use the 'Got it' button, which is highlighted in blue in comparison to the 'Settings' button. There is potential for this to be a 'harmful nudge' given the difference in salience of the buttons. We recommend that Google remove the difference in highlighting between the two buttons and will consider the issue to be resolved when this change has been made.
It is not made clear to the user when a site has delegated permissions to a third party.	We are concerned that it is not clear in the PA API settings page when a site has delegated permissions to a third party for user data processing such as IG creation. Instead, only the names of the first-party sites are surfaced to users, which can give users the impression that only those sites are involved in processing their data. Therefore, we are concerned that users would be basing their decisions about the use of their data on inaccurate information. This concern is compounded when considered alongside the issue in the next row below. Google has explored methods to surface more information regarding the use of data by parties but does not have a viable means to provide this information as the browser does not have a way of knowing if an IG has cross-site data added by the site or its partner. We acknowledge this and suggest that Google considers whether information on third party use of data should be moved up from the drop-down on the PA API/ARA first time notice to the main body. This is because Google's own research shows that just under 20% of users click on the drop-down on the PA API/ARA first time notice.

Potential concerns	The CMA's assessment including the ICO's feedback
The purposes of IGs are not made clear to users.	The purpose of an IG is not made clear in the PA API settings page. Also, users currently have no access to group or issuer names that are described in an intelligible / human-readable manner, which risks having negative downstream impacts on users' ability to control their privacy settings and make effective choices about blocking select PA API interest groups. We recommended that Google explore options for allowing users access to intelligible PA API group and issuer names via the settings page. Although the CMA appreciates that Google has limited control over the full suite of PA API group names that may be generated by parties using the PA API, it is our view that this does not preclude Google from taking effective steps to increase transparency to users via the Chrome Settings page. Without this information, it is difficult for a user to make an informed decision on whether they want to be part of the IG. This concern is compounded when considered alongside the issue in the previous row above. In response to our concerns that users may not understand the purpose of an IG, Google has begun exploring ways to communicate more clearly information regarding IGs through changes to user transparency notices. Google is also proposing to make updates to its compliance guidance with respect to the obligations of developers in relation to transparency and consent requirements . We welcome the steps Google is taking to increase transparency and improve communications in relation to IGs. Although we acknowledge the technical challenges in providing users with access to an intelligible list of groups and issuers, we recommend that Google continue to explore the option of providing users with this information.
Positive framing in the PA API 'first time notice' can make it more difficult for users to make informed choices about their data.	We expressed the concern that the initial prompt that users receive regarding the PA API provides an overly positive framing for the API that impedes the ability for users to make an informed choice. This view is based on the ICO-CMA joint paper on Harmful Design in Digital Markets which states that biased framing can encompass 'the practice of presenting choices in a way that emphasises the supposed benefits or positive outcomes of a particular option, in order to make it more appealing to the user [... which] can lead users to make ill-informed choices'.[45] We have engaged with Google on this point and consider our concern particularly relevant given that PA API will in fact be deployed without a number of key technical privacy controls, therefore raising the risk that the prompt in its current form overstates the privacy benefits to users. In response to this concern, Google has tested updated language in the PA API prompt that provides more information regarding how user data will be used. Google reported higher overall comprehension for the new language. While this is positive, we consider that wording such as 'help protect your browsing history and identity' can encourage users to assume that there will be more blanket protection for their data than in reality. Google's own wording earlier in the first time notice is a more accurate, and less positively framed description. We therefore recommend that Google consistently uses 'help limit what sites and their advertising partners can learn about you' instead of 'help protect your browsing history and identity' and 'personalised ads' instead of 'relevant ads'.

[45] See the ICO-CMA joint paper on harmful Design in Digital Markets, page 18 (accessed on 10 November 2024).

Measuring digital ads

Attribution Reporting API

Overview

29. 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 (eg creating an account or making a purchase) after clicking on or viewing an ad.[46] Measuring conversions is necessary for several of ad tech's key functions, including budgeting, campaign reporting, optimising bidding strategies, and pricing ad inventory.

30. ARA supports two forms of reporting:

(a) Event-level reporting. Event-level reports provide information about a specific ad event (like a 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.[47]

(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 them to the ad tech's aggregation service, a specialised server running in a TEE on the public cloud (ie cloud services delivered by an external provider). The aggregation service aggregates and decrypts the batched reports and adds privacy protections like noise.

---

[46] See Chrome Developer Blog, 'Attribution Reporting for Web overview', 18 May 2021 (accessed on 10 November 2024).
[47] ARA currently supports up to eight conversion categories for event-level reporting. See Chrome Developer Blog, 'Attribution Reporting for Web overview', 18 May 2021 (accessed on 10 November 2024).

The ad tech can then retrieve summary reports from the aggregation service.[48]

31. 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.[49]

Assessment

32. 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 assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
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. Google has acknowledged that, by necessity (ie 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 (eg limiting the information joined to between 1 and 3 bits (conversion	We recognise that there may be privacy and data protection risk associated with the continued availability of event-level reporting, depending on how API callers use ARA. Google's proposed reporting on risks to privacy from cross-site tracking on Privacy Sandbox on Chrome described in paragraph 14 above, if applied effectively, would provide a formal mechanism for Google to collate information on these risks and use that information as a basis for deciding on changes to ARA.

[48] See 'Aggregation Service for the Attribution Reporting API' on the 'Attribution Reporting API' repository on GitHub (accessed on 10 November 2024).
[49] See Google Ads Developer Blog, 'Optimally configure the Attribution Reporting API for ad measurement', 7 December 2023 (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	data) and applying event-level (ie 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 (eg 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.	

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	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.	
Key controls, such as epsilon values and API rate limits, have not been tested.	We understand that key controls (eg 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	Google proposes to monitor cross-site tracking risk under its proposed governance framework described in paragraph 14 above. We consider that annual reporting and review provide an opportunity to assess whether the privacy controls (eg rate limits and epsilon values) are working as intended. We also note that changes to third-party cookie availability under Google's revised approach to the Privacy Sandbox could change the effectiveness of key controls designed for a third-party cookie deprecation scenario. Our current view is that the governance framework, if applied effectively, could resolve this issue.

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	Library[50] and Noise Lab[51] and will also give ad techs enough time to test before any changes are made. We await Google's response on its governance process.	
Documentation, guidance and wider public-facing information relating to ARA do not make clear the requirement to consider the collection of consent required by PECR.	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, 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.	In May 2024, Google provided an update on changes it is making to the Privacy Sandbox Privacy-related Compliance FAQs. Relevant to this concern, these updates provide clarity on the requirement for API callers to obtain consent before using ARA. This guidance makes clear that the API involves the storage and access of data stored on the user's browser. While we are still waiting for these changes to be published, once live, these changes are likely to resolve this issue.

33. 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 assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
ARA does not support some types of attribution that are currently available with third-party cookies, for example multi-touch attribution.	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 (eg a publisher site, their social media	We have received responses from Google that multi-touch attribution is neither a preferred nor common method currently used to attribute conversions. Google has also stated that single-touch on a single device is generally the default

[50] See the 'Measurement simulation' repository on GitHub (accessed on 10 November 2024).
[51] See Noise Lab (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	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.	attribution model and is preferred because it is typically easier to understand and collect, and provides more immediate actionable insights. In any event, Google argues that any loss of multi-touch attribution is unlikely to substantially affect ad techs or publishers. We understand that Google believes that Privacy Sandbox does currently offer a multi-touch attribution solution via Shared Storage and Private Aggregation. We are following up with Google on the user journey elements but recognise that Privacy Sandbox does not need to replicate the same functionality as third-party cookies. We welcome stakeholder views on the extent to which multi-touch reporting is useful more broadly (ie for purposes other than attributing conversions) and on whether Google's recommendation to use Shared Storage and Private Aggregation meets stakeholder requirements.
The proposed '20 event per aggregatable report' limit appears arbitrary and undermines ARA's utility.	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.	Google continues to adjust Privacy Sandbox parameters in response to ecosystem feedback. For example, Google has proposed enabling sites to customise the number of contributions per report for the Private Aggregation API and increased the number of contributions allowed by default in some cases.[52] Parameter changes that significantly change privacy or utility will be subject to the formal consultation process within the context of the governance framework

[52] See 2 May 2024 comment on issue #81 in the 'Private Aggregation' repository on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
		described in paragraph 14. If applied effectively, this issue could be resolved.

34. We have consulted with the ICO regarding the application of **D&I D – User experience** and we do not currently have any outstanding concerns. We set out our updated assessment of each of the issues we previously identified in **Appendix 2**.

Trusted Execution Environments

Overview

35. Google introduced Trusted Execution Environments (**TEEs**) to support use-cases where privacy-preserving off-device processing is required. 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, so TEE-based solutions are intended to extend privacy protections to device-to-server interactions that extend the functionality of Privacy Sandbox APIs.

36. 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 parties.

37. Aggregation Service in a TEE is required for use of the ARA Aggregation API and the Private Aggregation API (for PA API). However, debug reports currently allow for the use of Aggregation Services outside of a TEE, and most users have debug reports. There are also TEEs for other contexts, such as the Key/Value (K/V) and Bidding and Auction (B&A) Servers for PA API. Google has updated the TEE explainer to provide more detail on timeline and feature availability. [53]

[53] For more detail, see the TEE explainer on GitHub (accessed on 10 November 2024).

Assessment

38. After consulting with the ICO, we note that TEEs are intended to address risks arising from API callers' ability to join user activity across sites when using B&A and K/V servers. TEEs are one way to address these risks. We consider that changes to Google's planned roadmap for imposing mandatory TEE requirements should be considered under Google's proposed governance framework. If Google decides to change its approach to TEEs, we consider that an alternative means to address the risks from cross-site identity joins should be implemented. As above, Google's proposed annual reporting on risks to privacy from cross-site tracking provides a formal mechanism for Google to collate information on these risks and that ad techs using the current bring-your-own-server (BYOS) functionality for K/V servers are responsible for their data protection compliance. The ICO retains its independence to take regulatory action where non-compliance is identified (see **D&I A – Privacy outcomes** table in the PA API section above).

39. 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 include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024.

Potential concerns	**The CMA's views in the April 2024 report**	**The CMA's assessment**
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 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	Google has published a K/V playbook and K/V cost explainer and has invited stakeholders to participate in the B&A and K/V beta programs to experiment and share feedback. A stakeholder commenting on the private cloud GitHub issue #68 (see below) has pointed out that one of the potential TEE architectures is relatively new, which means they may need to retire and replace hardware not intended for decommissioning for a number of years, therefore providing an additional cost burden. The overall assessment of costs and viability of TEE based solutions (including for ARA, B&A and K/V services) is still uncertain, especially at large scale. This is especially

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	would welcome stakeholder feedback on non-negligible cost concerns.	the case when assessing cost versus benefit. At least one stakeholder is concerned about the viability of what they consider an unproven technology at the large scales that would be required post third party cookie deprecation. Costs will vary, eg depending on whether ad techs already use public cloud for some workloads, and we have heard different views from ad techs on the impact on their businesses. Some TEE based functionality, eg B&A services, are due to become available for scaled testing in early 2025. Google has also said that it will provide 'substantial notice for developers to begin testing and adoption' before imposing the requirement to run K/V servers in TEEs.[54] A decision to impose the TEE requirement should be taken under Google's proposed governance framework described in paragraph 14, allowing a full consideration of the D&I criteria, including evidence from testing.
Google currently only supports two public cloud providers, Amazon Web Services (AWS) and Google Cloud Platform (GCP).	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 attestations are trustworthy, by ensuring compliance with recognised industry standards on cloud security, in particular ISO	We understand that Google is still considering an application from Azure for onboarding. We are not aware of requests from other cloud providers or of specific stakeholder requests to support a particular cloud provider. Google's proposed appeals process under the governance framework described in paragraph 14 is likely to apply to decisions to reject a cloud provider as a public cloud provider under Google's published cloud criteria.

[54] See 'FLEDGE services for Chrome and Android' 24 August 2024 (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	27001, ISO 27017 and ISO 27018, and certification from cloud security industry bodies ie. Level 2 in Cloud Security Alliance's STAR program. Google has now published finalised guidance and specification criteria for onboarding new cloud providers.[55] 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.	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	Google has stated that it is currently gathering feedback from the ecosystem on technical and operational aspects of running confidential processing infrastructure in private clouds. Google has requested feedback on proposed technical requirements for TEE deployment on private clouds[56]. Several stakeholders have responded and welcome the discussion.

[55] See 'Public Cloud TEE Requirements' on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[56] See Issue #68 on the 'PA API' repository on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	outside of public clouds will be available in production. Google has proposed publishing further details on its technical 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.	Google has also told us it has discussed this in meetings with interested ad techs. It has also informed us that the feedback it has received so far is helping it to validate design choices across several areas including infrastructure geometry, component sizing, networking, and deployment approaches, which are all inputs into a secure implementation of private cloud TEEs. Google has stated that, at the current stage of research, it cannot guarantee that it will be possible to support private cloud infrastructure. As above, testing could provide further evidence to inform decisions under Google's proposed governance framework on imposing TEE requirements for off-device processing to support the Privacy Sandbox tools.
Performance degradation and scalability	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.	Google has told us that where the aggregation service is concerned there is no need to delay the requirement for use of the service in a TEE on the grounds that it is a batch processing service that is not in the 'hot path' of an auction and has been available for testing on AWS since October 2022 and GCP since November 2023. Google has also told us that it is working with ad techs directly to address supporting greater scale for the aggregation service. Regarding the B&A services, Google has responded that such services have been available for testing with limited traffic since November 2023 and that they remain optional. We do not consider however that this addresses the concerns raised, especially

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	We have relayed these concerns to Google and await its response.	those regarding on-device performance and the fact that production level traffic will not be available until early 2025. Similarly, Google reiterated to us that the K/V service has been available for testing since April 2023 with expected general availability in Q4 2024 and that the requirement for TEE usage will not be enforced prior to Q3 2025. As above, we consider that testing could provide further evidence to inform decisions under Google's proposed governance framework on imposing TEE requirements for off-device processing to support the Privacy Sandbox tools.
Chrome restricting scope for innovation through its implementation of TEE services	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 said 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	We recognise that in the interests of required availability and functionality once Google's revised approach to Privacy Sandbox is implemented, design and implementation need to remain with Google for the foreseeable future. Google's proposed governance framework described in paragraph 14 requires stakeholder consultation on strategic decisions. Stakeholders will also continue to have opportunities to provide input on Google's TEE implementation as part of the 'development in the open' practices that will apply in the context of that framework. Any decision to support alternative implementations could be taken within the governance process.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	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 its competitors' innovations in machine learning models. Google has responded that it may limit functionality in order to maintain security and privacy, eg 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.	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 Google 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	Our view is that Google's proposed governance framework described in paragraph 14 could resolve this issue if applied effectively.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	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 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[57] 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	

[57] See Accenture's public statement (accessed on 10 November 2024).

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

40. 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.

Strengthening cross-site boundaries

Related Website Sets

Overview

41. RWS is intended to 'enable limited cross-site cookie access for specific, user-facing purposes'.[58] Google states that RWS 'is not intended as an ads solution'.[59] However, there is no technical prohibition on using RWS for ads

[58] See 'Overview' within the 'RWS Submission Guidelines' on the 'RWS' repository on GitHub (accessed on 10 November 2024).
[59] See 'Associated domain limit increase to five domains' within Chrome Developer Blog, 'Related Website Sets - the new name for First-Party Sets in Chrome 117', 31 August 2023 (accessed on 10 November 2024).

purposes; sites will need to consider whether their use of RWS meets data protection requirements. 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.[60]

42. Site owners declare related domains using one of three Google-defined subsets. The subsets reflect 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.[61]

(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.

(c) '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.

43. RWS relies on the Storage Access API to facilitate cross-site access for domains in the 'associated' set.[62] 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.

44. 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

---

[60] See 'RWS Submission Guidelines' on the 'RWS' repository on GitHub (accessed on 10 November 2024).
[61] For the list of country code top level domain', see ICANNwiki, 'Current ccTLDs', 19 March 2024 (accessed on 10 November 2024).
[62] For an overview, see 'Providing capabilities beyond the Storage Access API' within 'RWS (formerly known as: FPS) proposal' on the 'RWS' repository on GitHub (accessed on 10 November 2024).

repository.[63] Google applies technical validation to RWS submissions. There is currently no validation other than the technical checks.

Assessment

45. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
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.[64] 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.	Google has proposed to define enumerated lists of 'common' rationales that submitters could choose from when submitting their lists of associated and service sites. Google is seeking feedback on the initial list and the broader proposal.[65] Although we welcome this initial list as a starting point, we are engaging with Google on several of the proposed list items, including by providing feedback to improve the draft set of 'common' rationales. RWS set owners have obligations under Applicable Data Protection Legislation, including to collect consent to store and read cookies on a user's device. This requires set owners to communicate the purposes of this processing to users, including via their RWS set declaration.

[63] For an overview, see 'Set Formation Requirements' within 'Related Website Sets Submission Guidelines' on the 'RWS' repository on GitHub (accessed on 10 November 2024).
[64] See current RWS submission on the 'RWS' repository on GitHub (accessed on 10 November 2024).
[65] See issue #531 on the 'RWS' repository on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	In response, Google is considering the addition of structured fields (eg 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. 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	Linked to the issue in the row above, Google has outlined how enumerated rationales for associated and service subsets may be surfaced to Chrome users via the RWS UI. Surfacing information to the user in the browser is a positive development and can help to improve transparency. As mentioned above, we are providing feedback on Google's proposed enumerated list of rationales.

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	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/UX. 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 UX 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 (eg 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	While RWS limits the scale of cross site tracking via associated domains, we consider that this risk to privacy outcomes and data protection compliance persists. As with other APIs, whether that risk materialises will depend on how parties use RWS. The proposed reporting on cross-site tracking risks on Privacy Sandbox on Chrome provides a formal mechanism for Google to collate information on these risks and use that information to inform decisions on changes to RWS. For example, the governance framework allows for changes to the number of associated domains based on reporting on whether the current 5+1 limit is in fact sufficient to limit misuse. Therefore, subject to the governance framework working effectively, we consider the issue could be resolved, noting that privacy and data protection risks may persist, depending on how parties including publishers and ad techs use RWS.

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	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.	

46. 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 include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
Google discretion in merging RWS declarations into the canonical list.	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'.[66] We believe that moving to automated checks, as part of a broader governance process, is likely to resolve this concern.	Our view is that Google's governance framework could resolve this issue, if applied effectively. Google's proposals include setting up an independent appeals process for operational decisions. In our view, this should include decisions on whether an RWS declaration meets the criteria and can be merged into the canonical list.

[66] See Pull Request #148 on the 'RWS' repository on GitHub (accessed on 10 November 2024).

47. We have consulted with the ICO regarding the application of **D&I D – User experience** and set out our assessment in the table below. The CMA's assessment below includes the ICO's feedback.

Potential concerns	**The CMA's assessment including the ICO's feedback**
Users do not adequately comprehend the purpose and scope of RWS	Google's research involving Chrome users in the US is relevant to this issue. The research has shown that most users do not know about third-party cookies. This has raised concerns about users' ability to appreciate the extent and purpose of data sharing within the context of RWS as a third-party cookie carveout within a regime where third-party cookies are limited. Poor user comprehension can undermine users' ability to make effective choices about keeping RWS in its default-on state and to exercise control over settings. Google has shared with us the results of UX research targeting user comprehension of RWS in response to an updated settings page which can provide clear rationales for data sharing within specific sets. Google tested how well users understand each individual rationale which may be on display, and the results show variation in comprehension across rationales. For example, users had significantly better comprehension of 'performance monitoring' than other rationales, while other rationales had comprehension levels close to or below 50%. Moreover, on average, users conflated each rationale with the descriptions of 6 or 7 others, suggesting that users struggle to understand the scope of the rationale set out for a related website set. Google is considering further research to evaluate user sentiment and comprehension when multiple rationales are presented simultaneously. We look forward to seeing the results, with the continuing caveat that, as discussed under D&I A, some of the rationales in the list do not clearly communicate the intended use case by site owners. For example, while 'performance monitoring' is clearly a use case, others are not, so user comprehension would not be enough to solve our concerns. We acknowledge that Google is reevaluating the value of some of the rationales after considering the results of its UX research, so we welcome seeing whether the updated list of rationales will more clearly communicate the use cases intended by site owners. Google will also need to ensure under its revised approach to the Privacy Sandbox that users understand how RWS will operate within that context.
The user journey to find out which sites are in a RWS may not be intuitive.	Related to the issue in the row below, we are concerned that the user journey to find out which sites are in a set, whether through settings or the address bar, may not be intuitive for the user. We view the ability for users to easily access information on the sites connected via a RWS as important. This view is supported by Google's own research which suggests that Chrome users experience greater privacy concerns as the number of domains sharing data increases. Linked to the issue in the row above, we have viewed the friction when accessing this information as too high. Google has taken some significant positive steps to resolve this concern. As described in the row above, Google has shared with us user testing plans featuring an updated Chrome settings page and address bar, which simplifies the process of finding out which sites are in a related set by: • providing a badge and subtext (on the desktop and mobile settings pages respectively) to highlight which sites form part of a set, and allowing users to view individual set hierarchies

Potential concerns	The CMA's assessment including the ICO's feedback
	We welcome this change, and we are currently awaiting the results of Google's UX testing.
It may not be intuitive for users to understand how to clear data for specific RWS.	In the desktop environment users can clear data for specific Related Website Sets via controls located next to the address bar. While the existence of these controls is positive, we are concerned that the journey to these controls may not be intuitive for the user. This view is informed by the ICO-CMA joint paper on Harmful Design in Digital Markets and relates in particular to 'sludge' techniques where 'excessive or unjustified friction […] makes it difficult for the user to get what they want or to do as they wish'.[67] In a recent update, Google has shared with us robust plans to carry out user testing on an updated Chrome settings page and to measure the perceived ease and autonomy that users experience while navigating the task of clearing their data for specific website sets. This modified page design: (i) flags which sites storing cookies have related domains, (ii) allows users to view the hierarchies of sites and their subdomains, and (iii) offers a simple route for users to clear their data on a per-site and per-set basis. Google is also taking steps to establish parity between desktop and mobile settings. We welcome these steps. We are currently also awaiting the results of Google's UX testing.

Federated Credential Management

Overview

48. Federated Credential Management (**FedCM**) is intended to support federated identity on the web, 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 passwords in terms of trustworthiness, ease-of-use, and security.[68]

49. 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.

50. We are aware that both Mozilla and Apple are considering implementation of a variation of FedCM tools in their browsers, and that standardisation

[67] See the ICO-CMA joint paper on Harmful Design in Digital Markets, page 12 (accessed on 10 November 2024).
[68] See Chrome Developer Blog, 'Federated Credential Management API overview', 27 May 2024 (accessed on 10 November 2024).

discussions are likely to continue in the newly chartered W3C Federated Identity Working Group.[69]

Assessment

51. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
Websites will use the client_metadata_endpoint and dialogs to obtain invalid consent.	We understand that a website (relying parties - 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.[70] 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 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.	In May 2024, Google provided an update on changes it is making to Privacy Sandbox Privacy-related Compliance FAQs. Google has also published guidance in relation to the FedCM API that highlights the need for API users to consider the likely requirement for consent as the appropriate lawful basis when processing FedCM-related data for purposes outside of authentication. This makes it clear that consent for such processing must be obtained separately from the FedCM dialog. Although the updates to the guidance are welcome, invalid consent for personal data processing obtained via federated identity systems continues to be a risk. We are discussing with Google the additional steps it might take within the FedCM dialogue to further address this risk.

[69] For more information, see the 'Federated Identity Working Group' (accessed on 10 November 2024).
[70] Article 4(11), Article 6(1)(a) and Article 7 GDPR. For more information on valid consent, see 'What is valid consent?' within the ICO's 'Consent Guidance', 22 March 2018 (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	We are continuing our discussions with Google on this point.	

52. We do not currently have any outstanding concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**. In **Appendix 2**, we include our updated assessment of each of the issues previously identified.

53. We have consulted with the ICO regarding the application of **D&I D – User experience** and set out our assessment in the table below. The CMA's assessment below includes the ICO's feedback.

Potential concerns	The CMA's assessment including the ICO's feedback
The FedCM dialogue box is not sufficiently clear to obtain lawful consent for the likely full range of FedCM use cases (eg marketing purposes).	Google has provided UI mock-ups for the button flow of FedCM, ie the journey that users would go on as they click through the different screens of FedCM to log in via an Identity Provider (IdP). As no information is provided in the button flow to make it clear that users are not giving consent for the processing of their data for purposes outside of authentication, we are concerned that aspects of the button flow will create confusion. RPs and IdPs have the option of providing links to their privacy policies and terms of service to users through the FedCM dialogue box. In the current mock-ups, the button for 'continue' is highlighted in comparison to the button for 'cancel'. Further, the links to the privacy policy and terms of service are presented in a smaller font than the main body of text. Our view is that this design steers users to click 'continue' without engaging with the privacy policy and terms of service information. This assessment is based on the ICO-CMA joint paper on Harmful Design in Digital Markets that defines a 'harmful nudge' as 'when a firm makes it easy [for] users to make inadvertent or ill-considered decisions'. As a result, based on the current UX, the current interface cannot be relied upon by RPs and IdPs to obtain lawful consent which may be required for purposes outside of authentication. Where RPs and IdPs would require consent for additional data processing purposes, for example marketing, there is no facility within the dialogue box which would be capable of capturing valid consent. However, it is probable that some RPs, and potentially IdPs, might attempt to utilise these links to fulfil their transparency requirements when seeking consent for purposes outside of authentication. We expressed concerns to Google that the current UX design may lead to unlawful processing – ie. without valid consent. In its most recent response, Google has not addressed our concern that the design of the FedCM UI may incorporate 'harmful nudges'. This concern could be resolved by removing the difference in salience between the two buttons (ie by making sure that any highlighting of the buttons is the same) and by making the text size of links the same size as that in the main body of text. We are continuing to discuss this issue with Google.
The FedCM user controls page	We expressed concerns that the FedCM user toggle on the settings page does not have any accompanying text explaining (1) the purpose of the API,

Potential concerns	The CMA's assessment including the ICO's feedback
within Chrome settings does not provide any information on the purpose of the API.	(2) the potential implications of third-party sign-in beyond verification (eg advertising purposes) and (3) the fact that it is up to RPs and IdPs to collect consent for user data processing for purposes outside of authentication. Given this fundamental lack of information on point (2), Chrome users who might be interested in or concerned by the non-verification use cases of their data may not even be aware to look out for this information when providing consent. This circles back to our concern outlined above regarding the question of whether IdP prompts are collecting valid consent. Users would benefit from greater transparency on this topic and encourage Google to explore making edits to Chrome settings or the button-flow of FedCM to include a brief note on other possible use cases of FedCM. In response to this concern, Google has stated that it is undertaking some early explorative work on a range of strategies and methods aimed to improve user comprehension and knowledge when engaging with FedCM in Chrome, which we welcome.

Shared Storage API

Overview

54. 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.

55. 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.

56. The first gate is the content Selection output (Select URL) gate. This includes functionality for creative rotation of ads, A/B testing, and a limited ability to provide trust signals (although Google has 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.

Assessment

57. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report

was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
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.	There have been no significant updates on this issue. Under the governance framework, the proposed annual reporting on cross-site tracking risks on Privacy Sandbox on Chrome provides a formal mechanism for Google to collate information on these risks and use that information to inform decisions on changes to the Shared Storage API. Subject to this governance framework working effectively, this has the potential to manage the risk of the Shared Storage API being deployed without a number of key technical privacy controls in place. Particularly while key controls are missing, parties using the Shared Storage API are responsible for their data protection compliance. The ICO retains its independence to take regulatory action where non-compliance is identified.
Key controls, such as epsilon values and rate limits, have not been tested.	For the Private Aggregation API, as with ARA, we understand that key controls (eg epsilon values and contribution budgets) have been initially set as	Google proposes to monitor cross-site tracking risk under its proposed governance framework described in paragraph 14 above. We consider that annual reporting and review provide an

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	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 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.	opportunity to assess whether the privacy controls (eg rate limits and epsilon values) are working as intended. We also note that changes to third-party cookie availability under Google's revised approach to the Privacy Sandbox could change the effectiveness of key controls designed for a third-party cookie deprecation scenario. Our current view is that the governance framework, if applied effectively, could resolve this issue.
Future 'gates' may be added to the Shared Storage API, and this may change the risk profile of the API and potentially wider Privacy Sandbox Proposals.	We understand that, in the future, additional output gates may be added to the Shared Storage API (eg 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.	As in the rows above, our view is that Google's governance framework, if applied effectively, could resolve this issue, as it could ensure that any impact of changes intended to improve functionality was considered with reference to all of the D&I criteria.

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	We await further information from Google and will consider this as part of our wider work looking at governance and future decision-making.	
Data may be stored longer than is necessary.	No updates in this previous reporting window.	In the original design of this API, each key stored was cleared after 30 days of the last write. Following ecosystem feedback on critical use cases, this expiry limit was changed to expire 30 days following the last update. Based on this change, we are concerned that, for API callers with significant reach across frequently visited sites, personal data processed and stored via the Shared Storage API will persist well beyond the 30-day limit. In response to this concern, Google has tentatively suggested that excessive extension of the Shared Storage API storage can be monitored as part of an ongoing program of governance that can include metrics collected by the Chrome browser. This data would inform the wider privacy review Google has committed to in order to ensure continuous improvements in the privacy standards of the Privacy Sandbox tools. Subject to the governance framework working effectively, this issue could be resolved.

58. 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**.

59. We do not currently have any concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**, noting that Shared Storage is primarily used to support or extend other Privacy Sandbox APIs or as a general use API. We expect that future changes (eg a decision to add

new output gates) would be considered under the governance process that Google has outlined.

60. We have consulted with the ICO regarding the application of **D&I D – User experience** and set out our assessment in the table below. The CMA's assessment below includes the ICO's feedback.

Potential concerns	**The CMA's assessment including the ICO's feedback**
The Shared Storage UI does not sufficiently explain all the potential use cases of the API.	We expressed concerns to Google that the current Shared Storage API UI lacks transparency for users. We understand that the API has purposes wider than just ad personalisation and measurement, for example the trust signal functionality of the SelectURL gate. Google has said that the existing language for the Shared Storage API is broad enough to capture the range of use cases. Google has also conducted UX research to test new language in the PA API prompt (as Shared Storage is tied to the PA API control for Select URL), which was associated with increases in overall comprehension scores, and plans on making further language iterations to improve user comprehension regarding potential use cases of the API. We welcome these further revisions and will consider this issue to be resolved when the further iterations are implemented.

Cookies Having Independent Partitioned State

Overview

61. Cookies Having Independent Partitioned State (**CHIPS**) is intended to support the embedding of third-party services within webpages without re-enabling cross-site tracking.[71] 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.[72] Parties who set partitioned cookies on separate webpages are not able to join up this information.

62. 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;

[71] For an overview of the CHIPS proposal, see Chrome Developer Blog, 'CHIPS', 15 December 2023 (accessed on 10 November 2024).
[72] 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'.

(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.

63. Other browsers have considered measures to address these use cases. In addition to blocking third-party cookies from known trackers by default, Firefox has now enabled CHIPS by default for all users, while Safari previously attempted to partition based on heuristics before instead blocking all third-party cookies. Safari (WebKit) has also begun implementation of a feature to support CHIPS.[73]

64. 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 where the discussion appears to focus on performance and memory rather than security or privacy concerns.[74]

Assessment

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

66. The CMA does not currently have any concerns under **D&I B – Digital advertising, D&I C – Impact on publishers and advertisers** and **D&I D – User experience** and we do not currently have any outstanding concerns. We set out our updated assessment of each of the issues we previously identified in **Appendix 2**.

Fenced Frames

Overview

67. 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 API 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.[75]

---

[73] See 'Add a feature flag for supporting partitioned cookies' on the WebKit repository on GitHub (accessed on 10 November 2024).
[74] See for example, Issue #66 on the 'CHIPS' repository on GitHub (accessed on 10 November 2024).
[75] For an overview of the timelines, see Chrome Developer Blog, 'Status of pending Protected Audience API capabilities', 9 February 2023 (accessed on 10 November 2024).

68. 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 API 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.

Assessment

69. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
Outstanding cross-site tracking risks remain unmitigated.	We note that the Fenced Frames proposal currently maintains a range of unmitigated cross-site tracking risks.[76] 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. Once we receive further updates on how Google is planning to address these risks, we will consider whether our concerns have been resolved.	Following an update in April 2024, Google has stated that it is actively working on possible mitigations to known potential cross-site tracking vulnerabilities with the Fenced Frames proposal. Google has said that these improvements will be introduced incrementally and there is currently no concrete timeline available for mitigations to these risks. The reporting on risks to privacy from cross-site tracking under the governance framework provides a formal mechanism for Google to collate information on these risks to inform decisions on future privacy improvements and associated timelines for implementation. Therefore, subject to the governance framework working effectively, this issue could be resolved.

[76] See 'Privacy considerations' within the 'Fenced Frames Explainer' on 'Fenced Frames' repository on GitHub (accessed on 10 November 2024).

70. The CMA does not currently have any outstanding concerns under **D&I B – Digital advertising** and **D&I C –** Impact **on publishers and advertisers**. In **Appendix 2**, we include our updated assessment of each of the issues previously identified.

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

Fighting spam and fraud on the web

Private State Tokens

Overview

72. 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.[77] 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.

73. 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.

Assessment

74. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report

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

was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
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.[78] • 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	In April 2024, Google confirmed that it was exploring updates to the PST Issuer registration process and the introduction of new fields for completion. These new fields intend to contain more information on the purpose of the Issuer's use of the API, and the Issuer's privacy policy. Further, Google is exploring how to make sure certain information in these fields is transparent to Chrome users. These plans include: links to a 'learn more' page, clarifications regarding the relationship between issuers and sites, and increasing visibility of information contained in the Issuer JSON. Additional research is also planned to further clarify to users which PSTs are active on a particular site. In May 2024, Google provided an update on changes it is making to Privacy Sandbox Privacy-related Compliance FAQs. Relevant to this concern, Google states that Google will refer token issuers to Privacy Sandbox compliance guidance that will contain information regarding transparency, fairness and consent requirements. Additionally, Google intends to review PST registration guidance to include more detail on the information that is required in the submission process. In particular, further detail will be documented regarding expected / standard purposes for PST Issuers.

[78] For record of Private State Tokens issuers, see 'PST issuers' on the 'PST' repository on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	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.	We welcome the progress that has been made. This issue could be resolved, pending Google taking forward its planned actions to increase users' visibility of information on the purposes for which their PST data may be used.
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.	In April 2024, to address these concerns, Google stated that it planned to update both its Privacy Sandbox and PST Issuer guidance to highlight the need for Issuers to be transparent regarding their purposes. In addition, Google said that both the checks undertaken by its engineers on initial registration, alongside the technical constraints of the API, reduced the likelihood of misuse outside the intended purposes. In May 2024, Google provided an update on changes it is making to Privacy Sandbox Privacy-related Compliance FAQs. Relevant to this concern, Google has said that it will refer token issuers to Privacy Sandbox compliance guidance that will contain information regarding transparency, fairness and consent requirements. In particular, Google plans to add information to the Issuer registration form that highlights the need to consider PECR/ePrivacy requirements and whether exemptions may, or may not, apply. All the updates above are positive and welcome. The proposed reporting on privacy risks under the proposed governance framework provides a formal mechanism for Google to collate

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	Google has agreed to make it clearer that PSTs are 'not intended to convey arbitrary cross-site information'.[79] 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.	information on these risks and use that information to inform decisions on changes to PST. Therefore, subject to the governance framework working effectively to detect and mitigate misuse of PST, this issue could be resolved.

75. We do not currently have any outstanding concerns under **D&I B – Digital advertising and D&I C – Impact on publishers and advertisers**. In **Appendix 2**, we include our updated assessment of each of the concerns previously identified based on further submissions from Google and other market participants since our last report was published in April 2024.

76. We have consulted the ICO regarding the application of **D&I D – User experience** and note that we have no outstanding concerns with respect to PST.

Limiting covert tracking

Bounce Tracking Mitigations

Overview

77. 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 (eg sets a cookie, accesses local storage, and so on) and redirects the user again either back to Site A or to another site.

78. 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

[79] See 'Motivation' within the 'Private State Token API Explainer' on the 'Private State Tokens' repository on GitHub (accessed on 10 November 2024).

above) within the last 45 days, the 'stateful bounce' will be allowed, otherwise the state (eg the cookie set by Site B in our example) will be deleted.

79. 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.[80] 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.[81]

80. Third-party cookies can be used to achieve the same result as bounce tracking. Therefore, BTM only adds value when third-party cookies are disabled. Google enabled BTM by default in October 2023 for users who have blocked third-party cookies.[82]

Assessment

81. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
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.	See D&I B below.

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

[80] For an overview, see 'Out-of-scope use cases' on Chrome Developer Blog, 'Bounce tracking mitigations', 16 July 2024 (accessed on 10 November 2024).
[81] See Issue #24 on the 'Navigation-based Tracking Mitigations' repository on GitHub (accessed on 10 November 2024).
[82] See Chrome Developer Blog, 'Bounce tracking mitigations', 17 June 2024 (accessed on 10 November 2024)

table below, we include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
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. 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.	Google has informed us that providing stakeholders with a cross-site identifier or similar browser surface area risks undoing the user privacy gains that Privacy Sandbox seeks to deliver. Google therefore proposes to evaluate stakeholder proposals under its governance model. Our view is that Google's governance framework, if implemented effectively, could resolve this issue.
Sites that are regularly visited by users (ie 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 (eg login and payments).	Google has said that BTM 'by itself is not a complete solution and must work with other proposals to constrain sites with significant first-party activity'.[83] Google has proposed some options to address this, which we expect to be captured under the governance framework. On the basis that Google will continue to work with stakeholders to improve the solution in line with its governance framework, we consider this issue could be resolved.

83. We have consulted the ICO regarding 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.

[83] See 'Bounce Tracking Mitigations Explainer' on the 'Bounce Tracking Mitigations' repository on GitHub (accessed on 10 November 2024).

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

Overview

84. 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 (eg device model) rather than passively receive them.

85. **IP Protection** is a proposed privacy feature in Chrome that aims to avoid sharing a user's real IP address with third parties. The proposal involves using a privacy proxy to anonymise users' IP addresses.[84] 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 third-party domains embedded in a 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 destination site. Google has announced plans to 'introduce IP Protection into Chrome's Incognito mode'.[85]

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

87. A browser's network resources, such as connections, DNS cache, and alternative service data is 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.

[84] See the 'IP Protection' repository on GitHub (accessed on 10 November 2024).
[85] See 'A new path for Privacy Sandbox on the web', 22 July 2024 (accessed on 10 November 2024)

Assessment

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

88. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
Third party scripts are able to access all high-entropy client hints by default.	New concern identified after April 2024 Report.	The UA-CH proposal seeks to introduce a privacy improving way of providing information previously made available in the User-Agent string. Central to this improvement is the ability of sites to be able to limit third party access to high-entropy values. Currently, however, we are concerned that third-party scripts in the first-party domain are able to access all high-entropy client hints by default. In response to this concern, Google has agreed that a solution to prevent or reduce the amount of high-entropy client hints collected by third-party scripts would be beneficial. We await updates from Google.

89. 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**. We do not currently have concerns about UA-CH/UAR under D&I B and C. We expect that changes in future (eg a decision to remove or limit access to critical hints) would be taken under the governance process that Google has described.

90. 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*

91. After consulting with the ICO, we have considered the following potential concerns under **D&I A – Privacy outcomes**. In the table below, we include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
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.	We are working with Google to better understand the implications of its decision to introduce IP Protection in Incognito mode.

92. Based on stakeholder feedback and our own analysis of BTM, 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 include our assessment of each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024. We note that Google's decision to introduce IP Protection in Incognito mode significantly reduces IP Protection's scope. We consider that any scope changes, eg introducing IP Protection in default browsing, would be covered under Google's proposed approach to governance described in 14 above.

Potential concerns	**The CMA's views in the April 2024 report**	**The CMA's assessment**
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, especially regarding the final form, or source, of this list.	Google proposes to implement a list-based approach. IP Protection would only impact domains on the list in a third-party context. Google has said that it will 'explore using methods similar to other browsers, including using lists

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
		that identify these third parties'.[86] As with other elements of the Privacy Sandbox, we consider that Google's discretion in determining which parties appear on the list could create risks to competition. Our discussions with Google on the list-based approach are ongoing. For example, we are exploring whether it could be appropriate for Google to rely on an existing list (eg Firefox relies on the Disconnect.me list[87]) or what role an improved governance framework could play in mitigating any risks from Google's discretion.

- *Storage Partitioning and Network Partitioning*

93. **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.

Engagement with market participants

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

95. 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

[86] See 'Cross-site tracking and the role of IP addresses' in the IP Protection repository on GitHub (accessed on 10 November 2024).
[87] See 'Firefox Now Available with Enhanced Tracking Protection by Default Plus Updates to Facebook Container, Firefox Monitor and Lockwise ' on Mozilla blogs, 4 June 2019 (accessed on 10 November 2024).

views and suggestions, as summarised in Google's 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.

96. We received feedback from a number of stakeholders over Q2 and Q3 2024. Concerns that have been raised are largely in areas we were already working on and we have engaged with Google to resolve these issues. The concerns that have come to us have been shared with Google in a confidential manner. This process has directly informed our role in overseeing the design and implementation of the Privacy Sandbox proposals.

97. Details of the concerns raised by the market participants relating to the specific APIs have been included in the relevant sections above.

98. We also received feedback from a range of stakeholders in response to our call for input, which we issued following Google's announcement in July 2024 relating to the introduction of its revised approach to the Privacy Sandbox. Overall, industry stakeholders (particularly ad tech and publisher groups) were almost unanimously of the opinion that competition concerns remain, and that we should continue to oversee Google's new approach.

99. We also received a small number of responses mainly from individuals arguing that Google should revert to full removal of third-party cookies from Chrome to prevent the sharing of user data with third parties. This reflects the wider interactions between competition and privacy considerations which are an important aspect of this case.

Contact details

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

CMA: privacysandbox@cma.gov.uk; ioanna.batzoglou@cma.gov.uk angela.nissyrios@cma.gov.uk; and tania.vandenbrande@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.

Appendix 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 tools that does not rely on third-party cookies:

   (a) Attribution Reporting

   (b) Private Aggregation API

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)

Appendix 2 – issues concerning Privacy Sandbox tools that have been resolved

12. This appendix is organised by the function or use case that the Privacy Sandbox tools are intended to serve, and within each use case, by the specific Privacy Sandbox tool or API. A summary of the relevant use cases is included in **Appendix 1**.

13. Since publishing our last update report in April 2024, we have continued to make progress in resolving issues related to the individual Privacy Sandbox tools. Google will need to continue to resolve these issues as the Privacy Sandbox tools will remain important for the ad tech ecosystem to target and measure advertising for the proportion of traffic where third-party cookies are unavailable under Google's revised approach. In the section below, we outline the issues that we have identified and resolved for each of the tools and APIs based on the Commitments framework (**D&I A – Privacy outcomes**, **D&I B – Digital advertising**, **D&I C – Impact on publishers and advertisers** and **D&I D – User experience**).

14. The CMA's assessment below incorporates the ICO's feedback on the privacy and data protection impacts of the Privacy Sandbox. The ICO has been closely involved in this process, given that the aim is to ensure that both competition and privacy are protected. We have consulted with the ICO primarily in relation to **D&I A – Privacy outcomes** and **D&I D – User experience**.

15. In some areas, there continues to be a risk that parties and Google may use the Privacy Sandbox tools in a way that is not in compliance with Applicable Data Protection Legislation leading to ongoing risks for privacy outcomes. In most cases concerning compliance with this legislation, the responsibility lies with the parties using the Privacy Sandbox tools. Resolving these risks of noncompliance by parties through technical changes to the Privacy Sandbox tools has had to be balanced against the potential for distortions to competition arising from Google's plans with respect to the availability of third-party cookies in the Chrome browser.

16. The ICO will monitor how the industry responds to Google's revised approach to Privacy Sandbox and retains its independence to take regulatory action against all parties where non-compliance is identified, including by Google and organisations that use the Privacy Sandbox tools.[88]

---

[88] See ICO statement in response to Google announcing it will no longer block third party cookies in Chrome (Accessed on 10 November 2024).

Showing relevant content and ads

Topics API

17. After consulting with the ICO, we considered the following potential issues under **D&I A – Privacy outcomes**. We have assessed each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
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[89] 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, Google is now exploring ways to monitor potential abuse of the API.	Google's Privacy compliance FAQs state that '[s]ites and their vendors will need to decide what a user's choice means in terms of whether and how a given Privacy Sandbox API is used'.[90] Google's EU user consent policy also states that '[w]hen using Privacy Sandbox APIs, (topics, protected audience and attribution reporting), you may be using personal data for ads personalisation and/or accessing local storage. The EU user consent policy requires you to obtain valid user consent for these actions in the same way as you rely on consent today for ads personalisation and the use of non-essential local storage to the extent legally required'.[91] In September 2024, Google provided an update to the Topics consent UX. Google now informs users, within a dropdown menu, that Topics data can be used by parties for wider purposes and combined with wider data. While Google's efforts adding clarity to API callers in their guidance, and their clarification

[89] See the 2021 Opinion, page 44.
[90] See Google's 'Privacy compliance FAQs', 6 December 2023 (accessed on 10 November 2024).
[91] See Google's 'Help with the EU user consent policy', 31 October 2019 (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	Once we receive further updates from Google on these assurances, we will consider, after consulting with the ICO, whether our concerns have been resolved.	on purposes to users in their consent notice, are welcome, risks relating to purpose limitation remain. The burden remains on the parties processing the Topics data to comply with Applicable Data Protection Legislation, although Google retains accountability as a controller for topic generation. The ICO retains its independence to take regulatory action where non-compliance is identified.
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 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.[92] The ICO has also noted that solutions should avoid 'augmenting, matching or combining personal data without strong justification, transparency and control'.[93] Although the chosen epoch period may provide a proportionate storage limitation limit for topics data where it is	Google's Privacy compliance FAQs also state that '[s]ites and other API callers will need to determine if their current mechanisms for deletion rights are suitable if and when they have chosen to store data retrieved from Privacy Sandbox APIs or data related to calling the APIs'.[94] We also note that Google's attestation requires API callers to agree that they will not use the APIs to conduct cross-site identity joins or otherwise circumvent the privacy protections built into the APIs.[95] Google recently introduced a new change where each epoch expires after a longer fixed interval (between 26 and 28 days), while still exposing only the most recent three epochs to API callers. This was done to add a slight delay of 0 to 2 days on the epoch calculations, making it harder to correlate the same user across sites via the time that topics are changed.

[92] See the 2021 Opinion, page 45.
[93] See the 2021 Opinion, page 45.
[94] See Google's, 'Privacy compliance FAQs', 6 December 2023 (accessed on 10 November 2024).
[95] See 'Privacy Sandbox enrolment attestation model', 2 April 2024 (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	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.	Taken together, the requirements on API callers under Applicable Data Protection Legislation, the attestation requirement and randomised epoch calculations can reduce the risk that ad techs attempt to re-identify users by accumulating topics beyond the three-week epoch. It remains the case that there are no technical limitations preventing parties from storing the topics beyond the period specified in the Topics consent screen. As mentioned above, API callers are responsible for their data protection compliance. The ICO retains its independence to take regulatory action where non-compliance is identified.

18. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
The Topics API is likely to disadvantage small ad techs who have a more limited 'reach' and access to targeting information	We received stakeholder feedback that the Topics API disadvantages small ad techs, and that GAM will have broader information about user topics compared to competitors because it is embedded on most sites. We consider that the impact of this concern will vary based on the degree to which an ad tech relies on the Topics API as a targeting signal.	Since the publication of our last report, we have received further feedback from stakeholders who are concerned that the ability to read topics is contingent on being able to embed code on the sites that a user interacts with. For many stakeholders, this will necessitate additional cooperation

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
compared to large ad techs.	Our understanding is that ad techs can supplement or substitute topics data with other signals. Examples may include contextual information from webpages or user information obtained from data sharing arrangements, data on logged in users or from Protected Audience interest group membership. Our view is that 'reach' or unequal access to data is neither a new problem nor is it specific to Privacy Sandbox. At present, ad techs with a larger reach already have more opportunities to use third-party cookies. 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. 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.	between publishers and buyers when observing users' topics. However, this obstacle does not affect GAM and other large ad techs to the same extent, as it is able to access the first party context of all the sites it is integrated with. Our view is that unequal access to data due to differences in integration is not a new problem. When compared to the status quo, it unlikely that small players will be disadvantaged directly as a result of the introduction of the Topics API. In the absence of further stakeholder feedback, we consider this issue resolved.
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 responded to feedback about the risk and impact of misclassification in previous quarterly reports.[96] We agree with Google's view that allowing site owners to control classification risks incentivising site owners to game the system. We received further feedback from stakeholders requesting 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 relayed these suggestions to Google.	Google has informed us that investing in a mechanism to address misclassification would likely require significant resources due to the anticipated volume of requests and potential for abuse. Regarding the request for transparency, Google said that anyone can access its database and see the topic assigned to their site by using the chrome://chrome-internals tool in the Chrome web browser. Google informed us that the classification model was based on input received from hundreds of human raters, who evaluated thousands of websites and assigned them into the Topics taxonomy. Google used this data to directly classify sites into topics (in the case of the top 50k global sites) and to train the on-device machine learning model which classifies all other websites.

[96] See Google's Q2 2023 and Q3 2022 progress reports (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
		We maintain our view that Google's approach to classification is appropriate in balancing the utility of the Topics API against the risk of abuse. We also consider that the level of transparency is appropriate. In the absence of further stakeholder feedback, we consider this issue resolved.
Allowing sites to selectively contribute to a user's topics could create a free-riding problem (ie that some ad techs can choose to observe topics without contributing to the set of topics stored on the user's device).	We are aware of specific stakeholder concerns relating to SSP 'free riding'.[97] We have raised the concern with Google and Google responded 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 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 (eg 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.	We have received further feedback from stakeholders requesting an additional attestation that would require the caller to declare that they will take commercially reasonable measures to require that the URL of the web page is reported to the advertiser.[98] In response to this request, Google informed us that the enrolment and attestation process is designed to protect user privacy. An attestation, such as that requested by the stakeholder, would serve commercial purposes that are not a matter for the Topics API attestation. Rather, this can be agreed directly between API callers and advertisers should they wish to do so. We agree with Google's view that this type of information transfer should be agreed directly between API callers and advertisers. We therefore consider this issue resolved.
The one-week epoch means that topics are likely to be out of date, with implications for showing ads	Although reducing the epoch length could increase utility for advertisers, it would likely have a negative impact on privacy. Our understanding is that Google defined the Topics epoch after assessing the risk of re-identification. We therefore consider	In the absence of further stakeholder feedback, we consider this issue resolved.

[97] See Issue #92 on the 'Topics' repository on GitHub (accessed on 10 November 2024).
[98] See Issue #266 on the 'Topics' repository on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
where the user may already have acted on their interest (eg by making a purchase).	an epoch of one week to be appropriate.	
Classification based only on hostname means that sites covering many topics contribute less useful information than niche sites. For example, YouTube is assigned 'Online Communities', 'TV & Video' and 'Arts & Entertainment'.	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 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.[99] 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.	We have continued to receive feedback from stakeholders requesting an opt-in mechanism that allows the classification model to be trained on page title or body in addition to hostname. We have shared this feedback with Google and note ongoing public discussions on this issue. Our view remains that classification based on hostnames is a reasonable trade-off to achieve Google's stated aim to improve privacy outcomes for users. We recognise that the types of information available to the classifier could change in the future. Google's proposed governance model includes an approach to considering the D&I criteria and balancing alignment with privacy goals with utility for the ad tech ecosystem. The governance process would apply to future changes to the classifier model (eg expanding it to consider other information about a page).

19. We have consulted with the ICO regarding the application of **D&I D – User experience** and consider the following issues to be resolved. The CMA's assessment below includes the ICO's feedback.

Potential concerns	The CMA's assessment including the ICO's feedback
From the sequencing of the initial Topics, PA API, and ARA prompt, users do not understand that these are three different APIs.	We expressed concern to Google that the close sequencing of the prompts for the Topics, PA, and ARA APIs is impacting user comprehension of the fact that the prompts are informing them of three distinct features. On this point, Google's own UX research shows that users struggle to identify that the initial Topics, PA API, and ARA prompts are providing information about three different APIs. In response to this finding and our concern, Google conducted further testing with updated Topics, PA API, and ARA prompts, specifically targeting user comprehension of the separate nature of the three APIs as one of its behavioural outcome metrics.

[99] See for example, Issue #224 on the 'Topics' repository on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's assessment including the ICO's feedback
	This new UX research showed that average clarity ratings for the API screens were significantly greater than the midpoint of the scale in response to the question 'How clear is it to you that the two screens above describe three ad privacy features'. While we would have more confidence in the results if Google probed user clarity using a metric that targeted actual (as opposed to self-reported) comprehension, we welcome this research and consider this issue resolved. We recommend that Google avoid the use of leading questions in future, to increase the robustness of its research results.
Users are not able to access the full Topics hierarchy.	Users who are looking to explore (and potentially block) the topics they have been assigned currently have no means to explore the full hierarchy of topics in their settings. From a review of Google's research on the topic blocking feature, we support Google's own recommendation that users are provided with the means to explore the full topics hierarchy. However, this recommendation suggested that the subtopics should not be shown to users as part of the Topics API setting page UI. The number of subtopics would be useful information for users to aid informed decisions about whether to block any topic(s). In response to our concern, we received further information from Google, showing that users are now able to see all top-level topics and respective sub-level topics examples as part of the 'Manage topics' feature in Chrome settings. This should allow for users to explore and block topics based on their preferences. Google has confirmed that it has explored providing the full taxonomy of topics in the settings but believe that this would be overwhelming for users and would not help their decision-making. Google also does not have existing UX design patterns that can display this volume of information. Instead, the full taxonomy of topics can be accessed by clicking on 'Learn more' in the 'Manage topics' settings page in Chrome. Clicking this link will bring users to a help centre article, where a link to the full taxonomy can be found in the 'Manage ad topics' drop-down. Our view is that this solution should allow users to explore the full taxonomy of topics while taking into consideration the technical limitations of displaying this information and the desire to not overwhelm users with information. Therefore, we consider this issue to be resolved.

Protected Audience API

20. For our updated assessment of the outstanding issues relating to **D&I A – Privacy outcomes**, see the main body of the report above.

21. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

PA API Concerns

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
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.	We recognise that 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. 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. Google responded to the traffic shaping concerns by recommending SSPs use caching or DSPs make increased use of Trusted Key/Value servers to address these use cases.[100] Subsequent stakeholder feedback highlighted that caching is complex to implement, creates SSP dependency and hides the 'true' shape of traffic from DSPs, requesting to expose IG origins to the supplier instead.[101] We have shared this feedback with Google and await its response.	We acknowledge that at present traffic shaping relies on third-party cookie-syncing, allowing DSPs to receive only 'matched traffic' reducing server costs. Google notes potential fingerprinting concerns if this capability were to be implemented within the PA API (ie disclosure to SSPs whether individual DSPs have IGs present). Google acknowledges that reducing cross-site identifiers impacts traffic shaping techniques that rely on those identifiers. Google also maintains that caching, contextual-based filtering and using Private Aggregation to understand DSP preferences are workable solutions.[102] Discussions are ongoing on options in addition to the above. For example, whether a noised list of DSPs with at least one IG on the device would provide helpful information for SSPs while maintaining privacy outcomes.[103] We consider that the limitations on traffic shaping based on third-party cookie synching will apply equally to all ad techs and therefore is not a distortion in competition. We recognise that the impact across ad techs may be different (ie that ad techs with a greater query per second capacity may be less affected).
PA API does not currently support effective IG delegation (ie where one party assigns a	Google believes that its implementation accommodates all use cases and states that it	Google has repeated its view that PA API currently supports contract-based approaches to

[100] See Google's Q3 2023 progress report, page 10 (accessed on 10 November 2024).
[101] See Issue #951 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[102] See Google, 'Privacy Sandbox relevance and measurement FAQs', 14 August 2024 (accessed on 10 November 2024).
[103] See, for example, Issues #951 and #1213 on the 'Protected Audience API' repository on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
user to an IG and allows another party to bid on that IG in a PA API auction).	should 'build additional support to make some use cases flow more smoothly in the future'.[104] We have raised the issue with Google and are seeking clarification on the timeline.	IG delegation. As stated in the D&I A section above, IG delegation should be transparent to the user. In the absence of further stakeholder feedback, we consider this issue resolved.
PA API 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 API does not support this type of ad targeting, and that combining IGs is incompatible with PA API's current privacy model.[105] We currently agree with the approach to restricting remarketing and other custom audience use cases to one IG and have discussed our assessment of privacy issues (D&I A) in relation to the PA API privacy model. 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 (eg those owned by Google) to work around the restrictions in PA API.[106]	Google has reiterated that PA API will not support combining IGs during bidding or any other use case, due to privacy implications. The 'joint buying/selling logic' use case proposed in the April 2024 report would separate bidding and creative selection between the DSP and ad server to improve multi-party collaborative decision-making within each IG only.[107] Our view remains unchanged. We consider that restricting remarketing to one IG can improve privacy outcomes for users under D&I A. In the absence of further stakeholder feedback, we consider the potential concern on bidding on combinations of IGs resolved. We are aware of proposals to enable privacy-preserving IG combinations, for example suggestions from Prebid[108] and Microsoft in the context of their Ad Selection API.[109] Google's proposed governance framework could allow changes to support combining IGs, if an acceptable solution in privacy terms emerges. Since our last report, stakeholders have also raised concerns that parties such as

[104] See 'Publisher Interest Group Control' in Google's Q3 2023 feedback report (accessed on 10 November 2024).
[105] See Issue #818 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[106] See Issue #1028 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[107] See Issue #1028 on the 'FLEDGE' repository on GitHub (accessed on 10 November 2024).
[108] See Prebid's 'alternative solution' raised by stakeholders on Issue #1028 on the 'PA API' repository on GitHub (accessed on 10 November 2024); Or, see Issue #937 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[109] See for example, 'API difference highlights' on the 'Privacy preserving ads' repository on GitHub and Microsoft's Issue #59 on the 'Privacy preserving ads' repository on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
		Google may possess greater first-party data volumes and have the capacity to accommodate more data within a single IG. Google has said that IGs are 'subject to limits needed to bound resource utilisation on the user's device'. [110] We understand that these limits apply equally to all IG owners, including Google. Google is also subject to limits on its use of first party data under section G of the Commitments. Therefore, in the absence of further stakeholder feedback, we consider this issue resolved.
PA API auctions allow one ad auction per placement slot and each slot is treated independently. This creates challenges of competitive ad separation (ie. ensuring that ads for competing brands do not appear in ad slots on the same page).	We recognise that competitor ad separation could have contractual and revenue implications for the ad tech ecosystem and are aware that other browser vendors have proposed implementations that allow for coordinated ad placement via multi-tag support in the scoreAds function.[111] Stakeholders have suggested adding 'whole page'[112] or 'multi-tag'[113] auctions to PA API. Google has identified increased complexity and privacy risks associated with this feature, and therefore advise that direct sold ad serving by the publisher is the only reliable method for ensuring competitor ad separation.[114]	Google has reiterated the privacy and complexity considerations associated with multi-tag or multi-slot auctions in PA API but stated that it is open to further stakeholder discussion.[115] We agree with this approach and highlight that Google's proposed governance framework could allow changes to support multi-tag auctions, if an acceptable solution in privacy terms emerges. For use cases such as competitive ad separation, Google recommends direct sold as the most reliable method.[116] There do not appear to have been discussions on alternatives since December 2023 and therefore, in the absence of stakeholder concerns, we consider this issue resolved.

[110] See 'Interest Group Attributes' on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[111] See 'API difference highlights' on the 'Privacy preserving ads' repository on GitHub (accessed on 10 November 2024).
[112] See Issue #98 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[113] See Issue #846 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[114] See 'Competitive Separation' in Google's response to the IAB Tech Lab's report (accessed on 10 November 2024).
[115] See 'Multi-Slot Private Auction' within Google's Q1 2024 Report (accessed on 10 November 2024); See 'Multi-Slot Private Auction' in Google's Q1 2024 Report (accessed on 10 November 2024).
[116] See Issue #773 on the 'PA API' repository on GitHub (accessed on 10 November 2024); See 'Competitive Ad Separation' in Google's Q1 2024 Report (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	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 API auctions offer limited support for negative targeting ie. excluding some users from seeing a particular ad.	Discussions on negative targeting capabilities in PA API 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, such as excluding an entire IG, as opposed to filtering ads within that group[117] and other alternative methods.[118] 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.	Google is seeking views on its proposed approach to negative targeting. The public discussion, including on issue #896 in the PA API repository on GitHub, suggests that Google's proposal could address stakeholder needs. [119] We do not expect PA API to provide equivalent functionality to third-party cookies and consider that Google is actively engaging with the ecosystem to identify incremental improvements to respond to stakeholder requests.
URLs for loading scripts into PA API 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.[120]	Google has implemented the required design changes.[121] In the absence of further stakeholder feedback, we consider this issue resolved.

PA API Services Concerns

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
Moving processing to the device can raise concerns	Our understanding is that Chrome uses separate	In the absence of further stakeholder feedback on the

[117] See Issue #896 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[118] See Issue #1096 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[119] See Google's comment on Issue #896 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[120] See Issue #818 on the 'PA API' repository on GitHub (accessed on 10 November 2024).
[121] See Issue #818 on the 'PA API' repository on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
about overall page or device performance, with implications for search engine optimisation and UX.	worklets for the PA API auction and page rendering. This allows page rendering to complete before the PA API 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.	search engine optimisation point, we consider it resolved.
Fenced Frames restricts available ad formats. They do not currently support (1) native such as dynamic ad sizing and (2) video, such as transmitting signals from video players.	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 and transmitting signals from video players as specific concerns. 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.[122] 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	Google has confirmed its commitment to ensuring support for major ad formats before enforcing a requirement for Fenced Frame rendering.[124] Our understanding is that a decision to enforce Fenced Frames would be taken under Google's proposed governance framework, which includes elements of stakeholder consultation and considers the impact on the D&I criteria. We also note that discussion on design requirements for Fenced Frames are ongoing (eg with GitHub discussions on VAST, passing rendering signals, diversity filtering or multi-result auctions).[125] In the absence of further stakeholder feedback, we consider this issue resolved.

[122] See Issues #741 and #311 on the 'PA API' repository on GitHub (accessed on 10 November 2024). On how the one ad-size is decided, see Issue #908; on the possibility of enabling multi-sized PA auction output, see Issue #825; and on implementing an additional Ad-Slot Size signal, see Issue #869; all on the 'PA API' repository on GitHub (all accessed on 10 November 2024).
[124] For more information, see 'API Improvement' on Google's Q1 2024 feedback report (accessed on 10 November 2024).
[125] See Issues #741, #1074 and #1199 on the 'PA API' repository on GitHub (all accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	walled gardens and potentially diminishing the overall UX. 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 handling VAST in PA API using iframes.[123] We would welcome further industry feedback on the extent to which this resolves this concern.	
PA API auction design shifts data flows that were previously server to server onto the device. This raises concerns about transparency, and contractual issues (eg 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. 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,[126] as these tools are inherent to the browser and developers independently determine their usage.	Since the publication of our last report, stakeholders highlight their dependency on Google to ensure coverage for potential outages to maintain uninterrupted ad delivery when using the PA API and express concern about the risk associated with the lack of a contractual or service level agreement with Google.[127] The number of stakeholders raising this concern has increased since the outage affecting the APIs in late May 2024. Google has explained that a misconfiguration in the Chrome-facilitated testing setup impacted API availability for browsers that restarted during the relevant period. Google reassured the market that the disruption was unique to the Chrome-facilitated testing setup.[128] We acknowledge that, while no direct contractual relationship with Google exists, stakeholders can inspect the Chromium source code and monitor the development of

[123] See 'Instream video ad in a Protected Audience sequential auction setup' demo (accessed on 10 November 2024).
[126] See 'Data Guarantees' in Google's response to the IAB Tech Lab's report (accessed on 10 November 2024).
[127] See 'Data Guarantees' in Google's response to the IAB Tech Lab's report (accessed on 10 November 2024).
[128] See 'PSA - Privacy Sandbox APIs temporarily unavailable; fix deployed', 22 May 2024 (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
		ongoing debugging tools.[129] The governance framework provides guidelines for the usage and transparency of the PA API, establishing expectations for both API callers and Google, as the architecture provider, regarding service reliability, data flow access, and accountability. Any additional concerns related to 'contractual obligations' will be addressed on a case-by-case basis within this framework. We therefore consider this issue resolved.
PA API lacks adequate authentication to verify contextual responses, Key/Value server-originated responses, bid submissions and debugging tools.	Stakeholders have raised concerns that PA API 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 API. These concerns have been raised with Google and we await its response.	Stakeholders continue to request technical guarantees to ensure PA API bids are not tampered with as well as an exhaustive debug mode to provide real-time incident detection and efficient debugging. Google has reassured us that existing anti-abuse protections in the ad ecosystem will identify any potential attacks, therefore we consider this issue resolved.

22. We have consulted with the ICO regarding the application of **D&I D – User experience** and consider the following issues to be resolved. The CMA's assessment below includes the ICO's feedback.

Potential concerns	The CMA's assessment including the ICO's feedback
It is not sufficiently clear to users when the PA API is on / active (and that it is default-on unless the user intervenes)	We have expressed concerns to Google that users are not easily able to understand whether or not the PA API is on or active. As part of our continued engagement on this concern, we have welcomed some improvements Google has made in reducing the number of sub-menus a user would need to click through to access this information. Google also undertook user comprehension testing, with the inclusion of a dedicated measure of users' ability to understand that the combined PA API/ARA prompt informs them about a change that is default-on unless the user intervenes. To note, this issue is also applicable to ARA. For brevity, it has not been repeated in the ARA section of this report.

[129] See issue #430 on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's assessment including the ICO's feedback
	Recent UX research conducted by Google reported that average clarity ratings were significantly greater than the midpoint of the scale in response to the question 'how clear is it to you that the ad privacy features described in the screen above will be turned on unless you change your settings?'. Based upon the findings of its UX research, Google has said that it has no plans to make any further changes at this time. While we welcome this research, we would have more confidence in the results if users were asked a question that did not explicitly state the default setting. We recommend that Google avoids such leading questions in future, to increase the robustness of research results, but for current purposes view this concern as having been resolved.

Measuring digital ads

Attribution Reporting API

23. After consulting with the ICO, we considered the following potential issues under **D&I A – Privacy outcomes**. We have assessed each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
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.	In July 2024, Google provided an update on its approach to navigation tracking stating that: - Navigation tracking is a lower priority in comparison to more pervasive and scalable cross site tracking techniques (eg fingerprinting). - Navigation tracking requires user interaction and results in cross site tracking between only 2 sites, limiting scale. - Addressing navigation tracking poses a significant technical challenge and would pose a high risk to legitimate use cases. Given this, Google has said that it has no current plans to restrict link decoration for ARA click events. The lack of technical limits on navigation tracking could allow API callers to combine

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
		additional cross-site data with ARA source and trigger data. API callers are responsible for their compliance with Applicable Data Protection Legislation. We consider this issue resolved with respect to Google's decision to deprioritise technical limits on navigation tracking.

24. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
Coarser measurement may make it harder for publishers to value their ad inventory.	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 expect Google's ARA to provide the same functionality as third-party cookies.	Although the results of the Chrome-facilitated testing show that restricting third-party cookies is likely to have an impact on valuing ad inventory, ARA provides some value. We continue to maintain that it is unrealistic to expect Google's ARA to provide the same functionality as third-party cookies.
Advertisers are currently able to adjust their spending on ad campaigns in real time. ARA imposes reporting delays and could lead to wasted spend	The move to flexible event reporting windows has been reflected in the technical specification[130] and also in an explainer update.[131] Our	Google has said that it does not plan to support fields for currency or OrderID because current event level reporting already meets these needs.

[130] See the technical specification on the 'ARA' repository on GitHub (accessed on 10 November 2024).
[131] See 'Flexible event-level configurations' on the 'ARA' repository on GitHub (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
that could otherwise have been reallocated.	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.	Google suggested adding the user's geographical location to the existing source_event_ID to determine currency and using de-duplication keys to avoid double counting.[132] Our overall view is that we do not expect ARA to provide the same functionality as third-party cookies. In the absence of further stakeholder feedback, we consider this issue resolved.
ARA degrades open display measurement compared with measurement capabilities on O&O ad inventory.	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.[133] Our discussions with Google on further first-party data restrictions are ongoing.	The current Commitments allow Google to use first-party data to target and measure ads on its owned and operated (O&O) inventory. We consider this issue resolved on the basis that ARA could improve privacy outcomes for users when compared with measurement based on third-party cookies. We do not require the Privacy Sandbox tools to be like for like replacements for third-party cookies. Google's decision to implement its revised approach means that third-party cookies will continue to be available for a proportion of open display traffic. Third-party cookie availability on a proportion of traffic may mitigate the impact of a degradation in measurement capability on open display inventory.
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.	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.	Google disagrees with the view that ad verification companies offer conversion verification services. Google also claims that ad techs currently rely on incomplete data sources and that available solutions provide sufficient verification capabilities.

[132] See Google's Q1 2024 Feedback Report (accessed on 10 November 2024).
[133] See the CMA's Q4 2023 update report, paragraph 27 (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	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.	Further, Google has stated, concerning verification of data processing, that there is no existing verification system in the third-party cookie environment that makes sure that measurement software has run correctly. In contrast, ARA client-side code is open-sourced and therefore anyone could write additional tests to verify if the specified ARA code is running as expected. On stakeholder concerns about contracts and liability, Google has said that web APIs such as ARA are not services, nor is Google as a browser developer a 'party' to the processing performed by API callers. Web APIs are instead client-side tools built into the browser and made available to websites (and their service providers) to use according to their needs. Google's view is that to the extent that a commercial contract is desired, it is properly between the publisher or advertiser on the one hand, and the ad tech from whom they receive services like measurement or verification on the other hand. We note that Google has published approaches to detecting invalid traffic using PSTs,[134] debugging both aggregate and event level reports[135] and has asked for feedback with no response.[136] As the same verification limitations will apply to Google using ARA on open display advertising, we consider this issue resolved.

[134] See 'Preventing invalid aggregatable reports via report verification' on the 'ARA' repository on GitHub (accessed on 10 November 2024).
[135] See under 'Optional: transitional debugging reports' on the 'ARA' repository on GitHub (accessed on 10 November 2024).
[136] See issue #710 on the ARA repository on GitHub (accessed 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
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 are aware that Microsoft has proposed implementing 'ARA with modifications for better parity with CPA billing' in Edge. We remain keen to understand implications for interoperability and efforts to improve interoperability of approaches to attribution and reporting.	Google has stated that its 'long-term goal remains an interoperable standard that browsers broadly support, and we are actively working to identify such a solution'.[137] We recognise that interoperability depends on Google being able to find consensus with other browser developers and is not entirely within Google's control. In the absence of stakeholder feedback, we consider this issue resolved.
Google limiting the number of different attributions per advertiser to eight conversion types, potentially harming advertisers who have more than eight types.	Google has introduced custom trigger data, allowing ad techs to configure trigger data values and/or cardinality. The trigger data supports up to 32 bits. ARA adds noise depending on the number of distinct trigger values, eg limiting the number of distinct trigger values with reduced noise and vice versa. We understand that discussions within Google on ARA supporting multiple reporting domains for conversions is ongoing. In the absence of further stakeholder feedback, it is likely that the change to configurable trigger data will resolve the concern about limiting trigger data to 3 bits.	In the absence of stakeholder feedback, we consider this issue resolved.
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.	Our view remains unchanged from our view in our Q1 2024 update report.[138] We continue to agree with Google that this could undermine the intended privacy model for ARA.	Google has stated in its 2024 Q1 Feedback report[139] that it does not plan to support a Transaction ID field currently as part of full flexible event-level as providing a transaction ID would undermine privacy. In the absence of stakeholder feedback, we consider this issue resolved.

[137] See Chrome Developer Blog, 'Why Chrome shipped the Attribution Reporting API', 15 December 2022 (accessed on 10 November 2024).
[138] See CMA's Q1 2024 update report, page 36 (accessed 10 November 2024)
[139] See Google's Q1 2024 Feedback Report (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
The need to seek explicit feedback from advertisers concerning modification to their commercial contracts given the changes to aggregation and attribution.	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.	Google has responded that billing is primarily done via CPM (Cost Per Mille) or CPC (Cost Per Click). Google states that CPM or CPC billing is supported via event-level reporting in the PA API. Google is aware of two scenarios where billing is based on conversions: CPA billing (Cost Per Action) and affiliate marketing. For affiliate marketing, Google's understanding is that this is overwhelmingly click-based conversions where the advertiser is paying the affiliate a percentage of sales. In these cases, affiliates can use first-party cookies for attribution and/or can utilise ARA. On CPA, Google has stated that it has heard feedback that CPA billing is not common. However, Google has resolved latency concerns for ad techs that use CPA billing. Google has recently been engaging on the use of trigger data to satisfy CPA and affiliation attribution. In the absence of stakeholder feedback, we consider this issue resolved.
Stakeholders have expressed concern that the lack of a key discovery mechanism in ARA would make aggregated reports unsuitable for their use cases.	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.	Google's attribution reporting simulation library allows ad techs to experiment with noise and simulate noisy reports. Google opened a feedback request focused on noise in summary reports on 8 June 2022. At the time of writing, this issue had no comments.[140] In the absence of stakeholder feedback, we consider this issue resolved.
Stakeholders have expressed concern that adding noise to reports will have a disproportionate impact on smaller ad techs.	We understand this concern to focus on access to reliable signals for smaller vs larger market participants. Stakeholders have noted that	In the absence of stakeholder feedback, we consider this issue resolved.

[140] See Issue #485 on the 'ARA' repository on GitHub (accessed on 10 November 2024)

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	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.	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 event-level reports with summary reports to reduce the impact of noise and to meet stakeholders' manual and automatic optimisation needs.	In the absence of stakeholder feedback, we consider this issue resolved.

25. We have consulted with the ICO regarding the application of **D&I D – User experience** and consider the following issue to be resolved. The CMA's assessment below includes the ICO's feedback.

Potential concerns	The CMA's assessment including the ICO's feedback
Positive framing on the ARA settings page can make it more difficult for users to make informed	The ICO-CMA joint paper on Harmful Design in Digital Markets describes biased framing as 'the practice of presenting choices in a way that emphasises the supposed benefits or positive outcomes of a particular option, in order to make it more appealing to the user [which] can lead users to make ill-informed

Potential concerns	The CMA's assessment including the ICO's feedback
choices about their data.	choices'.[141] In this context, we expressed concerns to Google that the positive framing of ARA in Chrome's settings page can make it difficult for users to make informed choices. In response, Google suggested an updated version of the ARA settings page with the aim of making it clearer to users how their data will be used by the API. Google has introduced new language by changing the example of the type of data sharing allowed. The new example contains the language 'whether you made a purchase after visiting a site' as opposed to the previous example 'the time of day an ad was shown to you'. While we consider that language in the settings page stating that ARA would be 'helping sites improve the quality of the ads you see' may still create some positive bias, we acknowledge that the updated example provides users with a more meaningful example of how their data may be shared and therefore provides a more neutral framing through which users can make informed decisions with respect to how their data is used. Given this, we consider this issue to be resolved.

Trusted Execution Environments

26. For our updated assessment of the outstanding issues relating to **D&I A – Privacy outcomes**, see the main body of the report above.

27. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
Timings	Stakeholders have said that Google's recently proposed solutions cannot be tested in the timeframes available due to the preparatory steps that market participants would need to undertake prior to testing eg it could take up to 12 months to get regulatory approval with data protection/privacy regulators to use one of	Google has said that companies using Privacy Sandbox tools are responsible for their own compliance and for managing regulatory or legal issues. Google believes that timescales for which the relevant APIs have been available are sufficient.

[141] See the ICO-CMA joint paper on Harmful Design in Digital Markets, page 18 (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	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.	We recognise that adopting the Privacy Sandbox tools may create legal or regulatory requirements (eg if a company changes its data processing arrangements). We consider that there is no single 'right' notice period for changes. We also consider that Google's proposed governance framework described in paragraph 14, which includes formal consultation on strategic decisions, could surface compliance issues and allow Google to take these into account when setting timelines. Regarding holistic ARA testing, Google has restated that it believes the timeframes available for testing, including the availability of ARA app-to-web for production testing from May 2023, are sufficient. In the absence of further stakeholder feedback, we consider this issue resolved.
Self-preferencing risk associated with running TEEs on GCP.	Discussions with Google are ongoing on this issue.	This issue, concerning potential advantages to GAM through its use of GCP, falls outside the scope of the CMA's investigation, noting that the CMA may decide to investigate this issue in future, including under the Digital Markets, Competition and Consumer Act 2024.

28. 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.

Strengthening cross-site boundaries

Related Website Sets

29. For our updated assessment of the outstanding issues relating to **D&I A – Privacy outcomes**, see the main body of the report above.

30. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
Lack of clarity around the definition of 'ownership'.	We maintained our view that Google's approach to validating common administrative access to domains is appropriate.	In the absence of further stakeholder feedback, we consider this issue resolved.
RWS limits automatic cross-site data sharing to the first five domains in the 'associated' subset.	We have discussed the five-domain limit further with Google. We note that the proposal evolved over time, Google took and considered feedback 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	We consider this issue resolved. We expect that future changes to the limit would be subject to Google's proposed governance model, set out above.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	RWS should be managed within the Privacy Sandbox governance process that Google will set out.	
Prompting flow can be disruptive and undermine UX.	We maintained our view that the prompting flow strikes an acceptable balance between privacy and utility when used to mitigate the risk of site breakage.	We consider this issue resolved.
Restrictions on the ability to combine data across sites disproportionately affects sites without access to logged-in users (eg news). Sites with a large proportion of logged-in users (eg Google) are less affected by the restrictions.	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.	Google's proposals to introduce IP Protection in Incognito mode only means that publishers will have options other than logged in status to continue to build audiences. This may be mitigated further if a material number of users decide to retain cookies under Google's revised approach to third party cookie deprecation. Therefore, we consider this issue to be resolved. We note that under Google's approach there are ongoing risks that parties choose to use third-party cookies where they are available, or other identity signals (eg IP address) in a way that is not compliant with Applicable Data Protection Legislation. These parties have obligations under Applicable Data Protection Legislation. The ICO will monitor how industry responds to Google's approach and retains independence to take regulatory action against all organisations where non-compliance is identified.

31. For our updated assessment of the outstanding issues relating to **D&I D – User experience**, see the main body of the report above.

Federated Credential Management

32. For our updated assessment of the outstanding issues relating to **D&I A – Privacy outcomes**, see the main body of the report above.

33. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

Potential concerns	**The CMA's views in the April 2024 report**	**The CMA's assessment**
Google might unfairly benefit from greater use of federated ID within advertising solutions, as cross-domain signals are reduced.	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, Sign-in with Google, 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.	Google has now confirmed to us that it does not use information or activity from Sign-in with Google for ads or any other Google product.[142] In the absence of further stakeholder feedback, we consider this issue resolved.
FedCM might not support the broadest range of features, limiting its effectiveness.	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.	We expect that decisions related to future use cases will be taken within the context of the governance process Google has proposed. In the absence of further stakeholder feedback, we consider this issue resolved.

[142] See Google Account Help Center, 'How Sign in with Google helps you share data safely' (accessed on 10 November 2024).

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	Google has informed us of further feedback it has received about the lack of cross-browser support for FedCM. 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.	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. Google has stated that FedCM aims to reuse as much from other federated login systems (eg OAuth, SAML and OIDC) as possible and that it believes that FedCM should be straightforward to implement, including for smaller IdPs. It also said it hopes that the 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	Google decision to offer a user choice could have implications for the timeline relating to the availability of third party cookies. We anticipate that this will provide more time for industry to adopt technologies such as FedCM. In the absence of further stakeholder feedback, we consider this issue resolved.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	this potential concern.	

34. For our updated assessment of the outstanding issues relating to **D&I D – User experience**, see the main body of the report above.

Shared Storage API

35. For our updated assessment of the outstanding issues relating to **D&I A – Privacy outcomes**, see the main body of the report above.

36. As mentioned in the main body of the report above, we do not currently have any concerns under **D&I B – Digital advertising** and **D&I C – Impact on publishers and advertisers**.

37. We have consulted with the ICO regarding the application of **D&I D – User experience** and consider the following issue to be resolved. The CMA's assessment below includes the ICO's feedback.

Potential concerns	The CMA's assessment including the ICO's feedback
The user control for Shared Storage is combined with that for the PA API.	Currently, the user controls for the Shared Storage API are combined with PA API with one toggle for both APIs. From discussions with Google, we understand that this decision has been made as the SelectURL gate functionality and the PA API functionality, in Google's view, intuitively fit together by virtue of their shared relations to ad personalisation. However, we expressed concerns that the combined toggle represents a reduction in transparency and user controllability. If a user's privacy preferences were to differ between the two APIs, the combined toggle makes it harder for the user to act on these preferences and forces them to make the same choice for both APIs. If a decoupled toggle is technically unfeasible, Google should consider providing a drop-down section in Chrome Settings to offer some brief explanatory text for any interested users to learn more about the coupled toggle and the overlap between PA API and Shared Storage functionalities. In response to our concern, Google has said that the reason for having a single control for the Shared Storage and PA APIs is to avoid overwhelming users with choices that can be described together. Google may revisit this solution in the future as part of a workstream looking at UX and privacy controls. Given this, we consider this issue to be resolved.

Cookies Having Independent Partitioned State

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

39. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
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 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.	In the absence of further stakeholder feedback, we consider this issue resolved.
CHIPS might be implemented in such a way which does not sufficiently enable 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.	In the absence of further stakeholder feedback, we consider this issue resolved.
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 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.	In the absence of further stakeholder feedback, we consider this issue resolved. We note that CHIPS will continue to function under Google's revised approach to the Privacy Sandbox.
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.	In the absence of further stakeholder feedback, we consider this issue resolved.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
CHIPS may impact the ability of publishers to offer SSO sign-in services based on authenticated embeds.	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.	In the absence of further stakeholder feedback, we consider this issue resolved.
Implementation of both 'normal' cookies and CHIPS partitioned cookies for SSO during the transition period will create significant overheads for market participants.	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.	In the absence of further stakeholder feedback, we consider this issue resolved.
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.	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 has shipped a modified specification of the newly specified Storage Access API that reduces implementation differences.	In the absence of further stakeholder feedback, we consider this issue resolved.

40. We have consulted with the ICO regarding the application of **D&I D – User experience** and consider the following issue to be resolved. The CMA's assessment below includes the ICO's feedback.

Potential concerns	The CMA's views in the April 2024 report based on ICO's preliminary assessment	The CMA's assessment including the ICO's feedback
Users are not provided with controls to limit partitioned third-party cookies.	We have discussed with Google our concerns around the user controls for CHIPS and first-party cookies not being distinct from each other. Google maintains 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	Google has provided additional commentary and justification for its decision not to include a control for partitioned third-party cookies post the implementation of CHIPS. It is Google's view that: Functionality equivalent to partitioned third-party cookies will be available for those users who limit third-party cookies (eg first-party cookies and CNAME aliases).

Potential concerns	The CMA's views in the April 2024 report based on ICO's preliminary assessment	The CMA's assessment including the ICO's feedback
	adequate user controls for CHIPS are in place considering the trade-offs involved.	- Blocking partitioned third-party cookies is unlikely to have a material effect for users wishing to prevent third parties accessing information about their activity on a first party site. - Providing this option would be challenging to explain to users. - Google does provide an option for users to block sites from saving data to their device inclusive of partitioned third-party cookies. We continue to view it as an important principle for users to be able to understand and control third party access to their data beyond the first party site boundary; however, from these discussions, we accept that, in practice, providing this control to users who choose to limit third-party cookies is unlikely to have a material effect. As a result, we consider this issue to be resolved.

Fenced Frames

41. For our updated assessment of the outstanding issues relating to **D&I A – Privacy outcomes**, see the main body of the report above.

42. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
Fenced Frames does not sufficiently support brand safety.	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.	In the absence of further stakeholder feedback, we consider this issue resolved.
Fenced Frames does not sufficiently support expandable ads use cases.	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.	In the absence of further stakeholder feedback, we consider this issue resolved.

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

Fighting spam and fraud on the web

Private State Tokens

44. For our updated assessment of the outstanding issues relating to **D&I A – Privacy outcomes**, see the main body of the report above.

45. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
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. Our understanding is that the use of PSTs is optional and that anti-fraud organisations can rely on other signals besides PSTs. Google has told us that it does not currently envisage issuing/using PSTs. If Google were to become an issuer in future, the use of PSTs issued by Google will not be required and redeemers will be able to consume PSTs issued by a third-party other than Google. After careful consideration and discussions with Google, we came to the view that there is limited evidence that this concern would lead to a material impact on competition in the ad tech market.	In the absence of further stakeholder feedback, we consider this issue resolved.
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	Our view is that Google's governance framework, if applied effectively, could resolve this issue.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
	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. 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. We have not received further feedback from stakeholders on this point. We will continue to monitor developments.	Google has informed us of its intent to prototype and ship a feature that would allow third parties to invoke PST without waiting for first-party opt-in.[143] This is intended to facilitate wider adoption of PST by reducing the requirement to coordinate with first parties. In the absence of further stakeholder feedback, we consider this issue resolved.

46. We have consulted the ICO regarding the application of **D&I D – User experience** and note that we have no outstanding concerns with respect to PST.

Limiting covert tracking

[143] See 'Intent to Prototype & Ship: Private State Token API Permissions Policy Default Allowlist Wildcard'(accessed on 10 November 2024).

Bounce Tracking Mitigations

47. For our updated assessment of the outstanding issues relating to **D&I A – Privacy outcomes**, see the main body of the report above.

48. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

Potential concerns	**The CMA's views in the April 2024 report**	**The CMA's assessment**
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.	In the absence of further stakeholder feedback, we consider this issue resolved.
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[144] and relevant W3C groups.	In the absence of further stakeholder feedback, we consider this issue resolved.
BTM currently has a bug that causes it to delete Privacy Sandbox API storage.	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 fewer 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.[145]	Google has informed us that this bug has been fixed, tested, and fully deployed on 8 April 2024 in Chrome release M122. When BTM activates it no longer deletes Privacy Sandbox API storage. We therefore consider this issue resolved.

[144] See the 'Navigation-based Tracking Mitigations' repository on GitHub (accessed on 10 November 2024).
[145] See the message to the Blink Dev list, 7 May 2024 (accessed on 10 November 2024).

49. For our updated assessment of the issues relating to **D&I D – User experience**, see the main body of the report above.

User-Agent Client Hints/User-Agent Reduction

50. After consulting with the ICO, we considered the following potential issues under **D&I A – Privacy outcomes**. We have assessed each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider this issue to be resolved. The CMA's assessment below also includes the ICO's feedback.

Potential concerns	**The CMA's views based on the ICO's preliminary assessment in the April 2024 report**	**The CMA's assessment based on the ICO's feedback**
'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. 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	Since the April 2024 report, Google has confirmed to us that the conclusions of the Senol et al paper[146] on the use of UA-CH in the field are broadly correct and they describe the UA-CH API working as intended. Google has also confirmed that the use of normative language (eg 'using critical hints should be rare') in the UA-CH developer documentation is not intended to be binding on developer behaviour.[147] Google has said that this is just a recommendation and no restriction on critical hint functionality will result from developers not following it. The primary function of UA-CH therefore is to shift the consumption of User Agent data from a covert to overt mode. It still provides a modest net improvement in privacy. However, we agree with the ICO's assessment that it would be more effective in

[146] See Senol and Acar, 2023 (accessed on 10 November 2024).
[147] See Chrome Developer Blog, 'What is User-Agent Reduction', 19 April 2024 (accessed on 10 November 2024).

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
	understand the future intent for this API given the demise of Privacy Budget.	conjunction with other Privacy Sandbox proposals as originally conceived.

51. As stated in the main body of the report above, 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**. We do not currently have concerns about UA-CH/UAR under D&I B and C. We expect that changes in future (eg a decision to remove or limit access to critical hints) would be taken under the governance process that Google has described.

52. 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

53. After consulting with the ICO, we considered the following potential issues under **D&I A – Privacy outcomes**. We have assessed each of the concerns identified based on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved. The CMA's assessment below is based on the ICO's feedback.

Potential concerns	The CMA's views based on the ICO's preliminary assessment in the April 2024 report	The CMA's assessment based on the ICO's feedback
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.	Google's proposal to introduce IP Protection in Incognito mode means that it will apply to a very small proportion of web traffic. Therefore, we consider that this is no longer an issue.

54. Based on stakeholder feedback and our own analysis of the API, we 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 include our assessment of each of the issues identified based

on further submissions from Google and other market participants since our last report was published in April 2024 and consider these issues to be resolved.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
Google may continue to benefit from user activity data while limiting competitors' access to the same data.	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 its 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. 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 is subject to limits on its use of first party data under section G of the Commitments. For example, Google cannot use Chrome browsing history from signed-in users for targeting and measurement on either open display or O&O ad inventory.[148] We therefore consider this concern resolved.
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 views remain unchanged.

[148] See the Commitments, paragraph 25.

Potential concerns	The CMA's views in the April 2024 report	The CMA's assessment
Publishers and advertisers that rely on IP addresses for geographically targeting and personalising content will be forced to offer a worse service.	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.	Our view that coarse GeoIP data will serve most use cases remains unchanged. We also note that Google's proposal to introduce IP Protection in Incognito mode only significantly limits the impact on publishers. In the absence of further stakeholder feedback, we consider this issue resolved.
Publishers and advertisers may be less able to effectively identify fraudulent activity.	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).	Our views remain unchanged. In the absence of further stakeholder feedback, we consider this issue resolved.
Google may provide insufficient notice for 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.	Google's proposal to introduce IP Protection in Incognito mode means that it is unlikely to have a significant impact on ad techs given that only a small fraction of users choose to enable Incognito mode. Therefore, we consider that this is no longer an issue.

55. We have consulted with the ICO regarding the application of **D&I D – User experience** and consider the following issue to be resolved. The CMA's assessment below includes the ICO's feedback.

Potential concerns	The CMA's assessment including the ICO's feedback
We have received only limited information on the IP Protection UX.	As Google has announced that IP Protection will be introduced in Incognito mode, the proportion of users affected by this will be very small. Therefore, we consider that this is no longer an issue.

Storage Partitioning and Network Partitioning

56. As stated in the main body of the report above, **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.