# Privacy Sandbox Progress Report

## Q2 Reporting Period - April to June 2023

## Prepared for the CMA, 26 July 2023

## Overview

Google has prepared this quarterly report as part of its Commitments to the Competition and Markets Authority ('CMA') under paragraphs 12, 17(c)(ii) and 32(a). This report covers Google's progress on the Privacy Sandbox proposals; updated timing expectations; substantive explanations of how Google has taken into account observations made by third parties; and a summary of interactions between Google and the CMA, including feedback from the CMA and Google's approach to addressing the feedback.

## Progress of Privacy Sandbox Proposals

Google has been keeping the CMA updated on progress with the Privacy Sandbox proposals in its regular Status Meetings scheduled in accordance with paragraph 17(b) of the Commitments. Additionally, the team maintains the Privacy Sandbox developer documentation with specific pages for each API, an overall status page, along with regular updates for the Relevance and measurement unified origin trial. Key updates are shared under the "Privacy" tag on the developer blog along with targeted updates shared to the individual developer mailing lists.

## Updated Timing Expectations

Google's latest expectations for the timing of the Privacy Sandbox proposals are set out in the Privacy Sandbox Timeline.[1] The summary below includes all Q2 2023 updates, covering the period from April 1 to June 30, 2023.

[1] According to Annex 1 of the Commitments, if the development of an API is discontinued and/or alternative APIs developed, such changes will be reported and reflected in Google's public updates, as provided for in paragraph 11 of the Commitments. Under paragraph 17(a) of the Commitments, Google is required to proactively inform the CMA of changes to the Privacy Sandbox that are material and without delay seek to resolve concerns raised and address comments made by the CMA with a view to achieving the Purpose of the Commitments.

| Privacy Sandbox Q2 2023 Timeline Updates | |
|---|---|
| **April Timeline Updates** | • TIMELINE<br>  ○ "Bounce Tracking Mitigations" pill was updated from "Early phases" to "In Development" and was placed after "Storage Partitioning"<br>• PROPOSALS<br>  ○ Storage Partitioning and Network State Partitioning were moved under "Limit covert tracking" and removed from "Strengthen cross-site privacy boundaries" accordion (proposals section). Both were included at the end of the list after "Privacy Budget".<br>  ○ "Bounce Tracking Mitigations" was added after "Network State Partitioning" under "Limit covert tracking".<br>  ○ SameSite cookies and HTTP Cache Partitioning were removed from both the bottom timeline and the "Limit Covert Tracking" accordion (proposals section) |
| **May Timeline Updates** | • TIMELINE<br>  ○ Added a new separate timeline titled "THIRD-PARTY COOKIES (3PC) AND TESTING"<br>  ○ Removed the timeline entry for FLoC |
| **June Timeline Updates** | • No updates |

# Taking into account observations made by third parties

As part of its commitments to the CMA, Google has agreed to publicly provide quarterly reports on the stakeholder engagement process for its Privacy Sandbox proposals (see paragraphs 12 and 17(c)(ii) of the Commitments). These Privacy Sandbox feedback summary reports are generated by aggregating feedback received by Chrome from the various sources as listed in the feedback overview, including but not limited to: GitHub Issues, the feedback form made available on privacysandbox.com, meetings with industry

stakeholders, and web standards forums. Chrome welcomes the feedback received from the ecosystem and is actively exploring ways to integrate learnings into design decisions.

Feedback themes are ranked by prevalence per API. This is done by taking an aggregation of the amount of feedback that the Chrome team has received around a given theme and organizing in descending order of quantity. The common feedback themes were identified by reviewing topics of discussion from public meetings (W3C, PatCG, IETF), direct feedback, GitHub, and commonly asked questions surfacing through Google's internal teams and public forms.

More specifically, meeting minutes for web standards bodies meetings were reviewed and, for direct feedback, Google's records of 1:1 stakeholder meetings, emails received by individual engineers, the API mailing list, and the public feedback form were considered. Google then coordinated between the teams involved in these various outreach activities to determine the relative prevalence of the themes emerging in relation to each API.

The explanations of Chrome's responses to feedback were developed from published FAQs, actual responses made to issues raised by stakeholders, and determining a position specifically for the purposes of this public reporting exercise. Reflecting the current focus of development and testing, questions and feedback were received in particular with respect to Topics, Fledge and Attribution Reporting APIs and technologies.

Feedback received recently may not yet have a considered Chrome response. Located on privacysandbox.com, the Privacy Sandbox feedback form is appropriate for general and specific comments, including technical and non-technical feedback. Please feel free to provide feedback to the Chrome team directly through that form.

**Glossary of acronyms.**

CHIPS - Cookies Having Independent Partitioned State
DSP - Demand-side Platform
FedCM - Federated Credential Management
FPS - First-Party Sets
IAB - Interactive Advertising Bureau
IDP - Identity Provider
IETF - Internet Engineering Task Force
IP - Internet Protocol address
openRTB - Real-time bidding
OT - Origin Trial
PatCG - Private Advertising Technology Community Group
RP - Relying Party
SSP - Supply-side Platform
TEE - Trusted Execution Environment
UA - User-Agent string
UA-CH - User-Agent Client Hints
W3C - World Wide Web Consortium

WIPB - Willful IP Blindness

## General feedback, no specific API/Technology

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Data Governance & Regulatory Compliance | Ecosystem guidance on using Privacy Sandbox in compliance with regulatory requirements. | As with any new technology, each company is responsible for ensuring that its use of the Privacy Sandbox complies with the law; Google is unable to provide others with legal advice. We are aware, however, that this is a key area of interest for the ecosystem. For each API, we have published extensive technical documentation, which should provide the basis to make necessary legal assessments, and we are working on making available additional materials in support of companies' efforts to comply with regulatory requirements. |
| CMA Quantitative Testing proposal | More information on the CMA quantitative testing proposal | We are working together with the CMA to design experiments that will provide a picture of the impact of third-party cookie deprecation and the introduction of the Privacy Sandbox proposals on the ecosystem. In April, the CMA published high-level guidance on what to expect during the Testing and Trialing period followed by detailed guidance in June. We encourage questions or feedback on the CMA's Quantitative Testing proposal to be shared directly with the CMA. |
| Chrome-facilitated testing modes | More information and clarification on the testing schedules | We published a blog post on May 18 sharing more information on the two modes of Chrome-facilitated testing. These details are not final, and we'll publish further implementation guidance as we progress in Q3 2023. |
| Partitioned Storage | Will partitioned storage be used during Chrome-facilitated testing? | Storage partitioning will be shipping to all users prior to the third-party cookie deprecation experiment. Therefore it will be enabled for all arms of the |

| | | |
|---|---|---|
| | | experiment. Sites will have the option of enabling a deprecation trial to get back unpartitioned storage during this time period. |
| Production support | What is the process in place for Chrome to support Privacy Sandbox technical issues and escalations affecting the ecosystem? | Google provides a range of channels to allow ad techs to report issues and enable any necessary escalations.<br><br>Please see our developer post for more information on the public and private forums for feedback and escalation. |
| Enrollment Timeline | The current timeframe for enrollment is too short | We are still evaluating the enforcement deadline and we would like to hear from the ecosystem on what timeline would be more suitable. |
| D-U-N-S Number | More information about the D-U-N-S number requirement for Enrollment and Attestation | Participants can find the requirements for obtaining a D-U-N-S Number on the Dun and Bradstreet website. The requirements vary depending on the market, so participants should be sure to check the website for the specific market they are interested in. In general, however, participants will need to provide basic information about their business, such as the name of the business, the address, and the contact information for the business owner or manager. Participants may also be asked to provide financial information, such as the business's annual revenue. Once the application is complete, D&B will review it and issue a D-U-N-S Number if the application is approved. |
| Transitioning from Origin Trial to General Availability | Will the transition from Origin Trial to General Availability affect current Origin Trial testers? | From July, testers will be able to access the relevance and measurement APIs in general availability. This will provide an overlap between origin trial availability and general availability. |
| AdExchanger Study | More information on survey methodology | The survey asked respondents to estimate sync rates and revenue for their businesses. Respondents' methodology for answering their |

| | | |
|---|---|---|
| | | individual questions was up to them. |
| Parameter values | How are parameter values such as noise level, anonymity thresholds, and privacy budget determined? | This GitHub explainer sets out the more general principles behind the Privacy Sandbox APIs. Many values are still being finalized and we welcome feedback on this subject. |

## Show Relevant Content & Ads

### Topics

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| Privacy Preservation | Research evaluating the Topics API on privacy preservation | We are actively involved with the research community, presenting our research on the privacy properties of the Topics API in papers, reports, and workshop presentations. We are happy to see more external members of the research community engaging with this area.<br><br>The Topics API protects users against general tracking on the web by making it too difficult to track users at scale. These papers show that we're successfully doing so with the Topics API. It's more private than third-party cookies and protects users while supporting the sites they enjoy visiting. |
| Topics taxonomy not granular enough | Broad topics taxonomy does not include more granular topics, including region specific. | In response to previous feedback from the ecosystem, we published a blog post on June 15 detailing a new updated taxonomy that incorporates numerous improvements following feedback from the ecosystem. As part of our work on the revised taxonomy, we've engaged with several companies across the ecosystem, such as Raptive (formerly CafeMedia) and Criteo. The updated taxonomy removes categories we've |

| | | |
|---|---|---|
| | | heard are less useful, in favor of categories that better match advertiser interests, while maintaining our commitment to exclude potentially sensitive topics.<br><br>We encourage the ecosystem to review the latest taxonomy and provide feedback on the changes. |
| Taxonomy and classifier update process | More information on the Topics taxonomy and classifier release cadence and how companies can prepare for such updates. | As shared in the recent blog post, we expect the taxonomy to evolve over time, and for governance of the taxonomy to eventually transition to an external party representing stakeholders from across the industry. We also shared the ramp-up plan in the topics-announce group. |
| Impact on first-party signals | The increase in number of Topics in the recent Taxonomy update may be highly valuable and as a result devalues other first-party interest-based signals. | In the Q1 2023 report, the CMA commented that "We understand that Google has been discussing its proposed new taxonomy with several market participants across the ad tech supply chain. While a few large publishers have said that greater utility of topics would increase competitive pressure on their first-party data based solutions, our preliminary view is that greater utility is better for competition overall – in particular for the ability of smaller publishers to continue monetising their inventory after the deprecation of third-party cookies". Our view is aligned with this comment made by the CMA. |
| Usefulness for different types of stakeholders | Ad techs that act as SSPs and DSPs may have significant advantages over other ecosystem players. | Our response is unchanged from previous quarters:<br><br>"Google has committed to the CMA to design and implement the Privacy Sandbox proposals in a way that does not distort competition by self-preferencing Google's own |

| | | |
|---|---|---|
| | | business, and to take into account impact on competition in digital advertising and on publishers and advertisers, regardless of their size. We continue to work closely with the CMA to ensure that our work complies with these commitments. As testing of the Privacy Sandbox progresses, one of the key questions we will assess is how the new technologies perform for different types of stakeholders. Feedback is critical in this respect, especially specific and actionable feedback that can help us further improve the technical designs. We have worked with the CMA to develop our approach to quantitative testing, and are supportive of the CMA publishing a note on experiment design to provide more information to market participants and an opportunity to comment on the proposed approaches." |
| Descendant Topics | With Topic selection criteria being frequency of browser visits, will segment fragmentation lead to descendant topics never rising to the top? | Chrome is currently evaluating other ranking methodologies, and exploring other signals that may improve ranking. We will communicate our revised plans to the ecosystem in due course. |
| Sensitivity | The Topics API's goal should be to ensure user information obtained or derived from the Topics API should be less personally sensitive than what could be derived using today's tracking methods. | We believe the Topics API is significantly more private than current technologies, significantly limits re-identification of users, and is designed to exclude sensitive topics. We acknowledge that topics can be correlated or combined with first-party data to create sensitive categories, but we believe the Topics API is a step forward to user privacy and we are committed to continue improving the API. |
| Taxonomy Structure | Add ID, Versioning, and other metadata structure to the Topics Taxonomy | Currently, in the API response, we are including the taxonomy ID. As we move towards long-term governance, it |

| | | |
|---|---|---|
| | | makes sense to review the Topics object and include additional metadata on versioning if required. |
| Publisher control | Publishers should have a say in what Topics their sites should be classified as. | Misclassification of sites may make the Topics signal slightly less useful as a signal overall, but the specific sites that are misclassified are no more and no less harmed by this than any other sites. This is because a site's contextual information will always be available for auctions on their site, which would provide comparable information to the correct topic, even in the case of misclassification. We welcome feedback on this subject here.<br><br>Allowing publishers to control their classification has risks. Sites may incorrectly classify their sites intentionally, reducing utility for all, or encode sensitive meanings in less common topics, harming user privacy. |
| Chrome extensions | Allow Chrome Extensions to manage and filter Topics, similar to current Cookie Management extensions | This should already be possible, as discussed on GitHub, but we welcome additional feedback from the ecosystem. |
| Transition to General Availability | Will there be any impact on the Topics API when transitioning from Origin Trial to General Availability? | There will be no data lost for users transitioning from Origin Trial to General Availability. |
| Privacy | Host Names may contain private information that may be revealed by the Topics API | We have a number of mitigations to ensure privacy, as outlined here. |
| Fraud and Abuse | How to prevent manipulation of Topics by fraudulent visits | Mitigations are explained here. |
| Topics classifier | Can websites request to alter their Topics classification? | We are interested in hearing from the ecosystem on this topic and welcome feedback here. |
| Topics provider sites | Designate certain websites that host content for many Topics as "Special Topics Provider Sites" | We are discussing the proposal here, and welcome additional feedback. |

| | | |
|---|---|---|
| | and train classifiers based on tags provided on the web pages. | |

## Protected Audience API (formerly FLEDGE)

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| Traffic Shaping | Performance impact of SSP-driven filtering to optimize queries-per-second (QPS) load | We have spent a considerable amount of time thinking about traffic shaping and the recommendation is for SSPs to take advantage of caching. |
| Testing volume | Challenging to test Protected Audience as SSPs and DSPs are struggling to get large traffic volumes. | We are constantly engaging SSP and DSP partners to adopt and test Protected Audiences. General Availability has begun and we are confident the percentage of traffic with PA enabled will make it more palatable to partners to test. |
| Complexity | Implementing Protected Audience solutions requires substantial effort and costs. | We acknowledge that new technologies are difficult to adopt, including Privacy Sandbox. The Privacy Sandbox team is working closely with a wide range of stakeholders to educate and support their efforts and are continuously evaluating other accelerants to support ecosystem adoption. |
| Trusted Execution Environments | Support for Trusted Execution Environments (TEE) in non-public cloud environments | While we are exploring potentially supporting options beyond cloud-based solutions, it is not currently feasible to support on-premise TEEs given on-premise security limitations that would require a time-consuming evaluation for Privacy Sandbox. Given Privacy Sandbox security requirements and the significant challenges presented by on-premise deployments, we believe that continuing to expand and improve cloud-based deployments (e.g. supporting GCP in addition to AWS) is the most beneficial for the ecosystem. |

| | | |
|---|---|---|
| | | However, we welcome additional feedback on why such a requirement is necessary. |
| Cost Structure | Bidding & Auction Services proposal will increase cost and complexity for Ad Techs compared to client-side models. | We are currently developing a guide for estimating costs of supporting bidding and auction workflows in the Bidding & Auction server, which will be correlated with ad-tech usage, fulfilling one of the goals of our designs. |
| K-Anon Timelines | When will the planned k-anonymity constraints be enforced on `renderUrl` ? | We are working on an explainer for the enforcement timeline that we will release soon. |
| runAdAuction restrictions | Can Chrome restrict `runAdAuction` to only be callable from the top page? | While our design fully supports `runAdAuction` to be callable from the top page, we believe it would be more harmful for publishers to restrict it to only be callable from the top domain.<br><br>We have specifically heard from the ecosystem that the Privacy Sandbox needs to minimize the burden on publishers and advertisers. That feedback aligns with the general principle of web development that site owners can use third-party tools in running their sites. The Privacy Sandbox goal has been to encourage a healthy ecosystem without needing to prescribe how publishers and ad techs work.<br><br>By allowing the publisher to choose how and who calls `runAdAuction` on their site, we believe we offer flexibility to publishers to find the best path for their requirements. |
| Implementation support | Can Chrome build or contribute to an open-source implementation of a multi-seller auction? | The Privacy Sandbox aims to develop privacy-preserving technologies that don't rely on third-party cookies or other cross-site identifiers. We want to encourage a healthy ecosystem without needing to prescribe how ad techs need to work. |

| | | |
|---|---|---|
| | | We have published guidance on how the APIs work on our GitHub repository and are open to exploring solutions with the industry.<br><br>We do not plan to build any specific implementation as our core remit is to build platform technologies, not to dictate strategies for using those technologies. Our technologies will help enable ad tech companies to best serve their customers with the right privacy guardrails for consumers. |
| Multi-seller auctions | Will Chrome force sharing a “contextual” winner with component auctions? | The Protected Audience API is designed to offer the ability for parties initiating the multi-seller auction to pass information to the component auction (note: only prior to initiating the auction).<br><br>That said, we see no way for the browser to distinguish whether a piece of information is a contextual winner or not, so we could not enforce blocking or requiring certain information. |
| User preference for consent tracking | Adtech asking PA how to implement user consent tracking correctly | Our response includes what we said in Q1:<br>"For specific ads, the relevant ad tech is the party best positioned to offer controls over which creatives are shown or how they are selected."<br><br>We discussed a number of scenarios related to this issue during the May WICG Protected Audience Meeting and we welcome additional feedback and discussion on this issue. |
| Custom Audiences | Will SSP use cases related to creating Custom Audiences be supported by the Protected Audience API? | The Protected Audience API allows for SSPs and other ad-tech providers to own and manage Custom Audiences. Further guidance on how an SSP can integrate with the PA AP is being developed and |

| | | |
|---|---|---|
| | | will be made available for SSPs and other ad tech providers to support their integration efforts. |
| Formats | Is video supported by the Protected Audience API? | Video ads are delivered in one of two ways: as VAST XML or HTML (an outstream ad that ultimately may load VAST XML into a video player as well). Buyers can return either format via a renderURL. The VAST specification was recently updated to support the Attribution Reporting API. Sites serving video ads will need to prepare for the way ads are delivered via the Protected Audience API. This means making sure placement tags can pass the URL from a Protected Audience iframe to a video player. For Fenced Frames we will work to address video needs ahead of the requirement to use Fenced Frames which is no sooner than 2026. |
| Pacing | How does Pacing use case work with the Protected Audience API? | We appreciate the feedback. We would be interested in seeing more instances of this request with more details coming from more SSP partners as this has been mostly a DSP concern to date. |
| Update frequency | The frequency of calls from `dailyUpdate` (up to 1 per interest group per day) may not be enough for certain use cases, such as updating product information. | We appreciate the feedback. There are other solutions available for allowing ad techs to use signals that are refreshed in different cadences like K/V lookups. |
| Ad Quality Control | How do publishers implement ad quality control? | Today, the Protected Audience API offers functionality for publishers to inform their SSPs on certain controls they can establish as part of the auction config, pre-bid (i.e. denylists based on labels associated with ads). We welcome feedback on any additional functionality the ecosystem may require. |
| Debugging | When will `forDebuggingOnly` | We plan to retire `forDebuggingOnly` for loss events by third-party cookie |

| | | |
|---|---|---|
| | functionality be removed? | deprecation. We plan to retire `forDebuggingOnly` for win events in 2026 at the earliest. |
| Cross Device Interest Groups | Proposal to enable cross-device interest groups for authenticated user agents | We are evaluating this proposal, but the high specificity of cross-device targeting poses significant privacy concerns, as discussed in this GitHub Issue. |
| (Also reported in Q1) Dynamic Remarketing | Will Dynamic remarketing still be possible with the Protected Audience API after third-party cookie deprecation? | We believe this use case is possible using Protected Audience, as explained here. |
| Click related data | Add click-related data to `browserSignals.` | We are currently asking for clarification on when the click happened to give a preliminary position. |
| (Also reported in Q4 2022) User defined functions in Protected Audience | How will user-defined functions (UDF) be supported in the Protected Audience API? These are functions that can be programmed by end users to extend the functionality of the API. | The ad tech who raised this issue also mentioned they are still evaluating what they could do with UDF so there is no actionable feedback here yet to react to, not until at least General Availability. |
| Currency | Currency amounts should not be represented using floating points. | We addressed this issue in detail here. |
| Non-DSP ad selection capabilities | What role do Ad Servers play in Protect Audience API auctions? | We are aware of the requests for Ad Servers to continue offering post-bid ad selection / dynamic creative optimization services. We are currently assessing the detailed gap analysis that exists between the current Protected Audience API and these requests. |
| GenerateBid | Support for Google Ads' proposal to return more than one candidate ad per ad interest group from `generateBid` and have those candidates scored in `scoreAd`. | This is being currently evaluated. We welcome additional feedback here. |
| Auction Order | Are Protected Audience API | There's no technical requirement for the |

| | | |
|---|---|---|
| | Auctions required to be the last one to run so that it can take input from the outcome of all other auctions? | Protected Audience API to run last. |
| Non-user initiated navigation | Expose non-user initiated navigation | We are reviewing this request and discussing it here and welcome additional feedback. |
| Caching | SSP should not build a given DSP's perBuyerSignals from a cache if the user state changes. | We understand that caching does not work for every use case for perBuyer signals and are evaluating further options. We welcome any additional feedback from the ecosystem on whether caching would work for their use cases. |
| Attribution Reporting and Protected Audience | How can the Attribution Reporting API and the Protected Audience Audience API work together? | Integrations are currently available for Protected Audience API for both Attribution Reporting API modes (event-level and summary reports). We have shared more information on improved Protected Audience API and Attribution Reporting integration on June 1. You can read about them here. |
| Server Endpoint | Will the server endpoint be the Trusted Aggregation Server in the final design? | The server endpoint is an ad tech maintained endpoint that is independent from the Trusted Aggregation Servers used to process the collected and transformed reports. We don't have any changes planned for the reporting endpoint at the moment. The current design aims to ensure that the aggregatable reports themselves (with encrypted payloads) don't leak cross-site data, so a trusted endpoint shouldn't be necessary. An additional complication is that different ad techs will likely have different desired batching strategies. We welcome additional feedback here. |
| WebIDL | The current Protected Audience API spec is not compatible with WebIDL spec. | We are evaluating this feedback and discussing the issue here. |

| | | |
|---|---|---|
| Consent Management | How will consent signal passing be handled in the Protected Audience API? | Contextual information is not within the scope of Protected Audience API. We are discussing this issue and welcome additional feedback. |
| Account Based Marketing | Would account-based marketing use cases be possible? | Protected Audience API supports a variety of audience-based marketing use cases. We are continuing to understand how Protected Audience API can best support this particular use case, and welcome additional feedback on this issue from the ecosystem. |
| Component auction | What do component auction participants score? | The component auctions don't score Interest Groups directly – rather they score the ads and bids that a DSP submits from the `generateBid` function. The `generateBid()` function runs per interest group, and the DSP returns the following when executing generateBid:<br>`return {'ad': adObject, 'adCost': optionalAdCost, 'bid': bidValue, 'render': renderUrl, 'adComponents': [adComponent1, adComponent2, ...], 'allowComponentAuction': false, 'modelingSignals': 123}; }` |
| External Contributions | Request to support external contributions on the Key/Value Server GitHub code base. | We are looking to update our relevant processes to support external contributions to the GitHub code. |
| Interest Group Size | What is the supported maximum number of keys the IG can support? | The current limit is 50 kb on the size of one IG and keys count as part of that. We welcome further discussion on the size limit. |
| Batching | How can the number of K/V server calls be reduced? | You can use HTTP Cache-Control Headers to reduce the number of K/V calls. For example, it could be cached across component auctions, and also across ad slots on a single page. |
| Version control | Support for multiple versions of ad-tech code | Bidding and Auction services will support multiple versions of ad-tech |

| | | |
|---|---|---|
| | | code. In the Bidding and Auction API, the `SelectAd` request can specify the version of the code used for the auction request (i.e. for bidding / auction and also reporting). |
| Shared Storage | Support writing to Shared Storage in the Bidding and Auction Service. | Currently, Bidding and Auction Services does not support Shared Storage, but we welcome additional feedback on why such use cases are important to the ecosystem. |
| Web-to-app | Support web-to-app sharing of interest groups. | Web-to-app is not currently scoped in the Protected Audience API deployment across Chrome and Android, but we are interested in hearing from the ecosystem on the importance of this use case. |
| K-Anonymity | How to handle K-Anonymity fallbacks | We are discussing the issue and welcome additional feedback. |

# Measuring Digital Ads

## Attribution Reporting (and other APIs)

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| Alternative VTC Event Level Report Configurations | Feedback on Alternative VTC event-level report configurations | We've heard some feedback that the current event-level configurations are not optimal and we are asking for feedback on optimal global configurations. We are open to additional feedback regarding this and think that our flexible event-level explainer helps to address this as well. |
| Flexible event-level configurations | What is the status of the flexible event-level configurations feature? | We have shared documentation on flexible event-level configuration. The feature is still in the proposal stage and we are looking for more feedback on whether the feature will be valuable to the ecosystem. |

| | | |
|---|---|---|
| Flexible event-level configurations | How can conflicting reports from different parties be reconciled? | Most reporting scenarios are addressed through the use of aggregate reports, whereas the flexible event-level configuration proposal is specifically for additional flexibility for event-level reports, which are most often used for optimization use cases. We welcome any additional ecosystem comments/feedback regarding this scenario. |
| Source registration | What if the source registration happens after the trigger registration? | Currently, if a source registration occurs after the trigger registration, then the source and trigger will not be able to be attributed to each other. This seems to be an edge case scenario. We welcome any additional feedback regarding this issue and will look to address it if it's a scenario many ad techs seem to face. |
| Working with multiple Ad Agencies | How can DSPs use the Attribution Reporting API when an advertiser is working with multiple ad agencies? | The API supports redirects and therefore can be used even when an advertiser is working with multiple ad agencies. Additionally, there are some limitations in place regarding redirects in order to ensure that the API is improving privacy. We have also identified a potential workaround utilizing the Shared Storage API for the specific scenario the ad tech has raised. We welcome any additional feedback regarding this scenario and will continue to iterate based on that feedback. |
| Destination Limits | The auto-refreshing ads use case may be impacted by having destination limits. | We discussed this issue in the May 1 WICG meeting and are looking for feedback on what a reasonable limit would be. We have added to the Attribution Reporting with event-level reports explainer stating that browser can limit the number of `destination` eTLD+1s represented by source-sites. (See pull request). |
| Attribution Reporting and | How can the Attribution Reporting API and the | Integrations are currently available for Protected Audience API for both |

| | | |
|---|---|---|
| Protected Audience | Protected Audience Audience API work together? | Attribution Reporting API modes (event-level and summary reports). We have shared more information on improved Protected Audience API and Attribution Reporting integration on June 1. You can read about them here. |
| Flexible event-level configurations | Share best practices for noise simulation now that the parameters are configurable. | We have shared code on GitHub that anyone can use to assess the information gain and noise impact for whatever flexible event-level configs they want to test. We would be interested in hearing from anyone who chooses to test with the code and would like to share feedback. |
| Cross App and Web Attribution Measurement | When will cross-app and web attribution measurement be available? | We announced on May 9 an experiment for Cross App and Web Attribution Measurement via the Attribution Reporting API. While General Availability is planned for the relevance and measurement APIs in Chrome 115, Cross App and Web Attribution Measurement is not currently planned to hit general availability with Chrome 115. |
| Deduplicate conversions | How can independent measurement solutions be reconciled against ARA? | As with current standard practice, advertisers would work with a third-party independent measurement provider to de-duplicate conversion reporting. We have offered resources on how to deduplicate conversions for event level reporting here. |
| Data loss during Attribution Reporting database updates | Will there be any data loss when Chrome updates the Attribution Reporting Database as announced? | Starting with Chrome Stable 115, we will begin enabling the Relevance and Measurement APIs for a portion of Chrome users by default. This general availability will ramp up as we monitor for potential issues. The goal will be to reach 100% availability over a period of weeks, by Q3 2023. This will coincide with the end of the Relevance and Measurement origin trial. Starting in July, testers will be able to enroll for access to these APIs in general availability. This will provide an |

| | | |
|---|---|---|
| | | overlap between origin trial availability and general availability through enrollment. Your origin trial token will be valid until September 19, but we recommend you enroll for the APIs before the expiration in order to transition seamlessly out of the origin trial without interrupting any ongoing tests.<br><br>As mentioned in this announcement, the data registered from older versions (M113 and earlier) will not be migrated after the update, therefore there may be a data loss. This data loss won't show up in debug reporting, and we will try to avoid data loss from 114 to 115. |
| Billing | Using Attribution Reporting for cost-per-conversion billing | As stated in this article, the Attribution Reporting API may not be suited for cost-per-conversion billing needs, because of the noise added to event-level and summary reports. We encourage ecosystem players to share feedback about the impact on various billing models by the Attribution Reporting API on GitHub. |

## Aggregation Service

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| Aggregatable report delay change | Positive reactions to the proposal to change the Aggregatable report delay to be from [10-60 mins] to [0-10 mins] following feedback from the ecosystem | We are pleased to see positive reaction to the proposed change, and encourage the ecosystem to continue providing feedback on our proposals. |
| On-premise solution | Can the Aggregation Service be deployed in on-premise data centers? | While we are exploring potentially supporting options beyond cloud-based solutions, it is not currently feasible to |

| | | |
|---|---|---|
| | | support on-premise TEEs given on-premise security limitations that would require a time-consuming evaluation for Privacy Sandbox. Given Privacy Sandbox security requirements and the significant challenges presented by on-premise deployments, we believe that continuing to expand and improve cloud-based deployments (e.g. supporting GCP in addition to AWS) is the most beneficial for the ecosystem. However, we welcome additional feedback on why such a requirement is necessary. |
| Reprocess reports for different time periods | Ability to reprocess reports for different time periods | We have heard similar requests to be able to split up batches for different date ranges. One proposal is to allow the ability to extend the shared ID with an ad tech-defined label so that reports may be split into different batches. We are in the early process of evaluating this process and will keep the ecosystem updated as this proposal evolves. |
| Privacy Implications of Trusted Execution Environment | Positive sentiment towards privacy implications of Trusted Execution Environments | We are pleased to hear of positive reactions from the ecosystem regarding our proposals, and we welcome additional feedback as we continue to iterate and develop. |
| Terms of Service | What is the deadline to accept the Aggregation Service terms of service? | While we have not yet specified a deadline to accept the terms and conditions, we would encourage ecosystem companies to accept the terms and conditions as soon as possible in order to prevent delays in enrollment. We encourage companies to reach out if they have any questions. |
| Key Discovery | The key discovery feature will enable testers to query aggregate reports without needing the explicit list of possible key combinations in order to process summary | We are currently exploring possible solutions and workarounds and welcome additional feedback from the ecosystem. |

| | | |
|---|---|---|
| | reports for cross-network attribution for improved performance and accuracy. | |

## Private Aggregation API

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| Reporting Origin | How is reporting origin defined? | Reporting origin is always the script origin of the Private Aggregation caller. |
| 128 bit key space | Clarity on the 128-bit key space limitation | We will make this keyspace limitation more clear and resolve the inconsistencies across pages. We recommend using hashing strategies to stay within this keyspace. |
| Maximum contribution per report | Current limit of 20 contributions per report is too low. | Rather than increasing the maximum number of contributions, we are open to considering splitting reports rather than truncating at the limit. We will engage the ecosystem as this proposal evolves. |
| Reach reporting | Request for reach cross-platform/cross-device reporting. Reach is a foundational metric of brand advertising. Advertisers rely on cross-platform/cross-device approximations for Reach and Frequency reporting to analyze their campaigns and allocate spend. Reach models use third-party cookies as a signal for measuring ads shown in third-party environments, and so ad techs have requested an alternative solution once third-party cookies are deprecated. | The Privacy Sandbox team is exploring features to support cross-domain reach methodologies after third-party cookie deprecation.<br>We welcome additional feedback from the ecosystem. |

# Limit Covert Tracking

## User Agent Reduction/User Agent Client Hints

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| (Also reported in Q1 2023) Hints for additional form factors | Request for User Agent Client Hints (UA-CH) to provide additional form factors such as TV, VR | We are still working on some key design decisions (whether to provide a single value such as "TV", or a list of form-factor capabilities), but remain interested in prototyping this idea. |
| Privacy Budget | Privacy Budget restrictions could cause UA-CH requests to become non-deterministic when too many requests are sent. | We have no new updates on the Privacy Budget proposal at this time, but we have committed to not restrict requests for UA client hints before third party cookies have been deprecated. |
| Site Compatibility | Websites are using UA-CH brand to restrict certain browsers from accessing sites. | There are valid use cases for having a brand list, and one of them is precisely compatibility. A UA is free to have multiple brands to work around these issues. |

## IP Protection (formerly Gnatcatcher)

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Fraud & Abuse | How can companies set up anti-fraud measures with IP Protection? | We understand the importance of anti-fraud use cases and the possible impact to those use cases. We plan to publish more details about supporting anti-fraud later this summer. We are seeking ecosystem feedback on how we can better support anti-fraud use cases. |
| GeoIP | More information on testing and deployment timeline for GeoIP | Chrome has recently published new information detailing our GeoIP plans. We are planning to publish more information about deployment timelines in Q3. We expect to launch IP Protection as a user opt-in feature on a small percentage of |

| | | |
|---|---|---|
| | | traffic initially. The reason for this is that we recognize that this proposal may involve some significant changes for companies, and we want to give the ecosystem time to adjust and provide feedback before the feature is rolled out more broadly. |
| Account authentication | How will account authentication with the proxy server work exactly? | We plan to publish more details about account authentication later this summer, though we have shared some initial considerations already. |

## Bounce Tracking Mitigation

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| Testing Guidance | Information on how to test Bounce Tracking mitigation | We published a blogpost in May with further information on how to test Bounce Tracking Mitigation. |
| Documentation | Clarity in the Bounce Tracking Proposal | The current proposal is very much a work-in-progress and Chrome is continuing to update the proposal to provide clarity and information to the ecosystem. We are working on providing more details and welcome any additional feedback. |
| Cookie deletion | Will Bounce Tracking Mitigation delete all cookies in a domain? | Bounce tracking mitigation (BTM) will clear all storage and all cache, as explained here. |
| Circumventing Bounce Tracking Mitigation | Bounce tracker classification may be bypassed by performing redirects with pop-ups or new tabs. | The Bounce Tracking Mitigation specification is still a work in progress. We've been mostly focused on same-tab redirections so far but we plan to work on pop-up flows in the future. We welcome additional feedback here. |

## Privacy Budget

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|

| | | |
|---|---|---|
| Proximity Targeting | Privacy Budget may impact proximity-targeting use cases. | We have received feedback on this issue and would be interested in hearing more on the potential impacts from the ecosystem. |

## Strengthen cross-site privacy boundaries

### First-Party Sets

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| (Also reported in previous quarters) Domain Limit | Request to expand the number of associated domains | Chrome is evaluating the appropriate numeric limit for the Associated subset that will balance privacy and utility for the use cases that have been identified. From the very outset, Chrome shared that the exact number for the Associated subset was yet to be finalized. |
| Embedded Use Case | Support for Embedded use cases that require First-Party Sets, CHIPs and shared storage | Chrome has received the feedback on this use case, and the team is investigating and welcomes additional feedback. |
| Repository Management | Information on policies to remove First-Party Sets from the GitHub repository if there are discrepancies or neglect | Chrome has received the feedback on this use case. The team is investigating and welcomes additional feedback. |
| User Education | Chrome should increase user awareness and understanding of First-Party Sets to drive adoption. | Chrome is committed to educating users about First-Party Sets, and has published a Help Center article (linked from the Chrome UI) to this effect. Chrome is also invested in continuing to learn how to best educate users in the appropriate contexts. |
| Post 3PCD | Third-party cookies will continue to exist within a First-Party Set after third-party cookie deprecation. | While `requestStorageAccess` and `requestStorageAccessFor` do indeed make third-party cookies available again for specific, clearly-defined use cases, they now require active invocation by the site, instead of being available by default, as with the current state of third-party cookies (in Chrome). |

| | | |
|---|---|---|
| | | While this invocation within a single set will not require user approval, users have the ability to prevent this by opting-out of this behavior in Settings.<br><br>Further information is available to users in the Help Center article (linked from the Chrome UI). We plan to expand upon the existing developer guide as FPS ramps up to 100%. |
| First-Party Sets submission | Rename the required `.well-known/first-party-set` to include a .json extension. | We have made this change to ensure certain web hosting plans are supported. |
| IANA Registration | `first_party_sets.JSON` should be registered with IANA | We are considering the proposal and welcome additional feedback here. |

## Fenced Frames API

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Ad Blocking | Fenced Frames may make it easier for ad blockers to block ads. | Extensions can interact with fenced frames similar to how they would interact with iframes. The actual URL that the fenced frame is about to be navigated to will also be visible to extensions and therefore they can apply any URL matching rules for blocking as they would in iframes. Simply blocking all fenced frames unconditionally might break non-ads use cases of fenced frames. |

## Shared Storage API

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Wider adoption | Shared Storage should be an industry-wide standard available across browsers. | We welcome and acknowledge this feedback. Chrome is continuing to actively participate in W3C fora to champion the proposal, seek feedback, and drive adoption. |
| Output Gates | Shared Storage output gates are | We are considering this feedback and |

| | | |
|---|---|---|
| | too limited. | welcome additional ecosystem feedback on why the output gates are too limited. |
| Regulatory Compliance | How will Shared Storage handle regulatory compliance such as data retention policies? | Shared Storage provides the flexibility to implement and customize logic to control the lifetime and expiration of any stored data. Ad techs can update or clear Shared Storage data on the basis of write timestamps. |
| A/B Testing | How can A/B testing for Shared Storage and Protected Audience API be conducted? | We are working to publish additional guidance on this matter and hope to share more details in the future. |
| Shared Storage Limit | What will happen once the Shared Storage limit is hit? | If the limit is reached, no further inputs will be stored. |
| Multiple access on the same page load | What happens when Shared Storage is accessed multiple times on the same page load? | The best way to handle this is through the `window.sharedStorage.append(key, value)` function. Rather than updating the value for each ad, which could cause collisions if there are multiple ads. The append function will just add the new value to the end of the preexisting one. |
| iframe Functionality | Will Shared Storage support certain iframe functionality once they no longer work after third-party cookie deprecation? | Post third-party cookie deprecation, local storage in iframes will be partitioned by the top-level site but the iframes themselves won't be blocked. The data in an iframe's local storage can't be replicated across multiple top level sites, but the local storage can still be used within the iframe. |

## CHIPs

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| Partition limit | 10 KiB per partitioned site is still substantial and would like to see it lowered. | Firefox has already indicated a positive position on CHIPS. For Webkit support, we encourage developers to provide feedback to Apple directly on this GitHub issue regarding their use cases where partitioned cookies are preferred over partitioned storage. |
| Authenticated embeds | CHIPs may affect current SSO sign-in flow due to different partitioning impacting | We intend to leverage the Storage Access API (with user prompts) to support the authenticated embeds use case, and recently |

| | | |
|---|---|---|
| | authenticated embeds. | sent an intent-to-prototype. |
| Lifetime Policies | Will potential lifetime policies apply to first-party cookies? | We currently have no plans to impose lifetime limits on first-party cookies. |

### FedCM

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| OAuth Authorization Support | Align on authorizing non-profile Oauth scopes | We are actively seeking input from the Web Identity community through the W3C FedID CG on the best ways to support authorization beyond basic authentication post third-party cookie deprecation. |
| Support for SAML | Align on requirements for SAML support | The team is actively seeking input from the research and education communities on SAML support needs (in addition to OpenID-connect support) post third-party cookie deprecation. |

## Fight spam and fraud

### Private State Token API (and other APIs)

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| Exploring new signals | Several partners have expressed positive sentiment towards exploring browser-facilitated signals of device integrity or user trust. Generally, they are also cautious about new purpose-built signals being sufficient to retain current levels of fraud detection. | We are excited to explore new proposals together within the anti-fraud and web safety community, and also acknowledge and share their concerns - this is exactly why "fighting spam and fraud" has been a core workstream of Privacy Sandbox and why we continue to prioritize investment in preserving web safety as we improve user privacy. |
| Positive feedback on PST | Several partners have expressed interest in testing or utilizing PSTs for various anti-fraud or web safety use | We are excited to hear support and interest in further exploring new solutions which utilize PSTs. We have resources and sample code available through the Chrome developer site, |

| | | |
|---|---|---|
| | cases. | and welcome further feedback. |
| Fraud and Abuse | Guidance for Ad Fraud Prevention / Detection in measurement after third-party cookie deprecation when identifiers are no longer available. | We have introduced tools such as private state tokens, which help to recover some of the signal lost by third-party cookies for anti-fraud purposes, but with new privacy controls in place. We are actively investing in new anti-fraud and anti-abuse proposals to preserve capabilities with other Privacy Sandbox changes. |
| Issuer to origin information rate | Issuer-to-origin information rate is high enough to identify unique users. | We have updated the spec to be more clear about what user data is able to be conveyed using Private State Tokens. By design, up to six public keys can be used at a time, which may represent a "state" for a particular user. These sets of keys can only be updated every 60 days (except in rare cases where an emergency key rotation is necessary), which slows down the potential to join additional user data over time. With any new web API, there is a balance of utility provided and net new user information that it provides. We estimate that PSTs strike the appropriate balance in protecting user privacy while enabling key anti-fraud use cases impacted by third-party cookie deprecation. |
| Fetch Integration | The `fetch` integration is complicated and unnecessary. | There are pros and cons to utilizing `fetch`, and we would like to pursue further standardization within the web ecosystem, but we think it would be too early to make this change until we have a clearer sense of what the standard will look like. If and when a standard emerges, we are also committed to responsibly transitioning web developers to that standard. |
| Storage Location | Private State Tokens key configurations should be stored in the same location as PrivacyPass Protocol. | While testing during the Origin Trial, developers indicated they preferred the flexibility to store their keys at general URLs instead of in a .well-known directory. The key commitment format in PrivacyPass isn't particularly suited for a version where the keysets are intended to allow for an implicit "public metadata" value. If a variant of |

| | | |
|---|---|---|
| | | PrivacyPass ends up getting standardized with public metadata (either as a POPRF, partial RSA blinding, or keysets) we might move to a future version of PST to support that. |
| Header implementation of the API | Questions regarding the header implementation of the API | As the API gets standardized and the ecosystem usage of this API matures, we can hopefully either support both the standard non-header version of this API and potentially eventually deprecate the header version if usage is low enough or there's enough developer tooling/support for standard ways of correlating issuance/redemption requests with other data. We are discussing the issue here. |
| Registration | Is making issuers register with browser vendors practical? | We have updated the specification to describe the issuer registration process for Private State Tokens. While it uses its own process, it is similar to enrollment plans for the rest of the Privacy Sandbox work, where we ask issuers to make a public statement for how they intend to use PSTs and to acknowledge the technical restrictions which protect user privacy. |

# Google Ads Roadmap for Effectiveness Testing of the Privacy Sandbox Proposals

As we continue to approach the potential deprecation of third-party cookies, efforts to invest in testing the effectiveness of the APIs are increasingly becoming a priority. For its part, Google Ads is engaged in integration and initial testing of the APIs and providing feedback to the CMA and the ecosystem. Google is conscious of the importance of transparency for the ecosystem, so that they can plan their investments and forecast participation in future tests, and as such has included Google Ads' testing plans below:

***Topics API for Interest-based Advertising***:

- During Q2 2023, in consultation with the CMA, Google Ads has published a blog post and whitepaper that outlines the methodology and shares the results of an Interest-based Advertising experiment on Origin Trial Chrome Desktop + Mobile Web traffic, utilizing a combination of privacy-preserving signals including contextual information, the Topics API from the Privacy Sandbox and first-party

identifiers such as Publisher Provided IDs.

***Protected Audience API for Remarketing***:

- In Q4 2023, Google Ads plans to conduct an experiment with the Protected Audience API (individually) for Remarketing on Chrome Desktop and Mobile Web utilizing General Availability traffic from the Google Display Network.

***Measurement APIs***:

- In July, Google Ads published API integration guidance (summary, detailed) for third-party ad tech on how to effectively combine the Event and Aggregate Summary Reports from the Privacy Sandbox Attribution Reporting API for improving Ad-Measurement Fidelity.
- In Q3 2023, Google Ads envisages publishing guidance on how third-party ad tech could improve Event and Aggregate-API data from the Privacy Sandbox Attribution Reporting API via intelligent configuration.
- In Q4 2023, Google Ads plans to conduct an experiment with the Attribution Reporting API (utilizing both Event-level and Aggregate-level reports) on Chrome Desktop and Mobile Web utilizing General Availability traffic from a subset of Google Owned and Operated properties.
- In Q1 2024, Google Ads plans to continue the experiments with the Attribution Reporting API (utilizing both Event-level and Aggregate-level reports) on Chrome Desktop and Mobile Web utilizing General Availability traffic from an expanded set of Google Owned and Operated properties.

***Chrome-facilitated testing***:

- In Q1 2024, Google Ads plans to conduct an experiment to test privacy-preserving solutions and Chrome's Privacy Sandbox APIs in combination (Topics, Protected Audience and Attribution Reporting) via Chrome-facilitated testing on Desktop and Mobile Web with traffic from the Google Display Network.

Google's long term testing timeline, along with registration details for Chrome's Origin Trials and details of the APIs is available at the privacysandbox.com site.

## Updates on User-Agent Reduction

**Rollout of User-Agent Reduction**

During this reporting period Google has provided the CMA and the ecosystem with information regarding its efforts to limit passively shared browser data through User-Agent Reduction ("UAR"). In an effort to increase transparency, Google has coordinated with the CMA to publish these updates.

In particular, as announced in the blink-dev email thread, Google continued its roll-out of

User-Agent Reduction Phase 6 during Q2 2023. The final timeline for the roll-out of User-Agent Reduction Phase 6 stands as follows:

**Stable 1% [Completed]**: Feb 21, 2023

**Stable 5% [Completed]**: Mar 21, 2023

**Stable 10% [Completed]**: Apr 4, 2023

**Stable 50% [Completed]**: Apr 25, 2023

**Stable 100% [Completed]**: May 12, 2023

This updated timeline and all other timeline updates can be found on the blink-dev email thread.

# Google's Interactions with the CMA

## Efforts to identify and resolve concerns quickly

Paragraph 15 of the Commitments provides for Google to engage with the CMA in an open, constructive and continuous dialogue in relation to the development and implementation of the Privacy Sandbox proposals, in the context of which paragraph 17(a) envisages efforts to identify and resolve concerns quickly.

The intensive discussions between Google and the CMA set out below have focused on ensuring that the CMA is fully informed of developments in the Privacy Sandbox proposals, and of the underlying thinking. Google continues to respond to a continuous sequence of detailed questions in this respect. As part of this, Google provides the CMA with advance warning and an opportunity to comment on relevant Google announcements before they are published.

## CMA concerns

The CMA has not during the relevant period expressed concerns for resolution pursuant to paragraph 17(a)(ii), or notified any such concerns pursuant to paragraph 17(a)(iii) of the Commitments. However, the CMA has continued to raise detailed questions about how the Privacy Sandbox APIs would address the Development and Implementation Criteria set out in the Commitments, based on its own assessment and reacting stakeholder concerns as set out below.

## Stakeholder concerns

The CMA has shared with Google certain concerns expressed by stakeholders, a number of which overlap with issues raised in the tables above:

**Topics Taxonomy** - Google has recently announced some important updates to the Topics API, particularly the publication of an improved taxonomy compared to the one originally launched for testing and for the origin trial. The taxonomy is the list of available topics that may be returned by the API. We repeatedly received feedback that the testing taxonomy did not represent the topics that the advertising industry cared most about and that's why we decided to develop an improved taxonomy. We added 280 commercially-focused categories, and removed 160 categories which did not add much commercial value for ad selection on most sites. The new taxonomy has 469 topics, compared to 349 for the original version.

We engaged closely with the CMA and with a variety of representative stakeholders across the industry as part of the process of updating the taxonomy. The results of our

engagement has so far given us positive expectations about the improved utility for the ecosystem, but we look forward to hearing more comments on the revised taxonomy and we'll continue engaging with feedback throughout the upcoming months. Both Google and the CMA continue to ensure that design updates like these are in line with the Commitments.

**Topics Experiments** - In Q2 Google Ads published the results of its interest-based advertising testing (see the dedicated Google Ads section above). This was an experiment to understand how Google's interest-based audience solutions perform when they rely on a combination of privacy-preserving signals including contextual information, the Topics API, and first-party identifiers such as Publisher Provided IDs. The CMA had shared stakeholder feedback that Topics does not address certain advertising use cases due to a lack of frequency capping, and that Google's interest-based advertising test did not isolate Topics API results enough. Google Ads notes that for this experiment, the Topics API was one of the many signals used for ads targeting, precisely in order to assess an end-state where this broader suite of privacy-durable signals are available in a privacy-first world. Additionally, due to the limited traffic in Chrome's Origin Trials, the experiment setup could not include an additional control arm that removed data related to both 3PCs and the new APIs (but leaving ad-tech optimizations and mitigations in place), which could have enabled directionally quantifying the impact of the Topics API in isolation from other signals. Nor was it feasible for Google Ads to include an additional treatment arm in the experiment given technical constraints. Subsequent to running this experiment, Google Ads and the CMA had discussions about the appropriate metrics to report and the presentation of results (including measuring the composition of treatment and control groups). Google Ads will consider this feedback in the design of its forthcoming experiments. Chrome is currently exploring solutions to further improve Topics, and will continue to engage with the CMA and the ecosystem to do so.

**Protected Audience API (formerly known as FLEDGE API)** - As an update, In Q2 Google announced that FLEDGE API has been renamed Protected Audience API.

The CMA has shared that certain stakeholders have expressed concerns regarding the cost of Google's Bidding & Auction (B&A) Server proposal. We are conscious of this risk, and as addressed in the feedback table above, under 'B&A Services proposal will increase cost and complexity for Ad Tech compared to client side models', we are currently developing a guide for estimating costs of supporting bidding and auction workflows in the B&A server, which will be correlated with adtech usage, fulfilling one of the goals of our designs. The CMA has also shared that certain stakeholders have expressed feedback that the B&A server proposal could restrict the commercial freedom of third parties to use servers on-premise or their own choice of data center. We have addressed this in the feedback tables above, under 'Support for Trusted Execution Environments in non-public cloud environments'. We'd also like to recall that ecosystem participants are not required to use B&A servers to participate in Protected Audience API auctions, but the existence of the

option should help this API continue to serve as a way for publishers and advertisers to meet their different advertisement needs.

The CMA has also shared feedback from a stakeholder that in cases of side-by-side activation of openRTB and Privacy Sandbox, delay and complexity may undermine regular budget pacing mechanisms. We'd like to clarify that in cases of side-by-side activation across openRTB and Protected Audience API auctions, budget pacing can be supported by updating budget-related information into Key/Value servers. The Key/Value server is designed to solve for budget pacing, and facilitates real-time lookup of budget data.

In addition, the CMA shared feedback from a stakeholder that the programming language for Protected Audience API bidding algorithms is restricted. The current design of the bidding algorithms is necessarily limited as Google cannot support all languages. However, Google's support for WebAssembly (Wasm), expands language support to any language that can compile to Web Assembly including widely-used languages such as C++, Rust, and Go. We welcome feedback from the ecosystem on additional languages which stakeholders consider should be supported.

**Privacy Feedback** - The CMA shared some privacy concerns from stakeholders, including that Google should further substantiate its privacy claims regarding Privacy Sandbox, that the Topics consent screen was unclear for users, that anti-fingerprinting techniques are important as many fingerprinting techniques are worse for user privacy than third-party cookies, and that there is a concern with the continuing existence of retargeting. From the beginning of the Privacy Sandbox, Google has engaged with stakeholders' feedback on the privacy impact of our work, with the ultimate goal of building technologies that both advance user privacy and support a healthy open web. Preventing fingerprinting is a pillar of this effort, which is why Google is developing technologies to limit covert tracking, including IP Protection. Google also continues to consult closely with privacy regulators, including the ICO, to ensure that the Privacy Sandbox APIs offer robust protections for users and comply with applicable legal requirements.

**Whether Chrome-facilitated testing might trigger the Standstill requirement** - The CMA shared that a stakeholder was concerned that Google's deprecation of 1% of third-party cookie traffic for testing in Q1 2024 might trigger the Standstill requirement pursuant to paragraph 19 of the Commitments. Google is working closely with the CMA to facilitate testing of the Privacy Sandbox APIs. We'd like to reassure the ecosystem that Google's plan to deprecate 1% of third-party cookie traffic in Q1 2024 is expressly for the purposes of testing and the decision to do so was made only after consulting with the CMA. We'll work closely with the CMA to address any competition concerns before envisaging any further steps to expand deprecation beyond the 1% necessary to run the experiments.

**Stakeholder engagement with Google on the Privacy Sandbox APIs** - The CMA has shared with Google that certain stakeholders consider that involvement in W3C is too

expensive, and that GitHub is too developer-focused. Certain stakeholders consider that there is a lack of follow-up from Google following meetings. Google provides and engages in a variety of forums for discussion, in an attempt to enable all stakeholders to engage on the development of the Privacy Sandbox APIs. The Privacy Sandbox feedback form is appropriate for general and specific comments, technical and non-technical. The Improving Web Advertising Business Group is a forum for discussion via weekly calls and a GitHub repository.

Beyond the W3C, the Privacy Sandbox team has attended numerous **industry forums** and spoken to thousands of members of industry trade bodies, often in 'Question & Answers' sessions to engage directly with participants, ranging from high-level presentations to in-depth discussions of specific technologies. The Privacy Sandbox team has also interacted with market stakeholders at various **industry events** such as the Digital Marketing Exposition & Conference ('DMEXCO'), CES, Possible, and the Cannes Lions International Festival of Creativity with on-stage presentations, roundtable discussions and bilateral meetings, involving numerous individuals and participants.

More generally, the Privacy Sandbox team has been in contact with hundreds of companies in the sector for direct feedback and consultation in **one-on-one** meetings.

**Whether all ad tech participants can use the Privacy Sandbox APIs** - The CMA has shared that certain stakeholders are concerned that the use of the Privacy Sandbox APIs may be restricted to publishers, SSPs, and DSPs, and that not all ad tech participants can use the Privacy Sandbox APIs. While the Privacy Sandbox APIs are primarily designed to support ads use cases following third-party cookie deprecation, the Privacy Sandbox APIs are available via the browser to all members of the ad tech ecosystem. The APIs do have in-built privacy protections which will prevent harmful behavior by members of the ecosystem, such as sending certain data to untrusted servers. Google invites members from the industry—web browsers, online publishers, ad tech companies, advertisers, and developers—to participate in the development and testing of the proposed new technologies.

**Statements by Google on third-party cookie deprecation** - The CMA has shared that a stakeholder noted that a member of Google neglected to mention the Commitments when publicly discussing the timeline for the deprecation of third-party cookies. Chrome is working to signal to partners and the ecosystem that they should invest in, and test, relevant cookie-less technologies in preparation for the deprecation of third-party cookies. Unfortunately, in some specific instances, it is possible that a live conversation may be misinterpreted, and the importance of the Commitments lost in the reporting process. However, we'd like to reassure the ecosystem that Google is using targeted means to ensure that all members of Google discussing the Privacy Sandbox externally have the materials to talk about the Privacy Sandbox in compliance with the Commitments. We specifically train individuals within the organization about what is required when communicating externally, and extend this training to individuals well beyond the teams

more directly working on the Privacy Sandbox to ensure that all Google employees communicating externally do so in compliance with the Commitments. In addition, we have designated compliance specialists who are particularly attuned to what is needed who can validate that our external messaging is aligned with the requirements of the Commitments and to identify where further training might be helpful.

A stakeholder also commented that Google's blog on Preparing to ship the Privacy Sandbox relevance and measurement APIs suggested that the APIs are viable alternatives to third-party cookies without providing evidence, and failed to signal that Google's ability to proceed is conditioned on meeting its obligations under the Commitments. The focus of that specific blog is on the launch to General Availability and the testing of the APIs. It did not make any claims as to the utility of the Privacy Sandbox APIs as a replacement for third-party cookies, but rather invited third parties to participate in the process of adopting and testing the APIs. Although Google's blog did not expressly reference the Commitments, it did state that we have worked with the CMA to ensure our testing modes align with the CMA's testing framework, and that the "*the CMA anticipates that the results from testing in these modes can be used in its assessment of the Privacy Sandbox*". Moreover, Google noted that we will work closely with the CMA before taking any steps to expand third-party cookie deprecation.

Google recognises the importance of referring to the Commitments in its public communications, and reassuring the ecosystem that third-party cookie deprecation will only take place once the CMA's concerns under the Commitments have been resolved. Google will continue to share relevant announcements with the CMA in advance of publication.

**Whether the APIs are Google's intellectual property and could transfer control of market functions to Google** - The CMA has shared that certain stakeholders are concerned that the Privacy Sandbox APIs are Google's intellectual property and could transfer control of market functions to Google. As required under the Commitments, Google will not design or develop the Privacy Sandbox APIs in ways that will distort competition by self-preferencing Google's advertising products and services. The Privacy Sandbox is an open-source initiative. The APIs are implemented in Chromium, which is the open-source browser project that Chrome is built on. Code for the Privacy Sandbox APIs can be accessed via Chromium Code Search. Ecosystem participants are of course not obliged to make use of the Privacy Sandbox APIs and Google welcomes efforts to develop alternative, non-Google privacy-preserving technologies to support ads targeting and measurement.

**Design compatibility –** Concerns have also been raised that websites might break on other web browsers if they don't also implement Privacy Sandbox APIs, as well as the feasibility of implementing Privacy Sandbox alongside other marketing proposals. We are conscious of the importance of ensuring user experience is not compromised because of

cross-browser differences. Developers are familiar with these issues and there is already a wide range of capability support across browsers.

**Alternatives** - The CMA has shared that some stakeholders are keen to ensure that Google's technologies do not close off legitimate alternatives to Privacy Sandbox. Google's efforts are focused on developing the Privacy Sandbox Proposals in such a way that they comply with the Development and Implementation Criteria set out in the Commitments, and achieve the purpose of protecting privacy while supporting advertising use cases critical to a thriving web ecosystem. Google welcomes efforts to develop alternative privacy-preserving technologies to support ads targeting and measurement. While encouraging the development and testing of such technologies, Google will always keep in mind the privacy, safety, and security of its users.[2]

**Timeline & Industry Readiness** - The CMA shared that some stakeholders are still uncertain as to whether Google will meet the announced timeline for the phasing out of third-party cookies. The CMA also shared that advertisers are feeling 'cookie fatigue' and some are against further delay to the timeline, while some stakeholders, in particular SSPs, feel that the industry is not ready for third-party cookie deprecation. In addition, the CMA shared that certain stakeholders feel that Google should carry out tests on 100% traffic with its own properties before encouraging others to test.

Google is committed to third-party cookie deprecation and is investing significant time and resources into the APIs to ensure they meet the ecosystem's expectations with regard to their effectiveness in providing alternatives to third-party cookie functionality and meeting the Development and Implementation Criteria set out in the Commitments. We've recently reaffirmed that by publishing a detailed post on the next steps for Privacy Sandbox which hopefully resolves any outstanding concerns of this nature.

The development of the Privacy Sandbox APIs is progressing at pace. The Privacy Sandbox APIs are already available in Origin Trial for testing. The APIs will be generally available for 99% of traffic in Q3 until we reach full adoption. In its report for Q4 2022, Google published its new section "Google Ads Roadmap for Effectiveness Testing of the Privacy Sandbox Proposals", this has been updated in each quarterly report, including the current one, to raise awareness around the work Google Ads are doing and to signal to partners and the ecosystem that they should invest in, and test, relevant cookie-less technologies in preparation for the deprecation of third-party cookies.

Although third parties are of course not obliged to engage in testing, in order to further assist the industry in preparing for third-party cookie deprecation, during Q2 Google published a blog on Chrome-facilitated testing which will allow sites to meaningfully preview what it's like to operate in a world without third-party cookies. This will allow Google and the ecosystem to perform more effective API testing and improve confidence

[2] See Google's Q2 2022 Progress Report, page 22.

among stakeholders as to their readiness for the removal of third-party cookies. In addition, Google worked with the CMA which published its own guidance to third parties on quantitative testing of the Privacy Sandbox APIs at the end of Q2, which advises ad techs, publishers, and advertisers on how they can test the Privacy Sandbox tools in a way that would contribute to the CMA's assessment of the Privacy Sandbox technologies.

**Third-party cookie deprecation will benefit larger publishers and advertisers** - The CMA has shared with Google that certain stakeholders feel that third-party cookie deprecation will benefit larger advertisers and publishers, and will lead to an increase in the importance of first-party data, sign-ins, and paywalls. Google has committed to the CMA to design and implement the Privacy Sandbox proposals in a way that does not distort competition by self-preferencing Google's own business, and to take into account impact on competition in digital advertising and on publishers and advertisers of all sizes. The goal of the Privacy Sandbox APIs is to limit cross-site tracking of individuals and provide more private alternatives to existing technology while keeping the web open and accessible to everyone. We continue to work closely with the CMA to ensure that our work complies with these commitments. As testing of the Privacy Sandbox progresses, one of the key questions we will assess is how the new technologies perform for different types of stakeholders. Feedback is critical in this respect, especially specific and actionable feedback that can help us further improve the technical designs. We have worked with the CMA to develop our approach to quantitative testing, and are supportive of the CMA publishing its own guidance to third parties on quantitative testing of the Privacy Sandbox APIs.

## Status Meetings

The Commitments provide for Google and the CMA to schedule regular meetings at least once a month (before the Removal of Third-Party Cookies), to discuss progress on the Privacy Sandbox proposals. Currently, Google and the CMA typically have one substantial technical meeting a month, updating on progress and addressing an agreed agenda of testing, targeting, measurement, boundaries and user control topics to assist the CMA to carry out the regulatory scrutiny and oversight foreseen in the Commitments, as well as one legal status meeting focusing on legal, procedural, and competition considerations. Google and the CMA collaborate on the agendas for each meeting to ensure that adequate attention is given to each topic. Additional meetings are held to discuss specific issues when the need arises.

In addition to synchronous meetings, Google and the CMA typically engage with each other on at least a weekly basis. These engagements range from emails to formal written responses, and consist of questions and answers, the sharing of information, and the like.

## Standstill

Paragraph 21 of the Commitments on notification of concerns during the Standstill is not

yet applicable, as Google has not entered the Standstill Period.

# Compliance statement

The compliance statement provided for at paragraph 32(a) of the Commitments is attached.

[redacted]

**COMPETITION AND MARKETS AUTHORITY**
**Case 50972 - Privacy Sandbox**
**Compliance Statement**

I, Renée M. DuPree, Director, Competition Compliance of Google LLC confirm that for the three months to 30 June 2023, Google has complied in the preceding three-calendar-month period with the obligations relating to:

- Google's use of data set out in paragraphs 25, 26, and 27 of the Commitments;
- Google's non-discrimination commitments set out in paragraphs 30 and 31 of the Commitments; and
- Google's commitment in relation to anti-circumvention in this respect set out in paragraph 33 of the Commitments.

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

Signed.....[redacted].....

Full name..[redacted].....

Date..[redacted].....

Breaches (if any) listed on following page for completeness: Not applicable