# Privacy Sandbox Progress Report

## Q1 Reporting Period - January to March 2024

## Prepared for the CMA, 25 April 2024

## 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 unified Privacy Sandbox developer documentation with specific pages for each API, an overall status page, along with continued updates on core project processes such as Chrome-facilitated testing and preparing for third-party cookie deprecation. Key updates are shared 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 2024 Q1 updates, covering the period from January 1 to March 31, 2024.

[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 Q1 2024 Timeline Updates | |
|---|---|
| **January Timeline Updates** | • None |
| **February Timeline Updates** | • None |
| **March Timeline Updates** | • Resolved redirecting URLs in instances where we linked to developer.chrome.com. Fixed to point to correct developer.google.com destinations. |

In addition to our Q1 2024 timeline update, as we announced on 23 April, we are providing an update on the plan for third-party cookie deprecation on Chrome.

We recognize that there are ongoing challenges related to reconciling divergent feedback from the industry, regulators and developers, and will continue to engage closely with the entire ecosystem. It's also critical that the CMA has sufficient time to review all evidence including results from industry tests, which the CMA has asked market participants to provide by the end of June. Given both of these significant considerations, we will not complete third-party cookie deprecation during the second half of Q4.

We remain committed to engaging closely with the CMA and ICO and we hope to conclude that process this year. Assuming we can reach an agreement, we envision proceeding with third-party cookie deprecation starting early next year.

# Market Testing Grants

In an effort to encourage market participants to test the Privacy Sandbox APIs, Google announced on July 18, 2023 that it has made grant funding available for engineering and testing-related work to eligible SSP and DSP companies to meaningfully contribute metrics that are material to the CMA review of Privacy Sandbox. As of the end of Q4 2023, grantees have finalized and shared with the CMA their Test Plans, outlining their test setup and methodology. Grantees have begun performing their respective tests for a time period of at least 8 consecutive weeks between January 1, 2024 and May 31, 2024. Grantees are undertaking their testing in line with the CMA's guidance to third parties on testing, and will submit their results directly to the CMA. Google has been providing regular updates to the CMA on the initiative and will continue to engage with the CMA on the progress of this initiative as it develops.

# 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.

**Glossary of acronyms.**

ARA - Attribution Reporting API
CHIPs - Cookies Having Independent Partitioned State
DSP - Demand-side Platform
FedCM - Federated Credential Management
IAB - Interactive Advertising Bureau
IDP - Identity Provider
IETF - Internet Engineering Task Force
IP - Internet Protocol address
openRTB - Real-time bidding
OT - Origin Trial
PA API - Protected Audience API (formerly FLEDGE)
PatCG - Private Advertising Technology Community Group
RP - Relying Party
RWS - Related Website Sets (formerly First-Party Sets)
SSP - Supply-side Platform
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 |
|---|---|---|
| Governance | Interest in a public comment period for any governance updates to Privacy Sandbox. | We are open to reasonable stakeholder feedback on any significant developments regarding Privacy Sandbox, including the future governance of Privacy Sandbox. |
| Testing | Additional testing phases for 3PCD in addition to the current 1% Chrome-facilitated Testing. | We do not intend to offer Chrome-facilitated testing beyond the current 1% of Chrome traffic enabled since early January. |
| Web to App | 3PCD on mobile devices should not happen before full interoperability between web and app is achieved. | We agree that it's desirable to support app and web interoperability and have launched cross app and web attribution measurement and are exploring web-to-app targeting solutions. However, we are not planning to delay 3PCD on mobile web. We do not have a goal of 100% coverage at the end of 3PCD. Rather, we expect compatibility on Android for cross app and web measurement to be reasonably high at 3PCD and to increase over time as users update their phones. |
| Browser's Role | Chrome appears to be taking on the role of an ad server or SSP. | Chrome is not taking on the role of an ad server or SSP. With PA API, Chrome is providing a container for ad servers, SSPs, DSPs and other ad tech to bring their own bidding and scoring logic. |
| Use Case Guidance | Clearer guidance on what use cases will be supported by Privacy Sandbox APIs. | At the beginning of the Privacy Sandbox project the developer documentation was primarily focused on bringing developers into the discussion and feedback processes for all of the proposals. This meant the content was generally structured around understanding the motivation and concepts behind the project followed by details of the early development and testing details for each proposal.<br><br>This was effective in building real ecosystem collaboration in developing the proposals, but as the APIs have progressed through to general |

| | | |
|---|---|---|
| | | availability there is a new audience of developers who are here primarily to build on the APIs rather than contribute to their underlying development.<br><br>We have recently updated the navigation of developer.google.com/privacy-sandbox to be use case focused, using similar categorizations to the IAB Tech Lab in its recent Privacy Sandbox Task Force report. That use case-based approach to documentation is something we will continue going forward. |
| Local Development Environment | How do we continue developing and testing our frontend locally on http://localhost when the cookie is SameSite=Secure and the backend is fronted by a CDN? | We are discussing this issue here and welcome additional feedback from the ecosystem. |
| 3PCD Mitigation | Is there a programmatic way to know 3PCs are blocked or when heuristics are active? | In Chrome, both feature detection and document.hasStorageAccess called in an iframe allow a developer to know whether the origin in the iframe has access to 3PCs. |
| Video Testing | Currently unable to test video ads in Privacy Sandbox. | Chrome posted a discussion and demonstration of several possible ways that video could be accomplished with PA API today (see 242 and 254 in our demos repository on GitHub). Note that these are not intended as sample code that ad techs would adopt wholesale, but rather as a proof-of-concept and demonstration of the techniques that could support VAST video rendering with PA API.<br><br>In the course of this discussion, it has also become clear that while video rendering is already possible today, there are changes which Chrome could make that would simplify the implementation with PA API. For example, updates to macro substitution (discussed here) which we were already planning to address based on feedback about third-party ad verifier brand safety use cases, would also address feedback in the video use case, where the buyer is seeking which seller macros to use in rendering. |

| | | |
|---|---|---|
| | | Most discussion to date has been particularly focused on rendering VAST video ads. Rendering of Native ads could make use of the same approaches, and is in many ways easier. Native seems to currently be receiving less attention than video, but this is just a question of prioritization of the ad tech industry, not of any technical barrier to implementation. |
| Non-ads Measurement | 3PCD may impact non-ads-related audience measurement solutions. | The measurement APIs do not require that the use case be ads-related. While ARA is more specific to a typical advertising journey, Private Aggregation is general purpose. These two building blocks can be used to address a large range of measurement activity. |
| Content Creators | Privacy Sandbox is structured to encourage content creators to make more content for YouTube and less on their own sites. | The Privacy Sandbox initiative is focused on keeping people's activity private across an open and free internet. We know publishers rely on ads to produce content and make it as broadly available as possible. Advertisers help people discover new products or offers they may want. Privacy Sandbox features enable websites of all kinds, including those who work with content creators, to show people useful ads based on their activity with different parties, without revealing the user's identity to those parties. |
| Clearer Timelines | Clearer, more detailed release schedules for the Privacy Sandbox technologies. | Privacy Sandbox API documentation includes API status and availability pages. These pages list upcoming features and their timelines (e.g. PA API, ARA). There is a central view of these statuses here. |
| Machine Learning | Ad techs are not able to properly train machine learning models until 3PCD extends beyond 1%. | Expanding 3PCD to more browsers for testing would not guarantee that the APIs would see more usage, which is presumably what ad techs are looking for in order to further train machine learning models. If broader ecosystem usage is not what ad techs seek in order to further train machine learning models, then there is no reason to expand 3PCD as an ad tech wishing to train models on more traffic can do so today without increased 3PCD. This can be done without Chrome appearing to move forward on 3PCD ahead of the end of Standstill. |
| Unsupported Use | Self-service DSP use cases | There are multiple self-service DSPs who are |

| | | |
|---|---|---|
| Case | are not currently being considered. | regularly providing public feedback on the APIs. Several of those DSPs providing regular public feedback have also listed themselves as testers.<br><br>Furthermore, Chrome is actively engaging on typical self-service DSP topics like video and third-party ad servers. Recent weekly PA API calls have covered these topics. |
| Origin Trial | Request for OT for sites wishing more aggressive ramp up and test coverage for 3PCD. | Chrome is currently developing a first-party OT, which will allow origins to opt-in to 3PC phaseout behavior. Top-level origins that register for this trial and deploy tokens will have 3PCs blocked as if the user device had tracking protection enabled. This OT will provide a valuable opportunity for sites to perform broader testing of long-term alternatives to 3PCs, ahead of the eventual phaseout of 3PCs scheduled to take place after consultation with the CMA.<br><br>We are still working to finalize the timeline for the rollout of the OT. |
| IAB Tech Lab Report | Feedback about Privacy Sandbox received from the IAB Tech Lab Report. | We responded to the IAB Tech Lab report in detail here. We also acknowledged there that "the report raises questions around fragmented documentation, commercial requirements, third-party audits, industry accreditation, scalability, transparency and future governance, which we will engage with the ecosystem on and update our public FAQs accordingly."<br><br>We address fragmented documentation above. We address commercial requirements under "Data Guarantees" here and some Google ads products have shared their approaches. We address third-party audits under "Algorithm Integrity Guarantee" here. Regarding accreditation we would expect those bodies to continue accrediting products, including their use of technologies, instead of the technologies by themselves. Regarding scalability we continue to be open to data from developers that demonstrates issues. Regarding transparency and governance we continue developing in the open on GitHub and at forums like W3C while engaging with the CMA under |

| | | |
|---|---|---|
| | | the Commitments. |
| Google Sign-In | Google sign-ins would lead to the possibility for Google to use cross-identification log-in data contrary to the Commitments. | Google Sign-In does not enable Google to use data contrary to the Commitments. |
| Compatibility | What are plans for Privacy Sandbox APIs support and forward / backward compatibility? | Once Chrome launches a feature to general availability, we aim to maintain support for that feature. Of course it is not always possible to maintain backwards compatibility, and in such cases we have a clear process for deprecation and removal of existing features, described here.<br><br>We expect to continue to add more features to the Privacy Sandbox APIs over time, in response to ecosystem feedback about use cases that would benefit from improved support. In such cases we tend to include some kind of Feature Detection technique, so that an ad tech interested in experimenting with a new feature can directly ask the browser whether the feature is supported. This is better than asking developers to check for a certain Chrome version number, since some features may not roll out to all users of Chrome at the same time. For example, our feature detection work for the PA API can be found here. |
| Server Implementation | Rather than coupling to their own implementation, Chrome should specify the behaviors that a satisfactory implementation of a Trusted Signals Server, Aggregation Server, and any other required non-browser components, must meet. This would enable innovation within acceptable privacy boundaries. | We appreciate and welcome the desire for innovation by external parties. For all APIs and services, we aim to provide ad techs flexibility to implement their functionality. For example, we allow ad techs to use confidential business information in designing bidding logic for auctions. Moreover, we continuously engage with feedback from ad techs and, where justified, incorporate it into our designs.<br><br>To allow for others to run their own code in Trusted Execution Environments, Privacy Sandbox will need to review the code (and any changes) to confirm it does meet the privacy guarantees. This will require significant effort from the Privacy Sandbox team. Therefore, we would like to understand what benefits the |

| | | |
|---|---|---|
| | | stakeholder is looking to achieve, which aren't met by us today. |
| Heuristics | What are the long-term plans for heuristics? | Aligned with what other browsers have indicated, we intend to eventually retire these heuristics as alternative solutions become widely used, subject to further feasibility analysis. We have shared this here. |
| Testing Volume | Different traffic volume when comparing different dimensions. | The 1% experiment has exclusion criteria that lead to differences in eligibility for the experiment, between different populations of Chrome clients. For example, the experiment excludes Chrome Enterprise users, so it's expected that the fraction of traffic with experiment labels will be higher on weekends. Seeing different percentages of traffic across different data slices (such as geo, date, and platform) is to be expected, and this is in line with what we're seeing in Chrome data. |
| Manually Re-enable 3PCs | Will sites be able to know how many users (%) have manually re-enabled cookies after 3PCD is enforced? | Users will have the ability to re-enable 3PC access at the site level via User Bypass if they encounter breakage. 3PCs may also be re-enabled by other measures such as the Storage Access API. There are technical measures, like hasStorageAccess(), that allow sites to detect whether 3PCs are enabled or disabled. However, Chrome will not facilitate a way for websites to know the re-enablement reasons. |
| Tracking Protection | How long will Chrome's Tracking Protection UI feature be available? | The Tracking Protection UI in the address bar is anticipated to remain beyond when 3PCs are deprecated. |
| (Also reported in previous quarters)<br><br>Cross-browser Support | Other browser vendors adopting the Privacy Sandbox APIs. | Other browser vendors, such as Apple, Mozilla, and Microsoft, are active participants in the public forums where privacy principles and browser-based approaches are being discussed. We're encouraged by the collaborative discussions in forums like the recent W3C Annual TPAC meeting and ongoing W3C PATCG forums where we see signs of convergence. For example, Microsoft Edge recently announced its plan which "aims to maximize syntactic compatibility" with PA API and ARA while also offering additional features |

| | | |
|---|---|---|
| | | for developers. |
| Fallback option for incompatible embeds post 3PCD | Provide API hooks to detect if a third-party iframe / embed is compliant with 3PCD or not. | We are discussing the request here and welcome additional feedback from the ecosystem. |
| Testing | Request for additional flags in managed instances of Chrome that temporarily turns off the customized behaviors. | We are considering this request for managed instances of Chrome and welcome additional inputs from the ecosystem if such a flag would be useful. |

# Enrollment & Attestation

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Attestation Verification | How will Google ensure the authenticity of attestations? | All registrants are required to keep the attestation file in place while using the APIs. Google validates that the file is in place and the syntax is correct but Google does not validate the ad tech's behavior with respect to the attestation language. |
| Private Aggregation API Enrollment Process | Is there a way to check the status of Private Aggregation API enrollment? | All approved enrollees are notified via email from the Enrollment support team once the enrollment has been validated. If the registrant has any questions during the process, they can contact the support team (which they are connected with upon submitting their enrollment form). The support team will respond and answer questions and provide any additional guidance that is needed. |

# Show Relevant Content & Ads

## Topics

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| (Also reported in previous quarters)<br><br>Classifier Timeline and Documentation | There should be some form of mechanism to have classification reviewed or at least additional transparency on how classification mode determines categories. | Our response is unchanged from previous quarters:<br><br>"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." |
| Google Ad Manager | Google Ad Manager is already embedded on most sites and will have much broader information about user topics than competitors who are present on fewer sites. | The observation requirement exists to ensure the Topics API does not result in user data being shared with more entities than the technologies the API is replacing (including 3PCs). Other industry solutions such as Prebid work with 10,000s of sites and enable market participants to call Topics API through their technology. Further, it's worth noting that the limit of up to 5 top topics per week may have an equalizing effect, as market participants present on many sites who may be able to learn greater than 5 topic equivalent using 3PCs will be limited to 5. |
| (Also reported in previous quarters)<br><br>Usefulness for different types of stakeholders | Concerns about the value created and distribution of that value for sites depending on their level of traffic or how specialized their content is. | We recognise that specialized sites are more likely to contribute more granular topics than general interest domains. However, not all specialized sites contribute commercially valuable topics. Also, this dynamic reflects the status quo and is entirely independent from the end of support for 3PCs in Chrome. Also in the current environment, some sites provide more value than others in 3PC-based ad relevance systems. Additionally, topics among specialized sites can be mutually beneficial to one another as diverse advertisers can run campaigns across diverse sets of topics and bidding logic can observe value across a wide range of topics. |
| Hostnames vs Complete URLs | Is classification based on hostnames of websites sufficiently effective and does this reduce the privacy risk as compared to complete URLs? | We considered using information URLs or page titles in addition to hostnames, and determined that the potential benefits would be outweighed by the risks to user privacy and security. An example of user privacy risks include the classification of sensitive information included in the URL or page title into a user's topics. |
| Topics as a Signal | Request for guidance on how to combine Topics with | Ad tech solutions can unlock the best results by combining all available tools, such as machine |

| | | |
|---|---|---|
| | other signals, and what other signals could be useful. | learning and privacy-safe signals from privacy-preserving APIs, along with contextual data, creative data, and first-party data. Further guidance on this is available here. |

## Protected Audience API (formerly FLEDGE)

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Test Traffic Volume | Testers are reporting low volume of bid response for PA API auction. | 1. Bid density correlates with ecosystem participation in PA API, which we anticipate will continue to increase throughout 2024 and beyond. It is ultimately up to advertisers, their agencies and technology providers to determine how to allocate campaign budgets. We expect some ecosystem participants may delay their investment in various “cookieless” solutions including PA API until after 3PCD. At that time we expect they may increase their campaign budget allocation to such solutions.<br><br>2. The volume of bid requests in PA API auctions may be impacted by (1) in that publishers and their ad tech providers may decide not to initiate PA API auctions if they feel demand is low. It's up to publishers to determine priority of updating their pages and participating. We anticipate publishers may take time to test and ramp up traffic gradually for these reasons. This report also includes a response from Google Ad Manager about its publisher controls for PA API participation. |
| (Also reported in previous quarters)<br><br>Fraud / Abuse | How can the ecosystem reduce the risks and stop bad actors or buyers from positioning themselves as a desirable audience? | The reporting mechanisms of PA API ads retain the information used to distinguish humans from bot traffic today. Furthermore, current domain-based techniques of including or excluding domains can be used in PA API. This is described in more detail in our response to IAB Tech Lab’s report on Privacy Sandbox. |
| Same Origin restriction on IG owner and bidding logic URL | With same-origin requirement, endpoints for an IG owner will be forced to go through the same load balancer, which may lead to redirects being rejected. | The same-origin requirement for script loading is an important security protection. There is some detail on a proposed solution here that balances ecosystem feedback and other considerations here. |

| | | |
|---|---|---|
| Multi-Slot Private Auction | There is a great deal of room for allowing Multi-Slot Private Auctions within privacy boundaries by using noise and tighter integration with ad current practices. | We are considering this feedback and evaluating the request for multi-tag auctions against increased complexity and privacy risks associated with this feature. We discussed this issue further during a PA API Web Incubator Community Group (WICG) call here. |
| Top-level Sellers | The current structure of the PA API provides any top-level seller with significantly more data and understanding of the relative value of impressions than either publishers or component sellers. | In a multi-seller auction each seller will have a best bid. Additionally, we've learned from the ecosystem that publishers may want to consider direct-sold demand next to the best bids of each seller they work with. Looking across all of these potential monetization opportunities is necessary to determine which ad to serve. This situation, where it is necessary for some actor to see the full set of options in order to pick an ad to serve, predates PA API.<br><br>PA API seeks to support multi-seller auctions and publishers' desire to consider each sellers' best bid next to direct-sold ad campaigns, where the latter is applicable. This means there needs to be a mechanism to choose from among those monetization opportunities like there is today. We did not believe it should be the browser's role to select which ad to serve. Thus the concept of a top-level seller is necessary to select a winning ad from many possibilities. That top-level seller's logic must be able to consider the best bids from each seller the publisher chooses to work with. And that seller's logic may choose to provide information about the publisher's direct-sold campaigns where that information is available. All this information could be considered in top-level ad selection logic. This means the top-level logic sees the best bids from the PA API auction and, where applicable, any direct-sold ad options from the publisher to determine a winner.<br><br>Google Ad Manager details its implementation of PA API as a top-level seller in this report under the theme "Access to Information" below. |
| Competitive Ad Separation | Request for competitive ad separation, such as preventing ads from competing brands from | We are unaware of a way to ensure competitive separation in today's programmatic, bidded, multi-seller digital advertising ecosystem. |

| | | |
|---|---|---|
| | appearing next to each other. | However, PA API enables sellers to fetch additional real-time signals based on a combination of renderURL and hostname (representing the publisher's domain) that can be used during scoreAd() when scoring creatives. This may be used by sellers to prevent ads from competing brands from appearing next to each other, assuming the publisher would like to enforce this rule. |
| Limited Information | PA API reduces the information available to publishers such as ad value, component buyer name, advertiser name, landing page URL, creative size, response time, and bid rate as well as losing bids. | We have proposed some potential solutions here and welcome additional feedback from the ecosystem. |
| Event-level Reporting | Publishers are unable to get enough information about the ad served after the deprecation of event-level reporting PA API. | We are aware of the different reporting use cases that we must continue to support when event-level reporting is retired. This is why we have targeted the date for the retirement of event-level reporting to be no earlier than 2026. During the time between now and then we invite active participation as we engage with the ecosystem on durable paths forward which could include new ideas for obtaining information in a privacy-preserving manner. |
| Multiple SSPs | Added value from having multiple SSPs will be too low for publishers. | We do not believe this to be correct and would welcome additional feedback from the ecosystem to understand the rationale for this assertion. |
| Curation Activities | Curation activities are not possible with PA API. | We have heard feedback on the ability for sellers to use PA API to make their audience information to buyers across the web (AKA audience extension). We believe this is possible today, using the delegation functionality of PA along with business agreements. Concurrently, we are actively considering if and how we can better accommodate these types of use cases. |
| Buyer Opt-out | Buyer default opt-out is likely to cause lower outcomes for component auctions. | Whether defining a single seller or multi-seller PA auction, the seller must explicitly list out buyers in the interestGroupBuyers field of the AuctionConfig. This is based on ecosystem |

| | | |
|---|---|---|
| | | feedback that sellers have contractual agreements with some buyers and not others, so would need explicit control over which buyers to include in the auction.<br><br>We welcome further discussion on GitHub. |
| Adsize | Unable to do pre-filter based on adsize and adSlotSize. | We are working on adding this capability, and further details are available here. |
| Support for negative IG targeting | An API to support negative IG targeting: showing ads only if a user does not belong to an IG. | This GitHub issue proposed an alternative way to implement negative targeting, in which the browser directly tells the ad server which negative targeting rules should be in effect for a particular ad request. While this seems like an appealing approach, all versions of this idea that we have investigated turn out to enable the server to uniquely identify the user. |
| Digital Services Act | How can a publisher use Fenced Frames but also prevent responses containing information subject to the Digital Services Act from rendering? | 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. For each API, we have published extensive technical documentation, which should provide the basis to make necessary legal assessments. Fenced Frames are not required for use in PA API any sooner than 2026, allowing additional time for stakeholders to ensure that their use of this technology is in compliance with all relevant legislation. |
| Documentation | Is updateAdInterestGroups() temporary? | We haven't announced any plans to deprecate updateAdInterestGroup. In the future, we may apply similar privacy protections as we've publicly talked about for other IG update mechanisms, e.g. using an IP address also proxy and adding some delay before the update occurs. |
| Buyside metadata and logic ownership support for non DSPs | Request for a way to act as a proxy for DSPs. | We are aware of this feedback from non-DSP segments and are considering this request. We welcome additional feedback from the ecosystem. |
| Reporting | Request to add custom handler feature for signals bucket / value in Private Aggregation reporting. | We are aware and this feature request is on our queue for further discovery. We welcome additional feedback from the ecosystem here. |

| | | |
|---|---|---|
| Documentation | Is there a link where it is possible to view all the response headers that need to be set by the advertiser and the (delegated) owner domain? | We are planning documentation updates to clarify this and welcome additional feedback from the ecosystem. |
| Multi-tower Bidding | Request for an explanation of the workflow (training and inference) via an architecture / block diagram on how a multi-tower approach is envisioned in PA API context. | Thank you for the feedback. We have some presentations on the subject from which we anticipate building additional documentation. |
| Negative Targeting | Ability of Privacy Sandbox to protect sensitive audiences and minors from inappropriate ads, for instance gambling. | The PA API does not consider the content of the ads shown. This is in control of the ad tech developers using PA. In general, the publisher and their ad tech providers can block ad creatives within Protected Audience auctions using contextual information from the page as well as publisher rule sets. This mirrors our understanding of the ecosystem's approach to these challenges today. For buyers, the negative IG targeting functionality may also be useful for some compliance use cases. |
| API Design | Google is pushing back and wants ad techs to use a Universal bidding function thereby increasing latency, rather than different biddingLogicURLs in different IGs which is allowed. | During the course of our discussions of auction latency we have highlighted that reusing the same script across all of a buyer's IGs would make that buyer's bidding run faster. This is set out in further detail here, together with our other recommendations for improving PA API auction latency. |
| Account-based Marketing | PA API is not a clean API for account-based marketing use cases. | We welcome feedback from the ecosystem on any specific use cases that they believe are not possible and would encourage ecosystem participants to continue this discussion via our public GitHub repository or weekly calls. |
| A/B Test | When PA API is configured in GAM for a publisher, it currently must be enabled for either all inventory or none. This limits publishers' ability to run a viable A/B | **Response provided by Google Ad Manager:**<br><br>The PA API controls within Google Ad Manager (GAM) affect GAM's ability to use the API, provided the API is available to use. Publishers, therefore, can run A/B tests by using Chrome's permissions policy functionality to disable use |

| | | |
|---|---|---|
| | test. | of the API on a subset of traffic to use as a control arm for an A/B test. |
| Machine Learning | Publishers need more control over GAM's proposed use of machine learning. | **Response provided by Google Ad Manager:**<br><br>In January 2024, we launched a control that offers publishers the ability to disable our machine learning throttler, and enable PA API auctions with non-Google sellers on all of their traffic. More details on this control can be found in our help center. |
| (Also reported in previous quarters)<br><br>Top-level Auctions | Ability to use Google's publisher ad server without also giving GAM control of the top-level PA API auction. | **Response provided by Google Ad Manager:**<br><br>For the reasons explained in Google's Q3 2023 report, GAM's plans for its PA API integration do not include supporting publishers using GAM as their publisher ad server without control of the top-level auction. |
| Access to Information | GAM has access to valuable information from competitors, including contextual auction prices, signals provided by buyers to SSPs for the PA API auction, and configuration parameters from the SSPs. | **Response provided by Google Ad Manager:**<br><br>We have maintained a strong focus on auction fairness for years, including our promise that no price from any of a publisher's non-guaranteed advertising sources, including non-guaranteed line item prices, will be shared with another buyer before they bid in the auction, which we then later reaffirmed in our commitments to the French Competition Authority.<br><br>For PA API auctions, we intend to keep our promise and not share the bid of any auction participant with any other auction participant prior to completion of the auction in multi-seller auctions. To be clear, we won't share the price of the contextual auction with any component auction, including our own, as explained in this update.<br><br>Moreover, we do not use information about component auction configurations, including signals provided by buyers to SSPs, as part of our own auction. In fact, we would welcome changes to the PA API that allow component sellers to specify their component auction configurations in a way that is obfuscated from the top level seller. |

| | | |
|---|---|---|
| Component Auctions | As the top-level auction, GAM will control which SSPs run component auctions for each ad opportunity. | **Response provided by Google Ad Manager:**<br><br>As a publisher ad server, GAM offers a lightweight API for SSPs that a publisher might be working with to specify their component auction configurations via the Google Publisher Tag (GPT) API. More details can be found here.<br><br>If an SSP provides a component auction configuration via this API, then they will be included in the list of component auctions for that ad opportunity. GAM does not impose any restrictions on the component auctions included. Any SSP who desires to run a component auction will be able to do so, provided the publisher has permitted them to execute the necessary code on the publisher's page. |
| Component Auctions | GAM could apply a specific and undisclosed floor to each component auction winning bid. | **Response provided by Google Ad Manager:**<br><br>GAM has maintained a strong focus on auction fairness for years. As part of maintaining a fair and transparent auction, we do not support floor prices that only apply to specific segments of demand. That is a consistent principle in our product and will continue to be so for PA API auctions. |
| Third-party Ad Servers | Third-party ad servers would not have access to Google's participation in the higher-level auction, limiting its ability to benefit from Google SSP demand in the context of PA API. | **Response provided by Google Ad Manager:**<br><br>Currently, GAM supports testing the PA API with multiple sellers on GAM via the API described here. Participation of GAM as a component auction in other top-level auctions is not presently supported. |
| (Also reported in previous quarters)<br><br>Performance of PA API Auctions | Report from testers that PA API auctions have high latency. | We have heard concerns about latency and this is part of the reason that we have developed a number of features as part of the PA API which will make it possible for SSPs to both set limits on DSP latency as well as make improvements which can decrease latency. We recently updated our latency best practices guide which includes more information on how to take advantage of these features. We are also continuing to develop new latency improvements, some of which can be seen here. |

| | | |
|---|---|---|
| (Also reported in previous quarters)<br><br>Video Rendering | Support for video rendering using PA API and Fenced Frames. | In January we published a demo of how instream video might work in a PA auction, with additional detail on alternate approaches. We also see ecosystem players starting to propose how video rendering works for partners that integrate with them, like GAM's proposals on video compatible renderURL construction or the full E2E process.<br><br>Additionally, we are listening to ecosystem feedback on changes we can do to increase adoption, and one such change is detailed in GitHub.<br><br>We remain actively engaged with the ecosystem to identify any other obstacles to adoption that we may encounter and address them in a timely manner. |
| (Also reported in previous quarters)<br><br>Data Handling Policy | What is the data handling policy for IGs / PA API? | In the PA API design, all data stored in IGs, or about what people are in what IGs, either (i) remains on-device or (ii) is processed in the Bidding and Auction (B&A) Services running inside a Trusted Execution Environment (TEE). In both cases, the data cannot be read by any other parties, or used in any way other than to produce bids in the auction.<br><br>Some privacy enhancements that Chrome is exploring do involve interaction with a Google-run k-anonymity server. That interaction is being carefully designed to avoid sharing information about users, and to run in a TEE to ensure parity of information across the ads ecosystem.<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. We continue to work closely with the CMA to ensure our work complies with these obligations. |
| (Also reported in previous quarters) | Request to extend IGs' life from 30 to 90 days. | Such a change requires careful evaluation, weighing the benefits to the industry against the impact on Chrome users and other |

| | | |
|---|---|---|
| IG lifetime | | stakeholders. We are considering this request and welcome additional feedback here. |
| (Also reported in previous quarters)<br><br>modelingSignals | Request a new field in addition to modelingSignals that can only encode display and click information. | We have responded to this feedback with a counter proposal here. We are actively engaging with the industry to understand their views on our proposal, and are currently weighing the benefits to the industry against the impact on Chrome users and other stakeholders. |
| Additional bits in reportWin() | Provide additional bits in reportWin() from the current limit of 12 prior to 3PCD. | We are currently exploring approaches to support this use case. It is taking some time as we are also looking for approaches which can help ensure that we have a long-term privacy plan. |
| Auction Design | Requests for a single auction that returns render URLs with their corresponding score. | Sharing multiple renderURLs, and their respective score, from a single PA auction is something we considered but did not implement due to privacy concerns. We do understand the desire to avoid showing the same ad multiple times to a user on a single page and welcome further discussion on GitHub. |
| reportWin | log arbitrary fields in the reportWin() function. | This is already happening today throughout the testing period. Once Chrome will have ended support for 3PCs, the forDebuggingOnly version of the API will migrate to enable downsampled debugging, which is specified here. |
| Component Sellers | Have an independent mechanism to count its own impressions and other events and not have to be able to depend solely on ad techs' reports. | This feature request is on our queue for further discovery. We don't foresee addressing this during the Chrome-facilitated testing period. |
| Cost-per-click Billing | Implement cost-per-click billing in PA API. | We are considering this request here, and we currently see this as a request for suggestions on how to implement it with the current API surface. |
| browserSignals | Add incomingBidInSellerCurrency to reporting browserSignals spec for seller. | We are considering this request and welcome additional feedback here. |

| | | |
|---|---|---|
| Buy-side metadata and logic ownership support for non DSPs | The current design of the API could lead to a significant shift in product-level retargeting campaigns where campaigns may need to migrate to platforms that serve both as DSPs and DCO providers. | We are discussing this issue and welcome additional feedback here. |
| Buy-side metadata and logic ownership support for non DSPs | Share examples where the DSP is not the IG owner. | We understand non-bidders would like to utilize some functionality of IGs, but not others. We are actively evaluating options for addressing these use cases and welcome additional feedback here. |
| Timeout Controls | Publishers should be able to dictate the number of IGs able to participate and top-level timeout / global timeout. | We understand there is a desire for enhanced timeout controls and visibility between top-level and component seller and we are considering this request. |
| Multi Ad Size | PA API support for Multi Ad Size use cases. | We are considering this request and welcome additional feedback from the ecosystem. |
| Documentation | Is there a list of IG attributes that are subjected to k-anon? | We have responded to this question here. |
| Debugging | Improved debugging capabilities for PA API. | We recognize the importance of robust debugging tools for developers working with PA API. We are committed to enhancing the developer experience by exploring ways to better integrate .well-known file fetches with developer tools. Our goal is to provide greater visibility and troubleshooting capabilities within the development environment. We are discussing this issue further here and welcome additional feedback. |
| Labels | Do all users in the mode B treatment labels have the Privacy Sandbox APIs enabled? | Chrome experiment group assignments are randomly determined and independent of user-configured Chrome settings.<br><br>While these APIs may be available to users within specific treatment groups (e.g., treatment_1.*), their functionality can be modified or disabled through Chrome settings. - Mode B control_2 group: Inclusion in this group inherently disables the Privacy Sandbox |

| | | |
|---|---|---|
| | | relevance and measurement APIs, and this setting cannot be overridden by the user within Chrome settings. |
| API Usage | Are the call to reportWin() and the ad rendering happening in parallel or one after the other? | reportWin() is called directly after the completion of runAdAuction(). At the same time, the ad rendering process may begin when the auction result is placed within an iframe or Fenced Frame. After both reportWin() finishes execution and the ad begins rendering, the URLs provided to sendReportTo() will be fetched. |
| (Also reported in previous quarters)<br><br>A/B Testing Support | Request support for PA API A/B testing. | We are discussing this request here and welcome additional feedback. |
| Traffic Shaping | Proposal from Google to manage the required decision making via KV server is not helpful, as sellers are unable to interact with their backend, making traffic shaping challenging. | As discussed in the GitHub issue, exposing whether an individual DSPs have IGs present could have user fingerprinting concerns. We have suggested other alternatives in the issue and are open to further suggestions. |
| Traffic Shaping | Caching mechanisms add a significant layer of complexity and prevents DSPs from knowing the true shape of traffic they would be bidding on. | Caching mechanism was simply offered as a suggestion. AdTechs can choose to use the suggestions that serve their use-case and we welcome additional discussion here. |
| Labels | Chrome should share the label as a parameter in requests to buyer and seller trusted servers. | This appears to be a reasonable request as it appears to be broadly aligned with the goal of responsible IG data utilization. However, we're considering the request, subject to internal review, and will provide public updates on this matter as discussions progress. |
| API Usage | Clarifying the explicit definition of the "control_1" group in the "Additional CMA guidance to third parties on testing" document. Specifically, there's concern that a change in wording might be misinterpreted as | We have expressed our views on this in this GitHub thread. That said, we are not in a position to speak for the CMA and we suggest raising any issues regarding the interpretation of their testing guidance directly with the CMA. |

| | | |
|---|---|---|
| | requiring the exclusion of all Privacy Sandbox APIs from control_1. | |
| API Usage | Will Chrome allow calling joinAdInterestGroup() on a blank page while redirecting to another resource? | If a user is visiting some site, then the site owner can delegate the ability to call joinAdInterestGroup to a third party. This delegation lets a third party build IGs without needing to add any kind of redirect through a blank page.<br><br>We welcome feedback on specific reasons to build IGs in the middle of a redirect instead of using the intended delegation mechanism. |
| API Usage | Exchanges should be able to write IG's to the pages owned by the publishers they work with and that they can then delegate the permission to bid on that IG to any given buyer or DSP. | We have received the feedback and are evaluating whether such a request could be supported. We welcome additional feedback from the ecosystem. |
| API Usage | There is no debugging loss notification if no one wins a PA API auction. | Chrome's reportWin and reportResult functions are designed for event-level win reporting within the Privacy Auction (PA) system. In circumstances where all bids are rejected during a PA auction, these functions are not expected to be invoked as no winner is determined.<br><br>A recent update to Chrome may explain discrepancies where URLs passed to forDebuggingOnly.reportAdAuctionLoss() are not appearing in the DevTools Network panel. We recommend verifying this functionality using either a Canary or Dev channel build of Chrome. |
| API Usage | Can adCost returned from generateBid be negative (it is already stochastically rounded to 2 bytes)? | AdCost is the advertiser's click or conversion cost passed from generateBid() to reportWin(). This value can be Null or a double. Negative values will be ignored and not passed. The value will be stochastically rounded when passed. |
| API Improvement | Can Trusted and Encrypted Execution servers be used to handle the targeting / cohorts / attribution and | We recommend exploring the TEE-based components and options in PA API (e.g. KV servers and B&A Services) as well as the TEE-based components of Attribution |

| | | |
|---|---|---|
| | auctions rather than the Chrome browser? | Reporting and Private Aggregation (e.g. Aggregation Service) which address this question. |
| API Improvement | Can the Privacy Sandbox auction response be a bid response (like header bidding) rather than an ad response (like ad tags)? | This type of change fundamentally changes the privacy properties of the PA API, so is not something we are considering. |
| Publisher Controls | Can publishers block PA API creatives on their pages? | Chrome has a proposal for real-time creative scanning that is not yet available for testing.<br><br>While this is not yet available, we've observed most SSPs have created solutions to enable this. |
| API Usage | What is the size limit on perBuyerSignals? | In its classic form, perBuyerSignals carries no inherent size limitations within Chrome. The primary constraints are that the data remains JSON-serializable and does not cause excessive memory consumption. However, it should be noted that very large and complex perBuyerSignals may negatively impact performance.<br><br>An alternative method exists for passing perBuyerSignals via the directFromSellerSignalsHeaderAdSlot. This approach transmits perBuyerSignals within a header, subject to a 10kb maximum size limit for the entire header response. Additionally, individual servers may impose their own restrictions on maximum header size. |
| Documentation | The documentation on call registerAdBeacon from inside generateBid needs to be changed. | We updated this documentation on February 17. |
| API Usage | How does reportEvent choose the right beacon URL from multiple registered options? | Each auction results in a separate config, which in turn results in a separate reporting map. Individual auctions (and their resulting frames) are completely separate from each other, and do not share data.<br><br>The "Fenced Frames Ads Reporting" explainer provides more details on this topic. |

| | | |
|---|---|---|
| Chrome UI | Add filter in Chrome DevTools "Application -> "Interest groups" tab, allowing to filter by IG owner (or maybe also by IG name). | We are evaluating this request and welcome additional feedback from the ecosystem. |
| Headless Chrome | PA API support in Headless Chrome. | There are some components of PA API that are tied to Chrome, for example the k-anon calls to Google's servers, which may not work in the "old" Headless Chrome.<br><br>We believe that this may be addressed by the "new" version of Headless Chrome released in Chrome 112. |
| API Usage | In the case of loss reporting with reportAdAuctionLoss, we are seeing the "topLevelWinningBid=0" in many cases. What is the interpretation of this? | The topLevelWinningBid value originates from the scoreAd() function within the top-level seller component. This value plays a role in determining the outcome of the top-level auction.<br><br>As per the explainer, a topLevelWinningBid value of zero or any negative number signifies that the corresponding ad is ineligible to win the auction. This mechanism can be employed, for instance, to filter out interest-group targeted ads that do not surpass a contextually-targeted candidate.<br><br>While a zero-valued topLevelWinningBid may indicate that a contextual auction has prevailed, the PA API specification acknowledges that other factors could contribute to this outcome. |
| Mode A/B Testing | Clarification on Mode B and Mode A traffic selection and opt-out prompts. | The inclusion criteria for Mode A and Mode B are the same. The aim is to have groups that are representative of normal Chrome traffic as long as they support the Privacy Sandbox APIs and the labeling method, as such some client configurations are not compatible. For the purposes of the experiment, it's important to only compare labeled traffic to other labeled traffic.<br><br>Users in Mode B have the Tracking Protection feature enabled and as such, they receive a notification about that feature. |

| | | |
|---|---|---|
| API Improvement | Can "lifetimeMs" be included as a direct property within the joinAdInterestGroup call or manage it as a separate argument? | We are carefully considering feedback from the web development community regarding the "joinAdInterestGroup" functionality within the PA API proposal. A key discussion point focuses on the optimal method for managing IG lifetimes. We're evaluating the benefits of a separate argument for the "lifetimeMs" parameter, as it promotes flexibility and adaptability for potential future enhancements to the specification. We are discussing this issue here and welcome additional feedback. |
| API Usage | Potential for increased false negative rates in the PA API framework due to collisions with low-entropy browser IDs. | The Chrome team is actively engaged in the ongoing refinement of the PA API framework. We appreciate the discussion regarding potential false negative rates arising from browser ID collisions. We are carefully evaluating this feedback and will work to ensure that updated analyses comprehensively reflect all relevant factors. Our commitment is to a solution that achieves the desired privacy outcomes while maintaining accuracy and reliability. We are discussing this issue here and welcome additional feedback. |
| API Usage | Is a low-entropy browser identifier necessary to prevent clients from repeatedly submitting "Join" requests for the same object in a k-anonymity system? | We acknowledge and appreciate the ongoing discussion regarding the use of browser identifiers in the implementation of k-anonymity systems. We understand the concerns raised about the potential privacy implications of such identifiers. While our initial implementation employed a low-entropy identifier as an anti-abuse mechanism, we are actively exploring alternative techniques, such as Anonymous Counting Tokens, that prioritize user privacy while maintaining the integrity of the system. We are committed to finding solutions that balance responsible data usage with robust privacy protections, and we welcome continued dialogue with the research community. We are discussing this here and welcome additional feedback. |
| API Usage | Does AMP (Accelerated Mobile Pages) support PA API. | AMP currently does not natively support PA API. We welcome additional feedback from the ecosystem if support by AMP is a high priority. |

| | | |
|---|---|---|
| API Improvement | Consider removing the type from k-anonymity checks. | We are carefully considering the feedback on potentially optimizing k-anonymity request structures. We understand the suggestion to consolidate parameters and potentially unify types to streamline the process. Our goal is to ensure efficiency and maintainability, and we're evaluating all options as we continue to develop our privacy solutions. We are discussing this issue here and welcome additional feedback. |
| Chrome UI | Request for mechanism for less-technical users to easily view and manage the IGs they belong to, including potential website-level controls for opting out. | We recognize the importance of providing user-friendly tools for understanding and managing IGs. We've carefully considered various methods and find that identifying IGs by the website where they were joined offers the best balance of clarity and privacy protection. Currently, global management of IGs is located within Chrome's settings. We're continually exploring ways to further enhance the user experience in this area. We are discussing this issue here and welcome additional feedback. |
| API Safety | Is PA API vulnerable to privacy leaks through creative ad interactions, even within the context of Fenced Frames? | We acknowledge the potential for information leakage through sophisticated ad interactions. We are actively investigating the interplay between Fenced Frames, PA API, and potential attack vectors. Mitigating privacy risks is a top priority, and we're committed to developing robust solutions that balance innovation with user protection. We are discussing this issue here and welcome additional feedback. |
| Latency | Is the default of 50ms timeout for buyer bidding logic a realistic value? | We acknowledge the concerns raised about potential inconsistencies between the specification and the timing of network requests for bidding logic. We are actively reviewing the specifications to ensure their accuracy and investigating the optimal default timeout settings to balance performance and feasibility. We are discussing this issue here and welcome additional feedback. |
| Documentation | Potential timing leak in the specification where a website could infer whether an ad failed the k-anonymity threshold, and potential | We recognize the issue raised regarding a potential timing leak. We've confirmed a discrepancy in the specification and are taking steps to ensure that the k-anonymity status of ads is determined prior to the auction to prevent such leaks. We take these concerns |

| | | |
|---|---|---|
| | implications for cross-site tracking. | seriously and will update the specification to reflect these changes. We are discussing this issue here and welcome additional feedback. |
| API Usage | Ways to implement an SSP blocklist within the PA API. | We recognize the need for mechanisms to manage ad restrictions by SSPs. We encourage exploring solutions that prioritize on-device evaluation and leverage existing ad metadata to protect user privacy while enabling flexibility. We're committed to working with developers to identify optimal approaches within PA API. We are discussing this issue here and welcome additional feedback. |
| API Usage | Can someone tell their browser to pretend to do PA API in a way that sites cannot detect? | We acknowledge that, in its current form, opting out of PA API could be detectable by websites. We're actively working on features like Additional Bids and Negative Targeting, along with Fenced Frames rendering, to enhance privacy and work towards providing undetectable opt-out options. We are discussing this issue here and welcome additional feedback. |
| Mode A/B Testing | Data center traffic purporting to be treatment 1.1. | The Chrome team has confirmed with the GAM team that this traffic is now being filtered out of the experiment. We are discussing this issue here and welcome additional feedback. |
| API Usage | Efficiency and fairness of the interestGroupBuyers implementation in PA API. | We recognize the ongoing discussion about the efficiency and fairness of the "interestGroupBuyers" field in PA API auctions. We acknowledge the trade-offs between efficiency, privacy, and market fairness. While sellers need to manage business relationships with buyers, we're exploring ways to optimize the matching process. These may include dynamic adjustments based on real-time data and hybrid models. We remain committed to finding solutions that prioritize user privacy and support a competitive advertising ecosystem. We are discussing this issue here and welcome additional feedback. |
| Chrome UI | Potential memory concerns and UI clarity related to IG in Chrome. | We understand the concerns raised about displaying IGs in DevTools. While the current view reflects all IG events for historical tracking, we acknowledge the value in providing clearer |

| | | |
|---|---|---|
| | | visibility into the current state of stored IGs. We'll explore optimizations and potential UI improvements to enhance developer insights.<br><br>Regarding memory management, the IG implementation is designed to prevent memory leaks, but we continuously monitor and optimize resource usage. We are discussing this issue here and welcome additional feedback. |
| Documentation | The original poster is encountering an error when attempting to use named ad sizes directly within the "sizeGroup" field of the "joinAdInterestGroup" function. They want to know if this is intended behavior. | We recognize the value of streamlining ad configuration within the "joinAdInterestGroup" function. We are actively working to address this limitation and plan to enable this functionality in future updates. This enhancement aligns with our commitment to provide developers with flexible and efficient tools for ad management. We are discussing this issue here and welcome additional feedback. |
| Chrome-facilitated Testing Label | Request to have direct data about Mode A vs B and exact labels in sendReportTo so that we can track the experiment consistently. | We are discussing this request here and welcome additional feedback |
| Documentation | Is the seller's domain name included in requests made to a seller's trusted server for validation purposes? | We acknowledge the initial omission of the hostname parameter from the Protected Audience KV Server API documentation. We want to assure developers that the seller's domain name is automatically included in requests to the seller's trusted server. This functionality is essential for robust ad validation processes. We have updated the documentation to address this oversight and will continue to prioritize clarity and transparency for the developer community. We are discussing this issue here and welcome additional feedback. |
| API Usage | Potential methods to include the IG name within ad impression tracking calls for reporting purposes. | We are committed to balancing the need for robust reporting mechanisms with the fundamental principle of user privacy. The inclusion of IG names in ad impression tracking is subject to k-anonymity safeguards designed to prevent the identification of individuals. We will continue to explore innovative reporting |

| | | |
|---|---|---|
| | | solutions within these privacy constraints. We are discussing this issue here and welcome additional feedback. |
| API Feature | Request for the buyer trusted server to receive Client Hints HTTP headers. | We are tracking this feature request here. |
| API Usage | Whether the delegation file should require the "Access-Control-Allow-Origin" header to load, given that it dictates IG membership behavior for the browser? | We are committed to aligning with web security best practices. The requirement of the "Access-Control-Allow-Origin" header for delegation files ensures consistency with CORS principles and prevents the unintentional exposure of sensitive information. We are exploring ways to optimize this process while maintaining a strong security posture. We are discussing this issue here and welcome additional feedback. |
| API Usage | Enable ad servers to personalize creatives within the PA API framework. | We recognize the role ad servers can play in creative personalization. We are actively exploring solutions to empower ad servers within PA API, such as the 'joint IG' model where bidding and ad creative selection logic could be combined. Our goal is to strike a balance between enabling robust ad creative capabilities and safeguarding user privacy. We welcome further collaboration and feedback on evolving the API to accommodate the needs of all stakeholders here. |
| Privacy Concerns | Availability of alternate identifiers (e.g., RampID, ID5) in contextual bid requests could undermine the privacy goals of PA API by facilitating cross-site data collection. | We recognize the potential tension between cross-site identifiers and the privacy objectives of PA API. While publishers can choose to share such identifiers, the design of PA API fundamentally aims to decouple ad selection from the need for cross-site tracking. We are committed to fostering a privacy-centric advertising ecosystem and encourage developers to prioritize the PA API approach. We are discussing this issue here and welcome additional feedback. |
| Caching | Is there a way to prevent the reuse of bidding scripts across multiple auctions? | We acknowledge the observed caching behavior of bidding scripts within the PA API framework. While standard HTTP caching mechanisms are supported, the potential for script reuse across auctions exists due to |

| | | |
|---|---|---|
| | | device suspend behavior and the design of bidding executors. The team is investigating solutions to provide buyers with greater control over script caching to manage their bidding strategies effectively. We are discussing this issue here and welcome additional feedback. |
| API Usage | Centralize reporting of bidding activity across all IGs for a DSP, while respecting user privacy. | We prioritize user privacy when designing PA API. While direct reporting of individual bidding events is not feasible due to cross-site tracking risks, we offer mechanisms like Shared Storage and Private Aggregation. These enable DSPs to gain aggregated insights on bidding activity, in a manner that upholds user privacy. |
| API Usage | The fetch from sendReportTo() in reportResult() only happens 94% of the time relative to getting a fetch registered with forDebuggingOnly.reportAdAuctionWin(). | While they may not have the same timing, it is possible for both URLs to be fetched at the same time.<br><br>In some instances, the component seller's worklet was disposed of and needs to be reloaded to then run the reportResult() function. However, neither the time it takes to fetch the scoring logic nor the time for the worklet to reload affects the 50ms timeout of for reportResult(). Please note that Chrome will use caching headers to define its fetching behavior in cases where the worklet needs to be reloaded.<br><br>You can learn more about the phases of a PA auction here. |
| K-anonymity | Request for confirmation that the name of the interestGroup does not affect the k-anonymity of ad serving. | For a creative to be considered k-anonymous, the tuple of IG owner URL, bidding script URL, creative URL, and ad size must meet the specified threshold (k) over a past time period (w). The k-anonymity status is updated periodically (p). |
| Chrome UI | Proposal to provide the type of "internal visibility" that lots of MVC, ORM, etc frameworks offer. E.g. start with simple logging of selected internal events to a new panel in the Dev Tools --> Application --> Application section | We are discussing the proposal here and welcome additional feedback. |

| | | |
|---|---|---|
| Chrome UI | Dev Tools IG joining doesn't show priority related elements. | We have addressed this issue here. |
| API Improvement | It would be preferable to allow the creative ad server to track its own events. Could a list of allowed tracking domains be configurable? | We have shared a proposal here and welcome additional feedback from the ecosystem. |
| API Feature Request | Can PA API be extended to support non-RTB media transactions and maintain critical use cases such as ad serving and DCO? | We are discussing the issue here and welcome additional feedback. |
| Publisher Auction Timeout | Publishers need control over auction duration to prevent lost impressions, especially in header-bidding setups where ads are selected sequentially. | We acknowledge the importance of giving publishers granular control over ad auction timeouts. We are actively exploring how to implement a global auction timeout mechanism, potentially within the "auctionConfig" object, while carefully considering the edge cases. This feature aims to optimize impression fill-rates for publishers, and we will continue collaborating with the community to find the best solution. We are discussing the issue here and welcome additional feedback. |
| API Improvement | The current design of IGs in PA API leads to large metadata sizes due to lengthy renderURLs. Testers would like a way to compress these URLs for greater efficiency. | We recognize the importance of optimizing IG metadata size, particularly for efficiency-sensitive ad auctions. We think a template-based solution for compressing renderURLs offers significant potential. We will carefully evaluate the proposed template designs and ensure that any implemented solution includes robust abuse-prevention mechanisms to maintain browser stability.<br><br>Collaborating with the web standards community to develop the optimal approach, with these considerations in mind, remains a priority. We are discussing the issue here and welcome additional feedback. |
| API Usage | Testers handling native ad formats want to optimize the Privacy Sandbox auction process by retrieving | We recognize the performance concerns raised for native ad rendering in the Privacy Sandbox. We are committed to finding a balance between efficiency and strong user privacy protections. |

| | | |
|---|---|---|
| | multiple ad results in a single call to reduce network load and improve ad rendering speed. | While returning multiple ads with full scores compromises privacy, we are actively exploring ways to optimize the auction process.<br><br>We are dedicated to enhancing PA API support for native ad formats and investigating alternative mechanisms to improve efficiency within the strong privacy constraints of the Privacy Sandbox. We are discussing the issue here and welcome additional feedback. |
| API Usage | Flexibility in how ad bids are scored and sorted within the Privacy Sandbox, especially to represent priority levels or private marketplace rules. | We understand the need for fine-grained control over ad scoring and sorting within the Privacy Sandbox, particularly in complex bidding scenarios. We acknowledge the proposed solutions using tuples and mathematical functions to achieve multi-dimensional scoring without sacrificing user privacy. While these approaches may add complexity for developers, they offer the necessary expressiveness.<br><br>We are committed to exploring ways to streamline these processes, potentially through helper functions or guidelines, to ensure optimal use of Privacy Sandbox features for advanced auction logic. We are discussing this issue here and welcome additional feedback. |
| reportEvent() | Add a new reserved event (automatic beacon perhaps) fired by the browser once a frame with an ad creative is initialized. | We are discussing this request here and welcome additional feedback. |
| adCost | Allowing breakdown of adCost. | Each cost value is an opportunity to send a limited amount of information out of the auction. Allowing a whole list of N of those costs would be enough to send a whole user identifier, which would enable cross-site tracking. We are discussing this here and welcome additional feedback. |
| resolveToConfig | Should resolveToConfig be inherited from the top level and exposed in browserSignals? | We are discussing this request here and welcome additional feedback. |

| | | |
|---|---|---|
| Better Tools | Is there something akin to chrome://topics-internals but for PA API? | There is nothing exactly the same. However, there is extensive developer tooling for PA API. |
| Labels | Can Chrome use labels to identify the 20% k-anon population? | We are considering this request and welcome additional feedback from the ecosystem. |
| Documentation | Will Privacy Sandbox auction worklets become standard worklet types? | Due to unique privacy and security requirements, these worklets differ significantly from standard browser worklet types, so we do not anticipate that they will become standard worklet types within the HTML specification soon.<br><br>We are committed to enhancing our developer resources with clear explanations about the implementation and execution environment of auction worklets, making this information more accessible for Privacy Sandbox participants. We have discussed this further here. |
| Bring-Your-Own-Server (BYOS) Key-Value (KV) server | Parties may be able to learn multiple IGs (from the same owner) joined by a user through KV services queries in a BYOS KV Service setup. | This will no longer be possible when KV servers run in TEEs and we can ensure they can abide by the published trust model. |
| userBiddingSignals | update part of the "userBiddingSignals" while maintaining others. | This is already possible without any changes required to the API. |
| API Usage | Implement frequency capping across multiple IGs within the Privacy Sandbox, potentially using the KV server or modified "prevWinsMs" data. | We acknowledge the desire for advanced frequency capping capabilities within the Privacy Sandbox. We recognize that current restrictions on data sharing across IGs can present challenges when implementing these strategies.<br><br>While the KV server provides a potential mechanism with appropriate privacy safeguards, we encourage developers to explore solutions within a single IG model. We are discussing this issue here and welcome additional feedback. |
| API Usage | Component sellers (those participating in nested auctions within the Privacy | We recognize the need for improved timeout coordination between top-level sellers and component sellers within the Privacy Sandbox. |

| | | |
|---|---|---|
| | Sandbox) need visibility into top-level auction timeouts to optimize their own configurations and avoid unnecessary delays. | We are actively investigating the addition of new timeout mechanisms, including a potential whole-auction timeout and exploring ways to apply top-level timeouts to component auctions. Our goal is to enhance efficiency and predictability for all participants in the Privacy Sandbox auction process. We are discussing this issue here and welcome additional feedback. |

## Protected Audience Services

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Trusted Execution Environments (TEEs) | More expensive to run TEEs in public clouds as opposed to on-premise ad tech data centers? | Our response is similar to previous quarters:<br><br>Our current TEE security model benefits from the practices of public cloud implementations. In particular, current hardware-based TEEs do not defend against all physical attacks. Our existing supported public cloud providers, AWS and GCP, designed and implemented mitigations for physical access risks, including from employees. See further details below regarding on-premise support.<br><br>Ad techs have mentioned to us that running cloud services is more expensive than on-premise ad tech data centers. While we are not in a position to evaluate those statements, we welcome additional feedback on costs and continue to evaluate options for expanding our TEE support. |
| TEEs | Support for TEEs in non-public cloud environments | Our response is similar to previous quarters:<br><br>While we are continuing to explore support for options beyond public cloud-based solutions, we have no current plans to support on-premise TEEs. At this stage, 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 (for example, supporting Google Cloud in addition to AWS) is the most beneficial for the ecosystem. However, we welcome additional |

| | | |
|---|---|---|
| | | feedback on why such a requirement is necessary and feasible given the privacy and security constraints. |
| Other Cloud Providers | Support for other cloud providers | We are always open to suggestions for other cloud providers, but currently we are planning at least to support GCP and AWS when 3PCD is enforced. Refer to this explainer for more information. |
| B&A Services API | What is Google's direction for the B&A Services API? Will it be prioritized above or below the Chrome browser Protected Audience on device auctions? | Our response is similar to previous quarters:<br><br>We remain committed to the current Protected Audience on-device bidding design. The B&A services have been proposed to explore possible solutions to support a subset of use cases where the computational power or network speed of the device may be limited. |
| Standardization | B&A services have not gone through a standardization process. | The B&A Services proposal is in the middle of one phase of the standardization process, and we welcome additional engagement in support of that goal.<br><br>It began with a proposal (based on previous proposals), it is being publicly incubated through extensive open discussion at W3C and interested developers are able to begin experimenting with it and providing feedback. This is the usual pattern for web feature development, as described for example in our blog post here. |
| KV Server | Expose full URL to buyer's KV server for content / contextual / site targeting. | We are discussing this request here and welcome additional feedback from the ecosystem. |
| Documentation | The documentation for "Trusted/Enforced components vs. optional" on GitHub causes confusion with some ad techs who have their own set of deployment images and infrastructure. | We are looking to improve the documentation for "Trusted/Enforced components vs optional", and am interested in hearing from the ecosystem if such work needs to be prioritized. |
| API Improvement | The HTTP Status Code of a KV server call should also be available to the scoreAd() | We are evaluating this request and welcome additional feedback from the ecosystem. |

| | | |
|---|---|---|
| | function as a parameter. | |
| Documentation | Provide more information on how JS and WASM workloads would be handled exactly with the UDF execution. | We are looking into providing this information and welcome additional feedback here. |
| Documentation | Request to update repo name. | We have renamed the repository to "protected-auction-key-value-service".<br><br>This is in line with the term for the collection of services this belongs to, which also has other repositories such as the Protected Audience Services discussion, and the Protected Auction Services documentation repos. |
| Documentation | Remove reference to Cloud debugger API in bidding_auction_services_gcp_guide.md. | We have updated the documentation and removed the reference. |
| API Usage | Latency introduced by the KV lookup is taking more than 50ms. It's taking nearly 100ms.<br><br>Do you have any guidance on what's been working well for other sellers? Do you have any suggestions on how to measure the timeouts and timing? | The KV server call happens inside the context of the Script Runners, i.e. the special protected environment inside of the Chrome browser. It is intended to keep information in these script runners protected from any non-API access. We have provided a detailed explanation here. |
| API Usage | Is there a timeout for the KV server to respond in a particular time? | Sellers can specify the "perBuyerCumulativeTimeouts" field in the auction config. This timeout includes the time needed to fetch trusted bidding signals. |
| Latency | How is the Privacy Sandbox team working to address latency? | For strategies we are exploring to keep the latency within acceptable limits, see here. |

# Measuring Digital Ads

## Attribution Reporting (and other APIs)

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

| | | |
|---|---|---|
| Manual Campaign Optimization | ARA does not support manual campaign optimization. | We have discussed this scenario with the ad tech and shown ways in which ARA can be used to support manual campaign optimization. ARA has been built in a way that allows for ad tech customization and flexibility to solve a range of ad tech use cases. A few suggestions that were provided included using different flexible event-level configurations and, using event-level reports with summary reports to reduce the impact of noise and to achieve their manual and automatic optimization needs. We are open to additional ecosystem feedback regarding the customizability and flexibility of ARA configurations. |
| Conversion Type | Google is only allowing eight conversion types which is limiting. | We have implemented the majority of Flexible event-level reporting, which gives ad techs additional flexibility in terms of the number of reporting windows, number of attribution reports, and bits of trigger data that they can use. Ad techs can choose a configuration that allows measuring up to 32 different conversion types. |
| Aggregatable Report Event Limit | The numerical minimum of 20 conversion events per aggregable report is not workable for smaller advertisers with limited budget. | There is no minimum number of conversion events needed per aggregatable report.<br><br>Additionally there are a number of design decisions that can be made to optimize aggregatable reports for smaller advertisers such as changing the key structure / dimensions tracked, testing different levels of epsilon, testing longer batching frequencies, and testing different contribution budget allocations between measurement goals. Smaller ad techs can also experiment with combining event-level reports and summary reports as a way to reduce the impact of noise. |
| Real-time Data | Depriving DSPs of real-time data (e.g. on clicks, sessions, and conversions) which DSPs use to adapt their bidding strategy and achieve better campaign effectiveness, goes against the commitment to maintain existing functionalities. | Even with ARA, clicks and sessions remain real time, and conversions are always after the fact even with 3PCs. |

| | | |
|---|---|---|
| Missing Fields | Missing requirements in the Full Flexible event rollout: i) Currency field, and ii) orderID / TransactionID field. | We do not plan to support a Currency field or Order ID / Transaction ID field currently as part of full flexible event-level because there are already ways to do this with current event-level reporting. We are open to additional feedback regarding these fields, and will reconsider if there are additional use cases that require these.<br><br>The ways to use ARA's current design to measure currency and order ID type information:<br><br>1. Based on the feedback, the currency is determined by a user's geo, which can be added as part of the source_event_id as a way to determine what currency was used.<br><br>2. Based on the feedback, the order ID field is needed to ensure conversions and values are not double counted by mistake, which can be done by using deduplication keys. |
| Privacy Budget | ARA Privacy Budget limits the ability to measure across multiple dimensions | ARA has been designed in such a way as to allow ad techs to customize their own ARA configurations to cover a variety of attribution scenarios. With the current ARA design ad techs will need to think about the trade off between what dimensions are most crucial for them to measure and the impact of noise on their data. Adding noise to the data depending on the granularity of dimensions that are being measured is essential for privacy.<br><br>We are open to additional ecosystem feedback regarding the ability to measure across different dimensions, but would need to understand the specific use cases that require this. |
| Update Specification | Although Google has said it has moved from fixed to flexible event reporting windows, this has not been reflected in Google's Technical Specifications which still currently has a minimum window of one hour. | Flexible event-level reporting currently allows ad techs to change the number of attribution reports per source event, the bits of trigger data, and the number/length of reporting windows. ARA still has a minimum reporting window of 1 hour for event-level reports which is essential to maintain privacy and mitigate against certain types of history reconstruction attacks. |

| | | |
|---|---|---|
| | | Since summary reports provide information in aggregate, ad techs can opt in to receive aggregatable reports immediately with no delay, if needed for their use cases. |
| API Design | Concern that reducing information in conversion reports and adding noise could impact the ecosystem more than Google. | 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. |
| Attribution Correction | ARA doesn't allow the tech provider to control and verify the correct attribution. | There are many available solutions within ARA that provide verification capabilities:<br><br>1. Ad techs can verify that ARA behavior matches their expectations:<br>– ARA client-side code is open-sourced.<br>– ARA server-side code is also open sourced, and Coordinators ensure that only allowed versions of Aggregation Service can decrypt and process aggregatable reports.<br><br>2. Chrome has provided ad techs with a Simulation Library to verify attribution behavior, where the ad tech can test how ARA performs attribution in a mock environment.<br><br>3. ARA supports a number of debug signals that help to verify whether or not and why expected processing may not have occurred. |
| (Also reported in previous quarters)<br><br>Noise | Feedback that the level of noise is too high and it is impacting the usefulness of the reporting. | We have spoken to ad techs with this same feedback and were able to identify ways in which ARA can be customized to better suit their use cases, even with noise. We have developer documentation that contains the majority of design decisions and customizations that we discussed with the ad techs.<br><br>ARA has been designed in a way to allow ad techs to customize their own ARA configurations to cover a variety of attribution scenarios. But ad techs will need to think about the trade off between what dimensions are most crucial for them to measure and the impact of noise on their data. |

| | | |
|---|---|---|
| | | We are open to additional ecosystem feedback regarding the impact of noise and can provide additional guidance on ARA levers that can be used to change the impact of noise. |
| Cross-domain Attribution | How to track the attributions that are cross domain? | Ad techs can redirect to different reporting URLs to solve for this use case. We are open to additional ecosystem feedback regarding this design aspect of ARA. |
| API Improvement | Regularly change the scaling factor used when registering attribution for ARA Summary Reports. | Based on the discussion on GitHub, it seems that handling multiple scaling factors in Aggregation Service will most likely result in a higher amount of noise added to summary reports versus the current functionality.<br><br>We are open to additional feedback regarding the need for scaling factors as part of aggregatable reports, but want to call out the potential trade off with increased noise. We are also evaluating whether other future ARA features may help to solve this use case as well. |
| API Usage | Opportunity to unify how attribution events get shared with all participants which is beneficial for SSP, DSP, etc. | We plan to sync with ad tech to better understand their feedback and any limitations they are running into. |
| Test Traffic Volume | Is the test traffic for Mode B for all Chrome stable? | Inclusion in an experiment group is unaffected by (independent of) Chrome settings. |
| Documentation | Support ARA for pixels. | We have published information about how to support this use case and welcome additional feedback from the ecosystem. |
| API Usage | ARA may not be attributed to the correct source for third-party sellers on ecommerce platforms if the conversion is not done by the last touch. | Companies can use filters to prevent incorrect attribution from happening (as in no conversion report will be generated). We are also working on a proposal for pre-attribution filtering to help with this use case. |
| Browser Support | Will ARA be supported in different browsers? | We welcome other browsers to adopt the Privacy Sandbox APIs and continue to dedicate time to discussing our approach in the open at W3C.<br><br>We have explicitly stated interoperability as a goal for shipping ARA and ARA's design is |

| | | |
|---|---|---|
| | | intended to be browser-agnostic with flexible vendor-specified values for vendors with different privacy stances.<br><br>Other browsers are making their own choices on whether to provide viable alternatives to cross-site identifiers that can support the digital ecosystem of content and services. We're encouraged that Microsoft Edge has indicated it will support ARA. |
| API Usage | What is the expected source kind for ARA source registrations for registerAdBeacon/reportEvent (and navigation_start/commit automatic beacons)? | It depends if these beacons are automatic or manual:<br>- reserved.* (i.e. automatic) events to be of navigation-source type.<br>- Manually triggered events to be of event-source type. |
| API Usage | Does the maximum limit of 20 aggregatable reports per source mean for each source event? Is the limit global or daily? Is there a plan to increase the limit? | The 20 aggregatable reports per source limit is a global limit where 20 aggregatable reports can be created for each source. The limit is set by the browser and non-configurable. The purpose of this limit is to avoid abusing the protection of real attribution reports with null reports. We have discussed this further here. |
| API Usage | Support for email marketing using ARA. | Right now there is no direct support for this use case within ARA (if you don't control the email hosting site). We are discussing this here and welcome additional feedback. |
| Epsilon | When will the value of epsilon for the Aggregate API be determined? | The current epsilon value can be configured by ad techs up to a predetermined threshold defined by Privacy Sandbox (which is currently 64). We recommend testing different epsilon values and identifying inflection points for your own use cases and providing feedback. We will make sure to communicate to ad techs in advance prior to any changes to the range of epsilon values. |
| API Improvement | Support a use case where the advertiser can insert an identifier into the trigger_data field for matching with external CRM data to allow advertisers to verify the quality of | We are discussing the request and welcome additional feedback here. |

| | | |
|---|---|---|
| | conversions. | |
| API Usage | How to handle redirect URLs as destination urls. | Ad techs can do either of the following:<br><br>1. Put the final destination URL in the destination field;<br><br>2. Destination field allows up to 3 urls which allows you to put multiple URLs into the field.<br><br>Both options will require knowing the final destination URL. We have discussed this further here. |

## Aggregation Service

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Key Discovery Mechanism | Request for a key discovery mechanism | We have a proposal for key discovery and welcome feedback from the ecosystem on the proposal. |
| API Usage | Roadmap for observability on Aggregation Service | We are reviewing options to support more observability and welcome feedback from the ecosystem here. |
| API Improvement | Requesting to be able to requery reports. | Aggregation Service is working on a requerying proposal where ad techs can split their epsilon for each report. This can introduce more noise per query but will allow ad techs to requery and maintain privacy. |
| API Improvement | Would like to be able to associate multiple origins to the same AWS ID. | Aggregation Service will now allow multiple sites to be onboarded on the same cloud account (GCP or AWS). This will allow ad techs to use the same Aggregation Service enclave for processing reports from multiple sites and multiple origins from the same sites. |
| API Usage | When aggregatable batches fail, not sure if the budget is consumed or not and if they can reprocess their batch. When an aggregation service encounters a budget error for duplicate reports, the rest of the remaining reports are lost. How to | In a typical scenario, if the entire job fails, the budget will not be consumed. In cases of a rare failure where budget is consumed, ad techs can request budget recovery.<br><br>If the ad tech encounters frequent job failures with the budget exhausted error, they should confirm their batching strategy. Instructions on how to batch correctly and avoid duplicate |

| | | |
|---|---|---|
| | minimize this loss? | reports and errors can be found here.<br><br>We welcome feedback on budget recovery here. |
| API Usage | Using Private Aggregation API with the trigger described here would produce an aggregatable report for every auction. What are the scaling capabilities of Aggregation Service? | Aggregation Service itself does not put an upper limit on the number of keys or reports in a batch but a scale of 10^14 reports and 10^12 keys is currently unsupported due to the memory that would be required. Our sizing guidance indicates the ranges we have tested and recommend for optimal performance given expected load and the supported cloud vm instance types. |
| Data Processing | If an encrypted data has personal information, what is the legal arrangement of providing encrypted data to the Aggregation Service?<br><br>Can you advise whether it is guaranteed that the coordinator will not access encrypted data? | The Aggregation service does not share encrypted / user data with the Coordinator. The Aggregation service uses the coordinator for key management and accounting. Some details on the coordinator can be found here.<br><br>For accounting, Aggregation service only shares the shared ID and the reporting origin with the PBS for budget consumption. Once we launch a multi-site we will replace origin with site.<br><br>Note that Aggregation service runs in a TEE which is the only place where reports from clients can be decrypted. The code running in the TEE is open sourced and audited by external parties as outlined here. |

## Private Aggregation API

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| API Usage | Ability of component sellers to send reports to multiple aggregation servers within a TEE. | The current Private Aggregation API status does not support this feature. We have discussed this issue further here. |
| Documentation | What is the epsilon value used in Google's trials? | For the Private Aggregation API, the ε value specified in an aggregation service query corresponds to the L1 contribution budget of 2^16 that is enforced on a rolling 10 minute basis. There's also a 'backstop' L1 contribution budget of 2^20 that is enforced on a rolling 24 hour basis. So essentially, the privacy parameter |

| | | |
|---|---|---|
| | | is ε on a rolling 10 minute basis, and is 16ε on a rolling 24 hour basis (rather than 144ε).<br><br>Aggregation service currently supports a range of ε for testing (up to 64) to allow for experimentation with different aggregation strategies and provide feedback on the utility of the system with different privacy parameters for Private Aggregation and other APIs. We plan to revisit the maximum allowable epsilon value over time as we get feedback from testers and add features that allow for more efficient privacy budget usage. |

# Limit Covert Tracking

## User Agent Reduction/User Agent Client Hints

No feedback received this quarter.

## IP Protection (formerly Gnatcatcher)

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Resolution ID | Privacy Sandbox needs to be more vocal to press that resolution IDs often built on IP are not sustainable for advertisers. | Privacy Sandbox has made it clear that we aim to reduce cross-site tracking. Our public initiatives, which extend beyond cookies, are publicized both on privacysandbox.com and GitHub. We strive to reduce cross-site tracking, including that based on IP addresses. However, it is ultimately up to individual websites to decide whether to proactively enable cross-site tracking. In an era of increased scrutiny on regulatory compliance, it is prudent for individual companies to have an understanding of the practices employed by their service providers. |
| Chromecast | Will IP Protection impact Chromecast or other Chrome devices? | There are currently no plans for IP Protection to be applied to Chromecast devices. |
| IP Protection List | Will the list of third parties identified as potentially using IP addresses for web-wide cross-site tracking be published? | The list will be published once finalized, as discussed here. |

## Bounce Tracking Mitigation

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Single Sign On (SSO) Exemption | How will Bounce Tracking Mitigation (BTM) verify SSO use cases for exemption? | BTM will be disabled by Chrome heuristics. See here for details. |
| Deprecation Trial | Is BTM enabled for sites in the 3PC deprecation trial? | No, BTM honors the cookie exceptions created by the deprecation trial, as discussed here. |

## Privacy Budget

As noted in the GitHub explainer and developer site, Privacy Budget is no longer being actively considered as part of the Privacy Sandbox proposals.

# Strengthen cross-site privacy boundaries

## Related Website Sets (formerly First-Party Sets)

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Feature Request | CHIPs and / or Storage Partitioning are automatically allowed to be accessed across the RWS, without the need for the Storage Access API, nor user interaction. | We are considering the benefits and feasibility of a feature that may perform this function. One consideration is a potential gap in cross-browser interoperability, which RWS addresses by leveraging the Storage Access API. There is no current equivalent to this requested functionality supported on other browsers. We encourage developers to submit their use cases on this issue to facilitate discussion here. |
| Removal of Non-compliant Sets | What is the process to remove sets that become non-compliant from the repository? | We are working on defining a process for this, and we'll share updates as soon as they're available. |
| Enforcement Process | There is a lack of clarity around Google's subjective role in the RWS enforcement process. | As RWS is an ongoing project and we are continuing to receive new submissions, aspects of the process and our criteria are still being solidified. We do agree that it is important for our submission guidelines to fully outline our requirements for submission, and we will add greater detail to our submission guidelines going forward to avoid further ambiguity and |

| | | |
|---|---|---|
| | | confusion.<br><br>Our intent is for the submission process to be as technical as possible so that we can phase out human involvement and entirely rely on automated checks. PRs such as this one necessitate more human interaction because they include behaviors we did not anticipate, but they allow us to identify more areas for automation and ways we can fix our guidelines to avoid these problems going forward. |
| Sharing Data | Request for a feature that allows domain owners to indicate they would like a third party to also share RWS data, with user consent. | The requested functionality is already available through APIs such as FedCM, and Storage Access APIs that enable access to authenticated identity after the user accepts a permission prompt. We welcome feedback from the ecosystem on any specific use cases that they believe are not possible. |
| Other Storage Methods | Will information saved on local storage or session storage will also be interpreted as 3PCs? | Local storage, session storage, and other forms of non-cookie storage when used within third-party contexts have been partitioned in Chrome since version 115. See this blog post for additional details. |
| Associated Sets Limit | What happens to organizations who submit more than 5 domains even though this is “capped at 5 associated sites”? | These sets will be accepted via the GitHub process, but the browser (Chrome) will only apply our Storage Access API auto-granting rules to the first 5 domains; and ignore the remaining domains, as discussed here. |
| find_robots_txt | find_robots_txt check does not work with redirects. | A fix has been submitted to resolve this issue here. |
| User Gesture | Remove user gesture requirement for accessStorage(). | This requirement was made based on a similar design that is in place across all major browsers for the requestStorageAccess API. We invite additional feedback and use cases in this GitHub issue to help us prioritize this request, and enable cross-browser discussions. |
| User Gesture | Is a user-gesture required to grant permission for third-party storage access after a Chrome or OS restart? | Yes, but we welcome additional feedback from the ecosystem on whether to change this behavior here. |

## Fenced Frames API

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| adComponent | Lack of documentation and flexibility using AdComponents with Fenced Frames. | We are looking to share more documentation regarding this use case. Also to add, ad components are supported in Fenced Frames using getNestedConfigs() which is documented in the spec here. |
| (Also reported in previous quarters)<br><br>Render adComponent | Request for sample codes on how to render adComponents in Fenced Frame. | We are working on sharing some sample codes here. |
| Third-party Ad Verification | The role of third-party ad verification in the context of Fenced Frames needs more detail, especially regarding contextual/brand safety. | Today, Fenced Frames Ad Reporting does allow for DSPs to send impression and auction event-level data to 3P ad verifiers for post-render brand safety checks and billing. |
| Expandable Ads | Request to support expandable ads. | If the ad needs to switch between two sizes with the same aspect ratio, and there is no functional difference between the two (just size), the embedder could resize the Fenced Frame with the second ad size and the browser accordingly scales the Fenced Frame element. |
| (Also reported in previous quarters)<br><br>Support for Video & Native Inventory | Does Fenced Frames support video & native inventory? | Our response is similar to previous quarters:<br><br>PA API supports video rendering using a mechanism that relies on iframes. However, we haven't yet designed a solution for video and native ads rendering that is compatible with Fenced Frames, and this is one of the reasons we had decided to push back Fenced Frames enforcement to 2026. That means if a partner does decide to enforce Fenced Frames now, the support for video and native would be lacking for that partner. |
| Advisory Board | Requests the creation of an advisory board of native ad vendors to ensure Fenced Frames implementations follow industry standards. | Fenced Frames are not required for use in PA API any sooner than 2026. The additional time allows us to continue working with the industry to design and implement support for a broader range of critical use cases. We've previously stated we will evolve Fenced Frames ahead of their requirement to maintain support for video |

| | | |
|---|---|---|
| | | and native ads with PA API. Per our commitments, we will engage with and inform the CMA of any such changes, and we will continue engaging with feedback from the ecosystem ahead of requiring Fenced Frames. Our ecosystem engagement model at W3C and ad standards organizations like IAB Tech Lab allows for industry experts of all kinds to guide the designs before they are required. |
| (Also reported in previous quarters)<br><br>Size Difference Across Platforms | Reports that the size of content displayed in the Fenced Frame looks different between desktop and smartphones. | This is a known Chromium issue which we are investigating. We welcome additional feedback here. |
| API Improvement | Did the Fenced Frames requirement get pushed back to 2025 so that native ads are now supported under Privacy Sandbox? | As we noted in our public announcement for Fenced Frames enforcement no sooner than 2026, we had learned of a broad "significant effort to accommodate" Fenced Frames. Certainly, one of which was Native, but it was not the only factor. The intent was to provide more time to ensure ecosystem readiness to support key use cases, including, but not limited to, native. |

## Shared Storage API

| **Feedback Theme** | **Summary** | **Chrome Response** |
|---|---|---|
| Performance | Shared Storage return times outside of the worklet appear to be dependent on activity in the worklet. | We are discussing this test result here. |
| 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, including the WICG, to champion the proposal, seek feedback, and drive adoption. |
| Bidding Worklets | Is it possible to read from Shared Storage within the generateBid (which is already running in a worklet) to apply ad-decision / business logic (such as Frequency Capping) based | No, it is impossible to read from shared storage within bidding worklets. |

| | | |
|---|---|---|
| | on cross-site information and select a subset of ads? | |

## CHIPS

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Partition Capacity | Clarify behavior when over partition capacity. | When capacity is reached, the oldest cookies are ejected from the least recently accessed cookie(s) to free memory until the limit is no longer surpassed. Developers see the updated Cookie header in subsequent requests. |
| Third-party iFrame Access | Embedded third-party iFrame content opening a new tab/window to the same third-party site should have access to the same partitioned cookies as the opener. | We are discussing this use case and welcome additional feedback from the ecosystem here. |
| Duplicate Cookies | If there's a partitioned cookie and an unpartitioned cookie with the same name, which key value does the browser decide to send? | When having two cookies with the same name (one partitioned, and one not), you'll get both cookies – unfortunately, there is no way to differentiate which is which. The RFC spec on this is available here, which explains that the order in which cookies are sent should not be relied upon. |
| Feature Request | Opt into origin-partitioned cookies. | We are considering this request and welcome additional feedback from the ecosystem here. |

## FedCM

No feedback received this quarter.

# Fight spam and fraud

## Private State Token API (and other APIs)

| Feedback Theme | Summary | Chrome Response |
|---|---|---|
| Webview | Are Private State Tokens (PSTs) persisted across multiple Webviews on the same mobile device | Each app that uses webview will have a different local storage, which means PST issuers cannot issue tokens in one app's webview and then later in a separate app, allow token |

| | | |
|---|---|---|
| | (profile)? | redemptions. This is true for other forms of data stored locally on webviews as well, such as cookies.<br><br>PSTs are not yet fully available in webview. We expect to provide an update on this by the end of Q2. |
| New Token Type | Proposal for a new token type. | We are thankful for this proposal and continued exploration into applications and adaptations of PSTs, and look forward to learning more about this proposal in upcoming Anti-Fraud Community Group meetings in Q2 2024. |
| User Identification | How to prevent users being identified based on the particular PSTs a user has? | This is currently mitigated by limiting redemption attempts on a site to two issuers, regardless of whether there are tokens available from that issuer. You need to count an issuer against the limit even if there aren't tokens available as otherwise the site could iterate through all issuers until it hits a positive match. |
| Registration | How long will registration be required for PSTs? | Registration will continue to be required for the foreseeable future, as explained in further detail here. |
| Support for other Chromium Browsers | Will PST issuer registration for other Chromium-based browsers be supported through the Chrome Issuer Registration repository? | Chrome fetches the key commitments and distributes them to Chrome clients through a mechanism called Component Updater. As other browsers add more complete support for the API, they'll need to establish a process for getting the key commitments to the client, either through a component updater-style method or some other method. This is addressed in further detail here. |

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

Google Ads is engaged in integration and 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 updates below:

***Measurement APIs***:

- In Q1 2024, Google Ads conducted 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 Google Owned and Operated properties and also from non-Owned and Operated / Display.

***Chrome-facilitated testing***:

- In Q1 2024, Google Ads conducted 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 and and 3rd party inventory.

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.

# 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, the parties continue to operate a joint process by which the CMA carefully reviews relevant Google announcements before they are published.

## CMA concerns

The CMA has raised a number of concerns during the relevant period about impacts of the Privacy Sandbox changes. Google is working with the CMA to resolve these concerns, following the process set out in paragraph 17(a)(ii) of the Commitments. The concerns are summarized in the CMA's quarterly update report. The CMA has not notified any concerns pursuant to paragraph 17(a)(iii) of the Commitments. 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 to stakeholder concerns as set out below.

## Stakeholder concerns

The CMA has shared with Google certain concerns expressed by stakeholders. The concerns set out below are not exhaustive, and are in addition to those addressed above.

**Fees for Privacy Sandbox APIs** - The CMA has shared stakeholder feedback regarding fees Google may charge in connection with the Privacy Sandbox APIs. Google can confirm that it does not intend to charge developers for the direct use of the Privacy Sandbox APIs, although fees may be charged by the products and services which utilize the Privacy Sandbox APIs. When an entity decides to use Privacy Sandbox APIs that incorporate cloud services such as Aggregation Service or Bidding and Auction Services, the entity may be charged for the services of the cloud provider they use; this includes Google Cloud Platform, one of the supported cloud providers for Privacy Sandbox. Were this to change at any stage, we would provide substantial notice to the ecosystem ahead of any future changes.

**Competition Feedback** – The CMA has shared stakeholder feedback relating to Google's market power, and the fact that the Privacy Sandbox proposals could be anticompetitive or

damaging to the sector. The CMA has also shared a stakeholder concern that the PA API creates an advantage for Google, in particular regarding the use of first-party data, and would not be compatible with potential antitrust remedies. Google has committed 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 the Commitments, and we welcome feedback on how the APIs perform for different types of stakeholders.

**Timeline & 3PC Phaseout** – The CMA has shared stakeholder feedback regarding whether Privacy Sandbox is ready to be implemented in 2024, and that Google's proposed timelines do not detail how 3PCD will be scaled. As announced on 23 April, we have revised our timeline for 3PCD. The Privacy Sandbox APIs reached general availability on Chrome in September 2023. The APIs are now available for 100% of Chrome traffic and ready for scaled use to support key business use cases. Google is still in the process of considering the dynamics of how 3PCD will be facilitated, but can provide reassurance to the ecosystem that this will be a gradual process.

The CMA has also shared feedback from a stakeholder that Google may provide insufficient notice for ad techs to implement alternative solutions with their publishers and test and comment back on proposals, and requests that the minimum notice time be set at 12 months. As we set out in our blog post in January, there is ample opportunity for ad techs to develop privacy-enhancing technology offerings on top of the Privacy Sandbox building blocks we're offering, as well as non-Privacy Sandbox building blocks. Google welcomes efforts to use the Privacy Sandbox alongside other, non-Google privacy-preserving technologies to evolve existing solutions and create new ones. Google will provide the ecosystem with sufficient notice ahead of any future changes which may impact alternatives.

**Digital Markets Act** – The CMA shared feedback from a stakeholder that it is unclear today how the Privacy Sandbox can comply with the EU Digital Markets Act (DMA). Privacy Sandbox does not give rise to DMA compliance concerns. For completeness, Google's compliance with the DMA is monitored by the European Commission, rather than the CMA.

**Privacy Budget** – The CMA has shared a request for confirmation from a stakeholder that the possibility for publishers to access the original IP of users is outside the scope of the browser-assigned information budget referenced in the CMA's Q4 2023 Report (Privacy Budget). As was noted in the GitHub explainer and developer site, Privacy Budget is no longer being actively considered as part of the Privacy Sandbox proposals.

**Privacy Feedback** – The CMA has shared stakeholder feedback that Privacy Enhancing Technologies such as Privacy Sandbox are seeming to go beyond basic legal requirements which set new ways of operating for the industry. While we have sought to ensure that the Privacy Sandbox APIs enable compliance with applicable legislation, and have engaged with

the CMA and ICO in their development, we don't consider the basic legal requirements to be a cap on what we can offer to the industry and to users.

For example, the CMA shared stakeholder feedback that our justification for ARA's 3-bit / 8-conversion-type limit understates the point that de-identified data is not Personal Data unless there is a material evidence-based risk of re-identification. We did not select these limits in reference to a specific legal standard, however. Our aim was instead for the API to provide only as much information as would be reasonably necessary to achieve the intended use case.

In general, we are seeking to improve Chrome users' privacy while providing effective alternatives to 3PCs, which in some circumstances includes improvements to user privacy beyond what may be legally required of Google or those using the technologies.

**Attribution Reporting API -** The CMA has also shared a stakeholder query, asking whether, with the current language surrounding the ARA's Coordinator Service reliability guarantees, there is a point at which the Coordinator Service will have warranty language that protects both advertisers and ad tech partners that are being asked to leverage Privacy Sandbox tools for billing purposes. Processing of ARA aggregatable reports (including for billing purposes) is done by the Aggregation Service. The Aggregation Service is operated by the ad tech partner, and the code for the service is open sourced. The dependency on Coordinator Services is only for the cryptographic keys and managing aggregatable report accounting, and the Coordinator Services are provided for free. Google understands that reliability of the Coordinator Services is important for all stakeholders, as well as for the privacy of the system, and so has placed controls to ensure the services are reliable. However, Google has no plans to establish additional contractual warranties or guarantees for the services beyond what is already included in the standard Warranty and Disclaimer sections of the Google Terms of Service.

**Data-usage commitments** – The CMA has shared a request from a stakeholder for Google to clarify, with respect to paragraphs 25-27 of the Commitments, the scope of data that will not be used, and how and where this data would not be used. We agree that the scope of the data Commitments is important. We have engaged in detail with the Monitoring Trustee and Technical Expert as well as with the CMA over the course of the past two years with respect to the data covered by these commitments, and the technical mechanisms to ensure that, after Chrome ends support for 3PCs, data will only be used in line with the terms of the Commitments.

The CMA has also shared a stakeholder request for Google to clarify what is meant by "browsing history..." in respect of the data which Google is committing to not using for targeted advertising, as well as the paths that data cannot travel with their pipelines, to be clear about both the direct and indirect ways that targeted advertising cannot benefit. Google has set up internal controls to guarantee that browsing history data cannot be used in contravention of the Commitments, directly and indirectly, for ads targeting and measurement purposes. We have engaged in detail with the Monitoring Trustee and Technical Expert as well

as with the CMA over the course of the past two years with respect to the data covered by these commitments and the technical mechanisms to ensure that this data is not used in contravention of the Commitments.

The CMA has shared stakeholder feedback that Google, as an entity, should be prevented from using a broader set of data than just browser history, even if that is broadly defined, for targeting advertising purposes on their open web integrations. According to the stakeholder, if Google is able to use account data, search history, YouTube history, GMail, etc, for targeted advertising across the web, and are only restricted on URL usage from a browser bar, that will not be a meaningful restriction. Under Paragraph 27 of the Commitments, after Chrome ends support for 3PCs, Google will not be allowed to use its first-party personal data to track users to target or measure ads shown on 3P websites across the web.

**Topics Governance** – The CMA has shared with Google stakeholder feedback that the Topics taxonomy function should belong to an external group to ensure equity across the full ecosystem. Google does not exclude the possibility of involving external bodies in the governance of the Topics taxonomy in the long-term. However, Google has not identified any existing or potential forum that could (i) provide balanced stewardship of the taxonomy of the Topics API (in respect of both privacy and utility considerations), and (ii) take timely and actionable decisions necessary to progress the project efficiently. Google therefore does not have near-term plans to transfer governance of the Topics taxonomy to an external body.

The CMA has also shared feedback from a stakeholder that Google clarifying longer term governance models would not address the impact of changes to Topics. Material changes to Topics  are and will continue to be taken in line with Google's governance framework, as designed with input from the CMA and Monitoring Trustee.

The CMA has shared stakeholder feedback that if Topics were to proceed without an alternative third-party solution, then the governance model is critical, and that trusted stakeholders (e.g. a selection of consumer and industry representative bodies) could be used across the ecosystem. Google agrees that the governance model is critical to the success of the Privacy Sandbox project. Under the Commitments, Google is required to take into account various inputs, including feedback from the ecosystem and current ecosystem practice, as part of decision-making processes. Google will continue to consider ways in which stakeholders can contribute to this process under the governance framework going forward.

## 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 31 March 2024, 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