CMA Q3 2023 update report on implementation of the Privacy Sandbox commitments

October 2023

Summary

1. This report updates on the implementation of the legally binding Commitments that Google made in February 2022 to address competition concerns relating to its proposals to remove third-party cookies from Chrome and replace them with alternative Privacy Sandbox tools (see **Annex 1**). The report summarises the progress made in Q3 2023. We do not repeat points made in previous reports unless they continue to raise issues that we intend to explore further.

2. Google intends to remove third-party cookies from Chrome in the second half of 2024. Although the timeline for removal of third-party cookies has been set by Google, we are keen to ensure there are no further delays in the process, provided that our competition concerns are addressed.

3. We would like to reassure the ecosystem that deprecation of third-party cookies can only take place once the competition concerns, identified by the CMA during its investigation, are addressed by Google. We have asked Google to be clear about this in its communications. Under the Commitments, there will be a Standstill Period of 60 days that applies before third-party cookies can be removed. This period can be extended to 120 days. During the Standstill Period, we will determine whether third-party cookie deprecation can go ahead based on the evidence we are gathering. This includes evidence from tests of the tools conducted by Google and other market participants. Our aim is to gather evidence of the likely impacts of the changes by the middle of 2024. The Standstill Period will take place following this, and once testing has been completed.

4. Google's plan to disable third-party cookies for 1% of Chrome users from Q1 2024 is specifically for the purposes of facilitating testing, and it is not the start of third-party cookie deprecation which, as mentioned above, is subject to the Standstill Period and our competition concerns being addressed.

5.	Based on the available evidence, we consider that from 1 July 2023 to 30 September 2023 (the relevant reporting period), Google has complied with the Commitments. Any developments in October 2023 will be covered in our next update report.

6.	Building on the priorities for Q3 2023, as set out in our last update report, in Q4 2023 we intend to focus on the following:

(a)	Engaging with Google and market participants to identify and resolve any outstanding issues on the design and development of the Privacy Sandbox tools. Recognising the timeline for Google's proposed removal of third-party cookies and the fact that the APIs are now in stable release as part of General Availability, our priority for this quarter is to identify and resolve any significant design concerns. Our current focus is on Protected Audience API, but we are also monitoring changes to the other tools. We are continuing to ensure that Google applies the Development and Implementation Criteria in paragraph 8 of the Commitments in the design of its proposals, including by resolving issues surrounding the impact of the tools on user experience.[1] We are also examining issues surrounding the governance of the tools.

(b)	Working with Google to ensure it carries out effective tests, and encouraging market participants to carry out their own testing of the Privacy Sandbox tools. Market participants that are planning to test the Privacy Sandbox should refer to our recently published update to the testing guidance.[2]

(c)	Continuing to work with the Monitoring Trustee and Technical Expert to analyse Google's internal systems, particularly around data access and flows. This is a multi-period activity to ensure that Google is able to comply with the data use obligations in Section G of the Commitments upon third-party cookie deprecation.

7.	Market participants who have concerns about the design and implementation of the Privacy Sandbox should continue providing feedback to us using the contact details at the end of this report. While it may not be possible for us to respond to each individual concern, raising these points means we are better

---

[1] The Development and Implementation Criteria include impact on privacy, impact on competition, impact on publishers and advertisers, impact on privacy outcomes and compliance with data protection principles, impact on user experience, and technical feasibility.
[2] Quantitative testing of Google's Privacy Sandbox technologies - Additional CMA guidance to third parties on testing, October 2023.

able to monitor the development of the Privacy Sandbox and ensure that Google is meeting its legal obligations.

Dashboard

Dashboard: summary of CMA view on current position, July-September 2023

Relevant section of Commitments	Compliance	Level of focus by CMA[3]	Key actions during period	Summary of planned next steps
D - Transparency and consultation with third parties	**Compliant**	**Higher focus**	• Engagement with market participants on quantitative testing and development of individual APIs (eg Protected Audience API) • Ensuring Google continues to respond to stakeholder concerns.	• Continuing to engage with market participants on development of individual proposals (eg Protected Audience API) • Following up on the recently published update to our guidance on testing
E - Involvement of the CMA in the Privacy Sandbox proposals	**Compliant**	**Higher focus**	• Continuing to develop framework for testing and trialling and encourage testing and trialling by Google and other market participants • Continuing to engage on design issues including approach to RWS, Protected Audience API, Attribution Reporting API & Bounce Tracking Mitigation • Bringing in views from external experts and third parties	• Encouraging testing and trialling by Google and other market participants • Engaging on design issues including approach to RWS, Protected Audience API and Attribution Reporting API
F - Standstill before the Removal of Third-Party Cookies	**Compliant**	**Lower focus (currently N/A)**	• None	• None
G - Google's use of data	**Compliant**	**Medium focus**	• Building deeper understanding of Google's internal data control systems (particularly specific areas including structured controls on software and tools relevant to paragraphs 25 and 26, data anonymisation, and exceptions covered under paragraph 29) • Working to ensure that necessary data use protections are fully implemented well in advance of third-party cookie deprecation	• Continuing to build deeper understanding of Google's internal data control systems (particularly those relevant to paragraphs 25 and 26) • Working to ensure that necessary data use protections are fully implemented well in advance of third-party cookie deprecation
H - Non-discrimination	**Compliant**	**Medium focus**	• Systematising recurring elements of reporting on Section H measures • Reviewing any discrimination concerns around technologies moving to General Availability • Engaging with Google to understand how developments particularly around RWS and Trusted Execution Environments align in this context • Further testing Google's internal decision-making process, particularly at key decision points • Continuing to apply technical knowledge to monitoring artifacts and logs	• Continuing to engage with Google to understand how developments particularly around Protected Audience API and RWS align in this context • Continuing to apply technical knowledge to monitoring artifacts and logs
I - Reporting and compliance	**Compliant**	**Lower focus**	• Completion of regular monitoring report(s)	• Google to continue demonstrating ongoing compliance • Preparing for next monitoring report(s)

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

---

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

Progress during the most recent reporting period

Testing and trialling

8.   Testing and trialling aims to gather evidence on the likely impacts of the Privacy Sandbox tools before a final decision is taken on whether to remove third-party cookies.

Testing framework

9.   Under the Commitments, Google is required to test quantitatively, where feasible, the Privacy Sandbox tools according to a set of Development and Implementation Criteria, which include impacts on competitive market outcomes in the digital advertising market.[4]

10.   In this period, we have continued to focus a significant part of our activity on working with Google on how it will test the Privacy Sandbox tools. In particular, we have worked through several complex technical issues relating to Google's testing to ensure that its results are as informative as possible for our assessment. We will continue to work with Google on its testing programme over the coming period and ensure that Google will publish the results and methodology of tests that are material to evaluating the effectiveness of the Privacy Sandbox tools (see Annex 1).

11.   As we outlined in our previous update report, we recognise that Google cannot comprehensively observe impacts across the market as a whole. In June 2023, we therefore published guidance outlining how market participants can run their own experiments of the Privacy Sandbox tools and submit their results to the CMA to form part of our assessment (the '**testing guidance**').[5]

12.   The testing guidance outlined two experimental designs the CMA proposed market participants use to test the Privacy Sandbox, how these designs align with Google's Chrome-facilitated testing modes,[6] and how and when to submit results to the CMA.

13.   On 9 October 2023, Google published further details on how its Chrome-facilitated testing modes will work in practice, including details on how Chrome will label traffic so ad techs can identify which experimental group bid

---

[4] The Commitments, paragraphs 8.a to 8.e and 17.c.
[5] CMA guidance to third parties on testing, June 2023. The testing guidance built on proposals from our November 2022 note on quantitative testing of Google's Privacy Sandbox technologies and the feedback we received from market participants (which we discussed in our last update report): Quantitative testing of Google's Sandbox technologies, November 2022.
[6] See the announcement The next stages of Privacy Sandbox: General availability and supporting scaled testing; and accompanying developer blog post Preparing to ship the Privacy Sandbox relevance and measurement APIs - Chrome Developers.

requests/impression opportunities belong to.[7] In light of this update, on 26 October 2023 we published further guidance on two ways market participants should use Google's testing modes in their own experiments (the '**additional guidance**'). First, the additional guidance seeks to clarify how market participants should use Google's Chrome-facilitated testing modes and experimental labels to make informative treatment/control comparisons they can submit to the CMA.

14.   Second, the additional guidance advises advertisers and DSPs on how they can participate in experiments in a way that seeks to ensure advertisers/campaigns in the treatment and control groups are comparable. This includes setting ways in which demand-side market participants can engage with experiments – including how they allocate budgets to experimental groups and test new post-TPC deprecation features – in a way that does not make them significantly more likely to:

      a. Participate in auctions in one experimental group than others; or

      b. Create imbalances in the types of campaigns that are present in the treatment and control groups.

15.   We are continuing to use the expertise of Dr Garrett Johnson to develop the framework for quantitative testing by both Google and third parties.[8] Dr Johnson has helped us develop the aspects of our testing guidance, ensuring that the testing framework we have proposed incorporates best practices in quantitative testing.

16.   Google is making available a limited amount of grant funding for engineering and testing-related work to eligible ad techs (SSPs, DSPs) to test the Privacy Sandbox tools and submit results to us.[9] Google discussed its plans for funding with us prior to announcing this initiative. We have closely scrutinised the terms of Google's agreements with the funding recipients, and we are continuing to engage with Google to make sure we have all the details so we can have confidence in the robustness of the test results we receive.

17.   Although we are seeking to supplement Google's quantitative testing with results from third-party testing, this is not the sole source of evidence we will rely on to assess the wider market impacts of the Privacy Sandbox.

[7] See Google's blog update on Chrome-facilitated testing (Accessed 26 October 2023).
[8] In our April update report, we referred to our appointment of Garrett Johnson, an Assistant Professor of Marketing at Boston University, as a technical adviser working on the implementation of the Commitments. Dr Johnson was appointed through an open competitive process for his expertise in online experiments, privacy and online display advertising, as well as Google's Privacy Sandbox. You can read more about Garrett Johnson's academic work here: Garrett A. Johnson | Assistant Professor of Marketing Questrom School of Business Boston University (garjoh.com).
[9] See Google's blog update on Privacy Sandbox Market Testing Grants (Accessed 26 October 2023).

Throughout our investigation, we have engaged with market participants and technical experts to gather evidence on their experiences with the Privacy Sandbox.

18. During the reporting period, we also engaged with a wide range of market participants on our testing guidance to encourage them to conduct tests and submit results in advance of our assessment. Over the coming period, we will continue to engage with market participants on our testing guidance, including its update which was published on 26 October 2023.

19. We encourage market participants also to engage with testing throughout the Chrome-facilitated testing period, and submit their results to the CMA as early as possible, and at the latest **by the end of Q2 2024** to enable us to include the results in our assessment during the Standstill Period.[10] Figure 1 below illustrates the testing timeline.

Figure 1: A visualisation of the proposed testing timeline
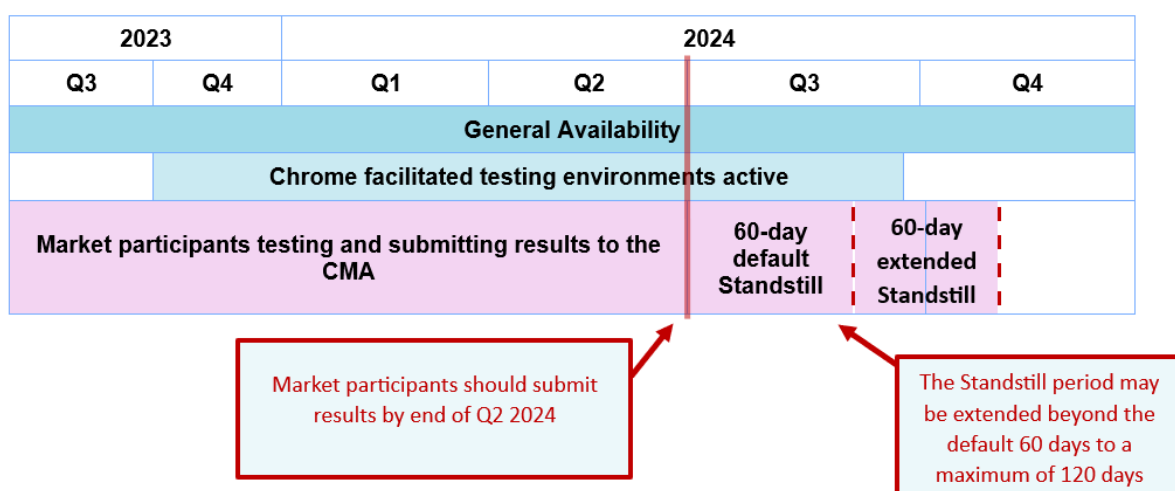
Google's tests

20. During Q4 2023, Google Ads is planning to test the Attribution Reporting and Protected Audience APIs in design 1 type testing.[11] These tests are mainly seeking to understand the functionality of the APIs, and although Google does not currently intend to publish quantitative results, we have engaged in

---

[10] Under the Commitments (paragraph 19), Google will not remove third-party cookies before the expiry of a standstill period of no less than 60 days after Google notifies the CMA of its intention to implement their removal (the '**Standstill Period**'). We will perform our assessment of the Privacy Sandbox technologies during the Standstill Period to determine whether any competition concerns remain. The Standstill Period can be extended to a total of 120 days at the CMA's request.

[11] Topics, Protected Audience and Attribution APIs moved to General Availability in September 2023. See Privacy Sandbox for the Web reaches general availability - The Privacy Sandbox.

discussion with Google on how they can share any relevant learnings with the ecosystem.

21.   Google Ad Manager (GAM) has also announced plans to gradually increase the proportion of traffic available to test the Protected Audience API, while monitoring and mitigating any publisher impact. GAM expects that, by the end of 2023, up to 10% of Chrome traffic will be enabled for Protected Audience API testing. GAM also intends to run small functional experiments (affecting less than 0.1% of traffic) with the Bidding and Auction services.[12]

22.   In Q1 2024, Google Ads will then launch an experiment using the 1% of traffic for which Chrome will deprecate TPCs to test the Privacy Sandbox tools in combination.

Design issues

23.   We continued our engagement with Google and ad tech market participants during this reporting period. This section summarises engagement on design issues, highlighting areas of concern and design changes. Many Privacy Sandbox APIs are now in General Availability, and we have seen an increase in stakeholder engagement on specific issues during this reporting period. We anticipate that this will continue as we move into the Chrome-facilitated testing period in early 2024.

24.   Many of the APIs include substantial governance elements. For example, the Topics API could include independent governance for the taxonomy. Clarity on intended governance arrangements will be an important element of our overall assessment.

25.   We are also focusing on the user experience aspects of Privacy Sandbox. We held a 'deep dive' with Google on user journeys, including consent pop-ups and user controls in the Chrome settings pane. We anticipate that the testing period will provide data on other important user experience criteria, such as page load times, and impacts on device performance.

26.   We are conscious of the need to consider Privacy Sandbox tools as they work together to impact the user journey. For example, if a site requests a Critical Hint under the User Agent Client Hints feature and runs a Protected Audience auction, both of those processes may add latency and could impact overall page load times. We will use data on user experience collected during the

---

[12] See Google Ad Manager Help, 'Protected Audience API and Ad Manager after Chrome GA', (Accessed 13 October 2023)

experiment phase to inform our overall assessment of user experience and ask Google to make changes where relevant.

Topics API

27.   Our previous report covered changes to the Topics API taxonomy. Google added 280 categories and removed 160 categories on 15 June 2023. Market participants have continued to provide feedback on the updated taxonomy during this reporting period.

28.   Some publishers have expressed concerns that the taxonomy is overly driven by advertiser preferences. More granular topics could enable advertisers to reach audiences in the open market, potentially disincentivising them from concluding direct deals with publishers. This could have a negative impact on publisher revenues as direct deals are typically more lucrative than bids for ad inventory on the open market.

29.   The concerns about whether Topics API incentivises advertisers to move away from direct deals can apply to both large and small publishers. Large publishers argue that granular topics could undermine the value of their first-party data, as advertisers could use topics to target similar audiences in the open market. Smaller, niche publishers are often more concerned about the lack of granularity meaning that their sites are misclassified, which could lead to degraded experiences for their users who would see less relevant ads.

30.   Stakeholders have also raised concerns that a larger number of more specific topics could reduce the likelihood that a smaller ad tech would have 'seen' a topic in the past and therefore reduce the likelihood that they receive a useful topic in response to their API call. Our understanding is that a similar challenge for smaller ad techs exists today; third-party cookies are more likely to be available to an ad tech with a broad reach (ie embedded on many sites) than to one with a narrow reach. We therefore do not consider this to be a significant concern with respect to the Topics API design.

31.   Given the diversity of actors in the ad tech ecosystem, we anticipate that discussions on the 'right' size and level of granularity for the Topics API taxonomy will continue. Google intends to explore future governance models for the taxonomy and to undertake further industry engagement on this issue.

32.   We are aware of stakeholder concerns that classifying sites based on hostnames creates an imbalance in contributions that sites make to determining the topics assigned to a user. For example, a user may be assigned the 'luxury travel' topic if they visit niche travel sites but the more

general 'news' topic if they visit a publisher like the BBC, even if they only read articles about luxury travel.[13]

33.   In response to this challenge, some stakeholders have suggested introducing a Topics API permission policy to allow publishers to choose whether the Topics API classifier consumes additional information (eg from the site's HTML head or body tags).[14] We understand that Google has considered and rejected this proposal. While we broadly agree with Google's assessment that including information about a page other than hostname could raise privacy risks, we recognise that Google continues to invite feedback on the issue and encourage stakeholders to suggest design changes that they believe could balance privacy risk and improvements to the API's utility.

34.   We are also aware that stakeholders have asked for the option to control which topics are associated with their site. Google responded to this feedback in their Q2 2023 report. Google's response focuses on the risk of misclassification, in other words where the Topics API classifier assigns a topic that the site owner considers incorrect. We believe that Google's response addresses the misclassification concern and agree with Google's view that allowing site owners to control classification risks incentivising site owners to game the system.

35.   We are also continuing to hear feedback on the approach to selecting which topic the API returns. This is currently based on the frequency of browser visits. Google is considering improvements to the 'top topics' selection methodology, and we expect to be able to update further on this in our next quarterly report.

Protected Audience API

36.   The Protected Audience API has been a significant focus for us during this reporting period. Stakeholder concerns broadly fall into four categories: a new auction model, on-device PA auction performance, GAM's approach to the Protected Audience auction, and the cost and complexity associated with the off-device architecture to support the API, including the Bidding & Auction service, Key / Value server and the Trusted Execution Environment (TEE) implementation.

37.   Concerns about the new auction model focus on the design choice to create a new type of auction. Our understanding is that the ad tech ecosystem has tended towards unifying auctions over the last decade, including through techniques like header bidding. Unifying auctions can increase auction

---

[13] See, for example, the notes of a stakeholder call on Topics on 31 July 2023 (Accessed 26 October 2023).
[14] See Github Topics repository issue #224 (Accessed 26 October 2023).

density, because all buyers interested in an impression compete in the same auction. This can in turn increase the competitiveness of those auctions and improve revenue outcomes for publishers.

38. Stakeholders, mainly SSPs and DSPs, have expressed concerns that they will incur significant costs to build new transaction systems to manage Protected Audience auctions. We are aware of ongoing debate about the scale and nature of these resource costs and note that implementation cost is a relevant factor to consider when assessing the Protected Audience API against the Development and Implementation Criteria.

39. Stakeholders have also expressed concern that Protected Audience auctions could reduce auction density and create a risk of buyers inadvertently bidding against themselves for the same impression. Google has made changes, eg introducing 'negative targeting' capability in Protected Audience auctions.[15] We welcome stakeholder feedback on whether this change fully addresses the concern. We anticipate that testing, including during the Chrome-facilitated testing period, will provide more information on these issues and look forward to market participants sharing test results.

40. We are concerned about the performance of on-device auctions, specifically whether Protected Audience auctions deliver acceptable latency under real world conditions. Stakeholders have raised this concern repeatedly and Google has implemented design changes in response. We are not aware of any stakeholders who have conducted further performance tests on the Protected Audience API and published results during this reporting period. Google Ads has announced plans to test the Protected Audience API during the next reporting period, and we aim to update on those tests in our next quarterly report.[16]

41. As designed, the Protected Audience API allows publishers to choose the structure of the auction, including the choice of top-level and component sellers. However, GAM will only participate in Protected Audience auctions where it is the top-level seller.[17] In practice, around 90% of publishers use GAM, raising questions about whether they have a genuine choice of top-level seller if they want to run Protected Audience auctions.[18]

42. GAM has also said that it intends to use machine learning models to determine whether to trigger a Protected Audience auction. The model will aim to optimise for total publisher revenue from all sources including direct deals, AdX programmatic auctions and revenue from other SSPs.

---

[15] See 'Negative Targeting' (Accessed 26 October 2026).
[16] See 'Ads roadmap for testing' in Google's Q3 report.
[17] See Issue #65 in the Ads Privacy repository on Github (Accessed 26 October 2023).
[18] See CMA, 'Online Platforms and Digital Advertising Market Study' (Accessed 26 October 2023).

Stakeholders have expressed concern that machine learning throttling could remove discretion from the ad tech ecosystem. 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 Protected Audience auction.

43. Market participants have also raised concerns about possible self-preferencing issues related to GAM's access to an auction's minimum bid to win. Google has told us that with the Protected Audience API, GAM will compute and share minimum bid to win information in line with its commitments to the French Competition Authority. Google has said that it expects to have fully incorporated Protected Audience auctions into the computation of the minimum bid to win by the end of the first half of 2024. We will continue to examine these issues in discussions with both Google and other market participants.

44. Stakeholders have raised concerns about the cost and complexity and the limited support for cloud providers for the off-device architecture intended to support the Protected Audience API. Google updated the timelines and specifications for the Bidding and Auction service and the TEE during this reporting period. The new timelines anticipate that beta testing for Bidding and Auction services will be available from November 2023.[19] The Key / Value service is currently available for testing.[20]

45. Google is confident that the off-device Bidding and Auction service will be an optional extra for market participants who want to develop larger, more sophisticated models in their auction process. If on-device Protected Audience auctions function as intended market participants may not need to use the off-device services, with implications for adoption cost. We are monitoring developments on this front.

46. Market participants have raised further concerns since our last report that only two cloud providers are currently supported to host trusted servers: namely Amazon Web Services (AWS) and Google Cloud Platform (GCP). This includes stakeholders who currently use on-premises infrastructure and will be unable to deploy the trusted server architecture locally. Google has stated that it expects to support more cloud providers but its plans for this have not progressed since our last report.

47. Stakeholders have also expressed concerns about the overall privacy impact of the Protected Audience API in its current state, as key privacy-preserving components will not be required, active or fully developed until after the

---

[19] See Bidding and Auction Services (Accessed 26 October 2023).
[20] See Fledge Docs (Accessed 26 October 2023).

proposed timeframe for third-party cookie deprecation. This includes mandatory trusted server architecture for the Key / Value server, enforcement of Fenced Frames, k-anonymity protection for Interest Group creation[21] and the ongoing availability of event-level data. We are continuing to discuss these issues with Google.

Attribution Reporting API

48.   Stakeholders continue to express concerns that the Attribution Reporting API will leave them dependent on Google. Without third-party cookies, some stakeholders are concerned that they will be unable to independently verify the attributions reported by the API. Google notes this feedback in its Q2 2023 report and points to resources for deduplicating conversations for event level reporting.[22] We anticipate that results from testing the Attribution Reporting API in early 2024 will provide more insight into design challenges and, in the meantime, we encourage stakeholders to continue to raise issues.

49.   Google published its plans to allow for more flexible timing in Event-level reporting configurations[23] which aim to provide greater control for market participants using this function of the API. The flexible Event-level reporting feature allows ad techs to choose their preferred reporting periods, number of reports, and cardinality of trigger side data, all with set maximum limits. We believe this is a helpful functional change for the API while still maintaining privacy for users.

50.   Stakeholders have expressed concerns that the design decision to allocate 64-bits of storage to the Event ID and the possibility to add metadata to the Event ID create privacy risks. We recognise the need to have an Event ID space large enough to uniquely identify attribution events balanced against restricting the Event ID such that it cannot be abused to track or identify individual users. Additionally, the advertiser side metadata is designed to be coarse and noisy to limit the risk that it could be used to share cross-site information. We welcome feedback on whether these technical controls fully address the privacy concerns.

51.   We have received feedback about the importance of measurement for the ad tech ecosystem, including the Attribution Reporting API. Google Ads published a paper 'Combining the Event and Aggregate Summary Reports from the Privacy Sandbox Attribution Reporting API'[24] detailing its approach to combining Event-level Reports and Aggregate Summary Reports to enhance

---

[21] Google has told us that it took the decision to remove k-anonymity for Interest Groups to help address latency.
[22] See Chrome for Developers blog, 'Prevent duplication in reports' (Accessed 26 October 2023).
[23] See explainer for 'Flexible event-level configurations' (Accessed on 26 October 2023).
[24] See Ads paper 'Combining the Event and Aggregate Summary Reports from the Privacy Sandbox Attribution Reporting API.pdf' (Accessed on 26 October 2023).

utility for advertising use cases. We would be interested in hearing from other market participants to understand if they have been able to replicate Google Ads' approach effectively.

Related Website Sets (previously First Party Sets)

52.   Google announced certain changes to First Party Sets this quarter. First Party Sets was renamed Related Website Sets (RWS), the number of 'associated' domains was increased from three to five, and Google added a user prompting flow to allow use cases requiring more than five 'associated' domains.[25] RWS rolled out to 100% of Chrome Stable clients on 29 September 2023.[26]

53.   We have heard a range of stakeholder views on the number of associated domains. We believe that a relatively small number of associated domains can improve privacy outcomes and support compliance with data protection principles. Chrome will surface information about RWS to users and the requirement for organisations to publicly declare sets via GitHub can support transparency. In addition, a relatively small number of associated domains may be more intelligible to users, aiding user comprehension.

54.   Google's prompting user flow enables websites to use the Storage Access API for use cases requiring more than five 'associated' domains. For example, a website where embedded third-party content requires user authentication can prompt the user to allow the embedded content to access cross-site storage.

55.   We understand that other browsers implement similar approaches to deal with site breakages linked to their policy to block third-party cookies by default.[27] Google proposes to allow a prompt only when the user has interacted (ie clicked or tapped) on the embedded content and when the user has visited the embedded site in a top-level context in the past 30 days. We have not heard significant stakeholder concerns about this feature or Google's proposed implementation. The feature is shipping in Chrome 117.[28]

56.   We continue to explore whether and how Google itself plans to use RWS, noting Google's statement that RWS is not intended as an advertising solution.

---

[25] See Chrome Developers blog, 'Related Website Sets - the new name for First-Party Sets in Chrome 117' (Accessed 26 October 2023).
[26] See Blink Dev, 'Intent to Ship: First-party Sets' (Accessed 26 October 2023).
[27] See for example, Safari's Storage Access API implementation (Accessed 26 October 2023).
[28] See Blink Dev, 'Intent to Ship: Storage Access API with Prompts' (Accessed 26 October 2023).

57.   In the last quarter, we raised concerns with Google regarding the RWS submission process and governance. We were specifically concerned that large numbers of developers would need to make RWS submissions and that there would be insufficient capacity to review and process these submissions.

58.   We have now clarified elements of Google's proposed approach to managing RWS submissions. Google intends to apply automated technical validation to domains in the 'ccTLD' and 'service' sub-sets as described in the RWS Submission Guidelines.[29] Although the number of RWS submissions is still small – eight at the time of writing – we are not aware of significant issues with the automated technical validation on either the 'ccTLD' or 'service' domains.

59.   Google has retained the requirement that associated domains clearly present their affiliation with the 'set primary'.[30] This requirement may make it easier for organisations that have chosen to use consistent branding to use the associated subset to share cross-site data. For example, Gmail and Google Maps use prominent Google branding whereas WhatsApp and Instagram are less prominently Meta branded.

60.   The RWS governance arrangement continues to raise three issues. First, that RWS declaration could become a bottleneck. Google currently proposes to merge pull requests that pass automated validation once a week. This could leave websites intending to rely on RWS with a gap between making the declaration and having their declaration merged.

61.   Second, Google may have to manage a large number of developers asking for support with RWS declarations or organisations seeking to challenge RWS declarations (eg on the basis that affiliation between associated domains is not clearly presented to users). We highlighted this issue in our previous report, noting that it was unclear how Google proposes to manage complaints at scale. Google has not elaborated its plans in this respect.

62.   Finally, Google retains significant discretion in governing RWS. For example, the weekly merge of valid RWS declarations is intended to be a manual process. Google has not yet specified an appeals or redress process in cases where the process is affected by human error. Similarly, Google owns the RWS repository and could make and merge changes outside of the submission process. Google rightly states that any changes would be public,

---

[29] See Related Website Sets, 'RWS Submission Guidelines' (Accessed 26 October 2023).
[30] A Related Website Set is a collection of domains, for which there is a single 'set primary' and potentially multiple 'set members' divided into use-case specific subsets. See Related Website Sets (Accessed 26 October 2023).

but a breaking change (eg due to human error) in a site's RWS declaration could have significant impacts (eg users unable to log in).

Bounce Tracking Mitigation

63.   Google updated their proposals for Bounce Tracking Mitigation (BTM) in mid-June, just before the start of this reporting period. Bounce tracking, also called navigational tracking, is a technique that sites can use to work around third-party cookie deprecation. Other browsers, including Firefox and Brave, use list-based approaches to combat bounce tracking.[31]

64.   Some use cases rely on redirect flows that are very similar to navigational tracking. Google has explicitly taken three of these flows out of scope for BTM, namely federated authentication, single sign-on and payments.[32] Google states that these use cases require some user interaction (eg clicking the 'login' button in the case of federated authentication).

65.   Stakeholders have raised concerns that BTM's rules-based approach undermine their ability to use redirect flows for purposes other than the three that Google has carved out. In contrast, a list-based approach gives stakeholders some flexibility to discuss their use case with the entity controlling the block/allow list.[33] We are discussing these concerns with Google.

Private State Tokens

66.   Google provided further information on the intended functionality of Private State Tokens (PST) during this reporting period. Although the primary use-case for PST is relatively straightforward – enabling sites to share and consume a token that can be used as evidence to decide whether a specific user-agent is trustworthy – the proposed implementation is complex.

67.   The current design requires a token issuance and redemption process whose limits are still in flux, and requires substantial cryptographic effort to develop a web-exposed version of the Internet Engineering Task Force (IETF) standard upon which it is based.[34]

68.   We recognise that PST is still at an early stage of development. However, we note that stakeholders have raised concerns that the design is open to abuse.[35] It is difficult to assess the potential risks, impact, and utility of this

[31] W3C, 'Navigational-Tracking Mitigations' (Accessed 26 October 2023).
[32] See Chrome Developer Blog, 'Bounce tracking mitigations' (Accessed 26 October 2023).
[33] See, for example Issue #64 on the Nav Tracking repository on Github (Accessed 26 October 2023).
[34] See IETF, 'Privacy Pass' (Accessed 26 October 2023).
[35] See the Trust Token API repository on GitHub (Accessed 26 October 2023).

API in its current state and we plan to provide a fuller update in the next quarterly report.

Fenced Frames

69.   Market participants have expressed concerns that Fenced Frames will have a negative impact on the display and appearance of advertising, which will in turn affect user experience, engagement with ads and publisher revenue. These concerns relate mainly to native ads, which would be unable to adapt to the 'look and feel' of the page where they are rendered if rendered inside a Fenced Frame.

70.   Stakeholders have also expressed concern that Fenced Frames would not allow video ads to render correctly. This would require changes to the Video Ad Serving Template (VAST) and OpenRTB specifications, and technical changes to video players currently in the market.[36] Google responded to this concern in its Q2 2023 report, saying that the VAST specification has been updated and that it will work to address the remaining video needs ahead of the requirement to use Fenced Frames no earlier than 2026.

Actions and conclusions of the Monitoring Trustee

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

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

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

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

   b.   Building a deeper understanding of Google's internal data control systems in order to robustly test Google's proposals to address its

---

[36] VAST is a specification that sets the standard for communication between ad servers and video players to display video ads. OpenRTB is a communication standard that enables real-time bidding.

commitments on Chrome browsing history, Google Analytics data, and ad inventory on websites not owned and operated by Google. These commitments only apply after Chrome ends support for third-party cookies, but we are working to ensure that these controls are fully implemented well in advance of third-party cookie deprecation.

c. Developing plans to investigate data flows within Google to ensure that the data controls are effective in practice (eg addressing potential risks arising from data use from any secondary storage locations).

d. Reviewing Google's proposals for the new technologies and the risk that these could self-preference Google through their design, development or implementation.

e. Speaking to, and reviewing submissions from, stakeholders who have raised concerns. We would generally not expect the Monitoring Trustee to respond directly to individual stakeholder feedback, but it would incorporate any relevant points into its overall review, as well as informing the CMA and/or Google as appropriate.[37] Submissions (or extracts of submissions) from stakeholders which are relevant to multiple elements of the compliance regime are frequently shared between the CMA, Monitoring Trustee, and Technical Expert to ensure that they are fully addressed.

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

Technical Expert

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

a. Analysing Google's data access and flows;

b. Analysing technical access controls and security; and

---

[37] Under paragraph 12 of the Commitments, '*Google will take into consideration reasonable views and suggestions expressed to it by publishers, advertisers and ad tech providers, including (but not limited to) those expressed in the W3C or any other fora, in relation to the Privacy Sandbox proposals, including testing, in order to better apply the Development and Implementation Criteria in the design, development and implementation of the Privacy Sandbox proposals*'.

c. Providing general ad tech expertise and advice.

76. We have also continued our direct dialogue with the Technical Expert. Discussions have focused primarily on market trends and issues concerning the design and implementation of Google's Privacy Sandbox proposals.

Engagement with market participants

77. 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.

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

79. Since the publication of the CMA's last report, in Q3 2023, our engagement has had a particular focus on reaching out to smaller publishers and continuing discussions with ad techs and publishers on outstanding design issues. We have also continued to monitor developments in W3C. Concerns raised throughout the stakeholder engagement process have been raised with Google, and directly informed our role overseeing the design and implementation of its proposals.

80. Details of the specific design concerns raised by market participants have been included in the corresponding section above. Other concerns raised have included the following:

   (a) Market participants are concerned that the current timeline for third-party cookie deprecation risks not leaving sufficient time for industry to prepare; including that deprecation in the second half of 2024 may coincide with the end-of-year holiday season and may be difficult to implement. We have continued to emphasise to Google that it needs to be clearer in its communications that, under the Commitments, third-party cookie deprecation is subject to our competition concerns being addressed.

   (b) We have heard that the effectiveness of the Privacy Sandbox APIs is reliant on user consent mechanisms which are out of the direct control of publishers. Others have raised the concern that the user consent

mechanisms may risk user privacy and choice by biasing towards opting-in. We are discussing these concerns with Google.

(c) Some market participants have said that Google's communications have lacked clarity over the role of the Commitments and conditionality of third-party cookie deprecation on the CMA's assessment. We have raised these concerns with Google and are working with it to ensure its communications are clearer. This is also being monitored by the Monitoring Trustee and remains an important element of the Commitments.

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

82. Our focus for market engagement over the next quarter will be on encouraging and guiding industry testing of the Privacy Sandbox APIs, further discussing outstanding design concerns, and understanding advertiser views and readiness for third-party cookie deprecation. Given the global nature of Google's developments, we welcome feedback from organisations both within and outside the UK.

Engagement with the ICO and international authorities

83. We have continued to work together with the ICO in implementing the Commitments. The ICO's role has included:

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

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

   c. Engaging with market participants on proposed alternative technologies to targeting.

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

Current views and next steps

85. Based on the available evidence, we consider that Google has been compliant with the Commitments.

86.   Over the next three months, we are planning to focus on the following activities:

   a.   Engaging with Google and market participants to identify and resolve outstanding issues on the design and development of the Privacy Sandbox tools. Recognising the timeline for Google's proposed removal of third-party cookies and the fact that the APIs are now in stable release as part of General Availability, our priority for this quarter is to identify and resolve any significant design concerns. Our current focus is on Protected Audience API but we are also monitoring changes to the other tools. We are continuing to ensure that Google applies the Development and Implementation Criteria in paragraph 8 of the Commitments in the design of its proposals, including by resolving issues surrounding the impact of the tools on user experience.[38] We are also examining issues surrounding the governance of the tools.

   b.   Working with Google to ensure it carries out effective tests, and encouraging market participants to carry out their own testing of the Privacy Sandbox tools. Market participants that are planning to test the Privacy Sandbox should refer to our recently published update to the testing guidance.[39]

   c.   Continuing to work with the Monitoring Trustee and Technical Expert to analyse Google's internal systems, particularly around data access and flows. This is a multi-period activity to ensure that Google is in a position to comply with the data use obligations in Section G of the Commitments upon third-party cookie deprecation.

87.   We are planning to publish our next update report and Google's quarterly update in October 2023.

Contact details

88.   We would welcome views from members of the online advertising ecosystem on this report, as well as on any other relevant publications (eg Google's own quarterly reports). The relevant contact details are:

   a.   **CMA:** privacysandbox@cma.gov.uk; matthew.allsop@cma.gov.uk; angela.nissyrios@cma.gov.uk; and chris.jenkins@cma.gov.uk.

---

[38] The Development and Implementation Criteria include impact on privacy, impact on competition, impact on publishers and advertisers, impact on privacy outcomes and compliance with data protection principles, impact on user experience, and technical feasibility.
[39] Quantitative testing of Google's Privacy Sandbox technologies - Additional CMA guidance to third parties on testing, October 2023.

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

c. **Google:** Feedback - Chrome Developers.

Annex 1 – current proposals in the Privacy Sandbox

At the time of publication, the list of proposals in the Privacy Sandbox include:

1. Use Case: Fight spam and fraud on the web

(a) Private State Tokens

2. Use Case: Show relevant content and ads

(a) Topics

(b) Protected Audience

3. Use Case: Measure digital ads

(a) Attribution Reporting

4. Use Case: Strengthen cross-site privacy boundaries

(a) Related Website Sets

(b) Shared Storage

(c) CHIPS

(d) Fenced Frames

(e) Federated Credential Management

5. Use Case: Prevent covert tracking

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

(b) DNS-over-HTTPS

(c) Storage Partitioning

(d) Network State Partitioning

(e) IP Protection (previously Gnatcatcher)

(f) Privacy Budget

(g) Bounce Tracking Mitigations