Privacy Sandbox Progress Report

Q4 Reporting Period - October to December 2023

Prepared for the CMA, 29 January 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 Q4 2023 updates, covering the period from October 1 to December 31, 2023.

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

Privacy Sandbox Q3 2023 Timeline Updates	
October Timeline Updates	• Q4 was added in 2024 in both "Third-Party Cookies (3PC) and Testing" and in "Privacy Sandbox APIs" timeline • For "Third-Party Cookies (3PC) and Testing" timeline the "Third-Party Cookie Phase Out" phase was updated to start mid Q3 and end in mid Q4 2024 • For "Privacy Sandbox APIs" timeline the "General Availability" phase was expanded to end at the end of Q4 2024
November Timeline Updates	• None
December Timeline Updates	• None

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. Grantees will undertake 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. 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 are expected to perform tests for at least 8 consecutive weeks between January 1, 2024 and May 31, 2024. Google 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.

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
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
3PCD Timeline	Share more information on the 3PCD timeline.	To facilitate testing, Chrome restricted 3PCs by default for 1% of users, from January 4, 2024. Subject to addressing any remaining concerns of the CMA, Chrome plans to gradually phase out support for 3PCs as of Q3 2024 and continue throughout the rest of 2024.
3PCD Timeline	Impact of the timing of 3PCD in Q4 2024, as it coincides with the holiday season and could have a negative impact on publishers.	There is no perfect time to deprecate 3PCs. We've been clear for well over a year that our intention was to deprecate 3PCs in the second half of 2024. Our Commitments to the CMA which include the potential timing for a Standstill period have not changed. While we understand the Q4 timing concern, making timeline changes has resulted in less industry preparation, not more.
Chrome testing (mode a/b)	Is the testing setup for Mode A and Mode B per instance or per chrome profile?	We have published clarification in documentation here that Chrome browser in this context refers to a Chrome client: a Chrome installation on a device. Each individual user data directory constitutes a distinct client.
Deprecation Trial	Share more information about the 3PCD Trial.	We have shared more information about the 3PCD trial here.
Deprecation Trial	Not enough time to provide Deprecation Trial tokens across all sites before January 2024.	We acknowledge that there is a short period of time between when deprecation trial registrations open and when the Chrome-facilitated testing period begins blocking 1% of cookies. To address these time constraints, Chrome is providing a grace period for participating origins while they work to deploy deprecation trial tokens. During the grace period, which will run through April 1, 2024, origins registered for the deprecation trial will have access to 3PCs in Chrome even if they have not yet deployed their tokens. The purpose of this grace period is to prevent web compatibility problems during the transition phase. Participating origins must deploy deprecation trial tokens before the end of the grace period in order to continue to have access to 3PCs after the grace period ends.

Chrome testing (mode a/b)	Mode B is too small of a sample to properly measure performance drops precisely.	There is a careful balance to be struck between the percentage of traffic and risk of impact on users and functionality across the web.
Testing Controls	Only the very largest publishers with significant development resources will be able to understand the performance during testing and pass this on to the CMA.	We're already seeing publisher service providers sharing insights publicly with the broader ecosystem and expect this to continue as Privacy Sandbox testing increases. We also expect ad tech companies building on top of the Privacy Sandbox APIs will continue to develop features their customers demand, like reporting based on labels.
Third-party data	Concern for third-party data companies.	There are different flavors of third-party data companies. Some may double down, turning to ever more opaque methods of cross-site tracking. Others may lean into privacy-enhancing technologies and develop new value propositions with their customers. We hope more choose to do the latter and travel in the direction both users and regulators are increasingly demanding. Change will breed opportunities for evolution and innovation.
Google Ad Manager	Need for more Google Ad Manager guidance on how publishers can test the Privacy Sandbox. Reporting insufficient for publishers to understand the impact.	**Response provided by Google Ad Manager:** Google Ad Manager has explained how it will be conducting testing using Chrome-facilitated testing labels in its help center. Ad Manager currently provides publishers with reporting on both Topics and Protected Audience. As of the time of this Feedback Report, Ad Manager can report on impressions served via the Protected Audience API and can indicate whether data from the Topics API was present on a given impression. Publishers interested in more sophisticated reporting such as segmenting reporting based on Chrome's facilitated labels can do so by reading the labels directly from Chrome (using Chrome documentation), and pass them as key-values in ad requests to Ad Manager, and key-value reporting to report on the labels.

Testing incentive	Advertiser concern about sufficient time to test Privacy Sandbox, and potential for material API changes that may come.	We understand some people want more time, but we have heard repeatedly from the industry that moving the timeline is likely to result in less ecosystem preparedness, not more. While the timeline to deprecate 3PCs is subject to addressing any remaining competition concerns from the CMA, we are encouraging everyone to prepare for 3PCD in 2024. Like any technology, Privacy Sandbox APIs will continue to evolve. That evolution stems from advancements in technologies and ecosystem input. We will continue to be responsible as we make changes and do not think that changes in technology should indefinitely inhibit usage.
CTV	No path to support linear or CTV video.	We look forward to exploring CTV use cases more, but do not think APIs for CTV devices stand in the way of 3PCD in Chrome.
Advertiser Ad Servers	Google seems to be shifting ad targeting to DV360. What support will be provided for advertiser ad servers?	**Response provided by Chrome:** PA API is designed for advertiser ad servers to serve and measure ads shown to a user through the use of iFrames / Fenced Frames and Beacon reporting. Additionally, they will work with upstream and downstream parties to integrate into the serving flow, as they do today.
Google Ads Data Manager	Recently announced “Google Ads Data Manager” builds upon Customer Match and Enhanced Conversions, which enable advertisers to share their first-party customer data with Google to maintain all the marketing functions performed by 3PCs. How does this new feature align with Google’s commitments to the CMA?	**Response provided by Google Ads:** Google Ads Data Manager simply facilitates uploading of first-party data from advertiser data storage systems (cloud systems) for use by advertisers for Customer Match (CM) and Enhanced Conversions (EC), making it easier for small-to medium sized businesses with fewer technical resources. Google Ads Data Manager does not enable any net-new capabilities for CM or EC in terms of addressability or measurability of ads on Google O&O OR third-party publishers. Google’s ads platforms have the same access to the capabilities available in the Privacy Sandbox technologies as other Ad Tech companies.
Chrome settings	Chrome's internal setting	The requested functionality is already available

	page should provide more information about size of cookies.	in Chrome Developer Tools. We welcome additional feedback on why this feature should be prioritized in the settings page as well.
Heuristics	What heuristics are Chrome deploying to preserve critical user experiences during 3PCD?	See our response to this question on GitHub here.
Browser versions	Differentiate stable from non-stable Chrome browsers?	A rough matching of Chrome major version to the Stable release cycle will work.
Compliance	Can Chrome provide SOX-related reports?	Chrome will not provide SOX-related reports. Privacy Sandbox APIs are one of many web APIs that Chrome makes available to the websites a user visits. As with all web APIs, the API caller doesn't enter into an agreement with Chrome to use Privacy Sandbox API; access just depends on whether the API caller meets any technical requirements and the user has the appropriate settings enabled. If so, the API caller alone determines how to use the API, including what data to store, what bids to place, what reporting to request, etc.
Compliance	Expanding the Privacy Sandbox Compliance FAQs to address more questions.	We appreciate the feedback and plan to further build out the FAQs.
Chrome question	Is the deprecation of 3PCs on Chrome impacting the availability of 3PCs on Android WebView (embedded browser)?	We don't currently include WebView at this stage of 3PCD or Privacy Sandbox API rollout and testing, beyond enabling Cross App and Web Attribution Measurement.
API question	How can clicks and impressions of sponsored products be tracked?	This use case is covered by the Attribution Reporting API.
Timeline	Why has the timeline changed for 3PCD?	We have discussed the reasons here.
Chrome extension SSO	Allow the use case of single sign-on between a website and a Chrome extension after 3PCD.	We are discussing this issue and welcome feedback on additional use cases here.
API usage	Can Google confirm a list of	Details of testers who have publicly identified

	partners to test APIs with?	themselves are available on GitHub for the following APIs: - Topics API - Protected Audience API - Attribution Reporting API - Shared Storage - CHIPs
Utiq initiative	What is Chrome's view towards the Utiq initiative?	We are discussing this here.
Chrome question	How to detect users browsing without 3PCs?	There's no explicit setting to detect 3PC blocking. For a general "feature detection" approach, we would recommend creating the iframe / cross-site request and trying to set a similar cookie to the required use case is going to be the closest solution.
Chrome question	Is browsing in incognito mode the same as running the flag test (launch Chrome using the --test-third-party-cookie-phaseout command-line flag)?	The incognito mode is different from the flag. The flag not only blocks 3PCs but also enables FedCM and third-party storage partitioning.
Chrome question	More details on what is the expected impact of 3PCD for each region/country when 1% happens.	Clients are included in the 1% at random, globally, though there may be regional variations. For example, there may be differences in the distribution of devices and Chrome versions.
Alternative Privacy Enhancing Technologies	Alternative Privacy Enhancing Technologies should be allowed to perform privacy-preserving cross-domain tracking to prevent a data monopoly on Chrome & Android.	There is ample opportunity for developers to build privacy-enhancing technology offerings on top of the building blocks we're offering as well as non-Privacy Sandbox building blocks.
CookieGraph Study	What is Chrome's perspective on the CookieGraph method as described in this paper within the Privacy Sandbox framework?	We are reviewing this paper and welcome additional feedback here.

Enrollment & Attestation

Feedback Theme	Summary	Chrome Response
Enrollment is restrictive	Google has introduced specific terms of use for Privacy Sandbox APIs. Terms effectively prevent companies who specialize in helping publishers recognise consenting visitors to test and/or integrate Privacy Sandbox features within their identity solution. Terms and conditions unfairly limit their ability to operate within the Privacy Sandbox.	The enrollment and attestation process does not involve agreeing to API terms of use. Enrollment and attestation are instead mechanisms intended to improve transparency regarding which developers call the Privacy Sandbox APIs and how they use the data they access. Specifically, the attestation is a public statement that the attesting developer does not use the APIs to identify users across sites or apps and does not otherwise circumvent the APIs' privacy protections. The attestation does not require making representations about developers' use of other data or technologies.
Privacy Sandbox Enrollment	How to update the point of contact / email address for attestation?	Enrollment information can be updated using the enrollment form. Further detail is available here.
Privacy Sandbox Enrollment	Can you please clarify access cut-off scenarios in case the attestation is not available?	Privacy Sandbox will allow 3 weeks for a technical contact to re-establish the attestation file for the enrolled site before denying an enrolled company access to the (measurement and relevance APIs).
Privacy Sandbox Enrollment	How can we test the APIs in a local environment using non-production endpoints?	We have responded to this question here.

Show Relevant Content & Ads

Topics

Feedback Theme	Summary	Chrome Response
Usefulness for different types of stakeholders	Publishers are concerned about the impact of topics on data-driven sales. Larger sites are assigned a general 'news' Topic, no data links it to the specific publisher. Specialist publishers give	We acknowledge that sites with more general interest domains are likely to contribute less granular topics than sites with more niche interest domains. However, not all niche sites contribute commercially valuable topics. Also, this dynamic reflects the status quo - that some sites provide more value than others in

	away their data for limited information in return.	3PC-based ad relevance systems. Topics (and the Privacy Sandbox overall) provides publishers with more control over how their information is used by the adtech companies they partner with. Further, the information available via Topics is much coarser than existing signals.
Publisher Ad servers	Publisher ad servers who use dedicated ad servers may not be able to directly observe Topics API.	We are discussing this issue here and welcome additional feedback.
Attestation	Expand attestation requirement to address known undesirable consequences of cross-context transfer of information.	At this time, attestation is not intended to cover this broad category of risk, but rather to address the abuse of the API.
Volume of Topics traffic	The current volume of impressions received is not sufficient for testing.	Chrome is aware of feedback regarding the volume of Topics available in the programmatic ecosystem. We are investigating the potential reasons - both within the browser and among relevant testers. If deemed necessary, Chrome will assess what potential API design changes are available in order to increase the coverage rate and to enable testing at sufficient scale, while preserving user privacy.
API usage	Is there a Topics API rate limitation?	There are some Topics rate limits in place to prevent abuse and protect users' experience on the web. You can see some more details here.
V2 taxonomy	Guidelines from the IAB for the topic details to be included in open RTB protocol?	Yes, guidelines from the IAB on including Topics within the Open RTB protocol can be found here.
Impact on first-party signals	Granular Topics taxonomy v2 coupled with a process for returning the highest value of this granular segmentation (top topics) will distort the market for data in advertising.	Our response remains unchanged from Q3: "While a more granular Topics taxonomy may indirectly decrease the appeal of other solutions, such as those based on publisher first-party data or those relying on direct deals, as we develop the Topics API our main goal is ensuring that it supports interest-based advertising use cases after 3PCD as effectively as possible, for all stakeholders alike. Our belief

		is that greater utility for Topics will improve competition overall and benefit the ecosystem as a whole.”
Testers list	What is the adoption of Topics and PA API amongst your publishers?	We are unable to share such information. You can reference the tester list, where publishers may opt-in to sharing their testing status.
Topics selection	Allow users to proactively select topics of interest?	We have certainly considered enabling users to proactively add topics. We aren't planning to address it in the short term, but are open to exploring it further longer term.
Topics selection	If an ad-tech has code on a site to observe topics, are they able to know what the topics are that might be observed?	An ad tech company can determine the topics associated with a site. The API does not share this information in real time because it may introduce latency costs.
V2 taxonomy	Since Topics can return up to 3 Topics, what is the expected behavior as Taxonomy v2 rolls out?	The API will still return up to 3 Topics and will include the relevant taxonomy version for each Topic in the response.
(Also reported in previous quarters) Topics observation	Allow publishers to give Chrome permissions to categorize topics based on page content (for example, head or body).	Our response remains unchanged from Q3: "We previously considered offering functionality to classify sites into topics based on page content, and made the decision not to move forward based on privacy and security concerns. This proposal may mitigate some of those concerns, but it's unclear as to what extent. Due to the upcoming CMA experiment period, we don't expect this change to occur before 3PCD. We welcome additional feedback here."
Topics selection	How are domains being classified with Topics given the fact that they are general?	We only use hostname to classify sites into Topics. A site being classified broadly is not harmed by this. This is because a site’s contextual information will always be available for auctions on their site, which would provide more specific information to the broad Topic.
V2 taxonomy	Wish for better alignment of topics with other standards (e.g. IAB).	We would like to learn more about why they hoped for closer alignment between the IAB and Topics taxonomies. What steps do they need to take to adopt the Topics API, and how does a more distinct taxonomy impact those

		steps? We are considering releasing a mapping between the Topics taxonomy and IAB content taxonomy. It'd be helpful to understand if doing so would address the challenges publishers face.
Data storage and usage	Do you have more information on how the data is stored and where data is transferred?	Topics information is generated and stored locally, on a user's device. Upon request, the API returns up to 3 Topics to callers. In Google's view, callers are responsible for complying with local regulations when handling and storing Topics information. Further, all callers must attest that they are not using Topics to re-identify users across sites. Please refer to the Privacy-related compliance FAQs for further details.
V2 taxonomy	Effect of Topics Taxonomy Upgrade and the state of the browser while transitioning from v1 to v2.	The Topics inferred with previous Taxonomy are still available and can be eventually fetched by the adtech until they expire (4 weeks old).
API Description	The user experience of the Topics API is misleading.	We have shared this feedback with the UX team.
API question	How are Yahoo domains being classified with Topics considering they are general?	We only use hostname to classify sites into Topics. It is important to understand that a site being classified broadly is not harmed by this.
Topics availability rate is low	Testers are receiving low volume of Topics from Google Ad Manager.	Google Ad Manager rolled out several optimizations to improve coverage - buyers should have seen an increase in coverage. There are some expected factors that may limit the coverage (e.g. user preferences, observation requirements by the caller, potentially some latency/timeouts).

Protected Audience API (formerly FLEDGE)

Feedback Theme	**Summary**	**Chrome Response**
Differentiation	Lack of clarity on how SSPs bring differentiation to the new auction.	We have heard of multiple strategic plans that have Protected Audience and/or other Privacy Sandbox APIs front and center.

		Bigger picture, the reduction of ubiquitous cross-site identifiers is often viewed by the sell-side of the ecosystem as a positive step not only privacy-wise, but commercially. Businesses, small and large, who embrace this change are likely to find opportunity.
Ad rendering	Chrome as the only path to render ads stifles innovation. Protected Audience rendering reduces the viability of today's standards around native advertising.	Ads rendering in browsers have always used browser technologies to render. That doesn't change. Perhaps this concern is specific to plans to require the use of Fenced Frames in conjunction with Protected Audience in the future. Part of the reason those plans are "in the future" is exactly because we want Fenced Frames technology to support ecosystem innovation and differentiation when it comes to ad rendering. There is time for interested developers and companies to weigh in on the direction of Fenced Frames which includes how native ads approaches can be supported.
Input	Concern Protected Audience API (PA API) was delivered as more or less complete by the time many ad tech began exploring Privacy Sandbox APIs.	The APIs will continue to evolve based on what we learn from usage as well as new ideas that come from both inside and outside of Chrome. Today's generally available relevance and measurement APIs are stable, but that doesn't mean development has stopped and we welcome additional feedback.
Auction design	Protected Audience design places all audience building and ad selection logic in the hands of the buy side platform, removing the ability for a SSP to offer audience building and ad selection logic for campaigns executed on its platform.	Protected Audience is agnostic to who creates audiences and who bids on audiences. It is possible for an SSP to create an Interest Group (IG) it makes available for bidding. It's also possible for an SSP to provide bidding logic, which seems to align with the direction many SSPs are taking going direct to agencies. While there's always room for additional use cases, the foundations of Protected Audience are flexible enough to support many different approaches to audience creation and activation. The privacy characteristics of those foundations also mean that raw user-level data is not shared between sites.
Auction design	Does the Protected Audience auction run counter to ecosystem Supply Path Optimization (SPO)	No. A winning ad in Protected Audience will pass through at most two seller entities (e.g. a SSP and a publisher ad server) and as few as

	efforts to reduce the total amount of intermediaries between an advertiser and a publisher and/or duplication of a given ad opportunity?	none—if the buyer builds a direct integration with the publisher. Duplication of the same request via multiple intermediaries remains a publisher's choice. Protected Audience should not impact this one way or the other. Protected Audience auctions do occur outside of today's server-to-server real-time system in order to not leak cross-site user data. Some may say this duplicates an ad request. Getting to technically demonstrable privacy does require some tradeoffs. However, it is possible in the long run that the ecosystem decides to use Protected Audience without traditional server-side auctions. This choice could lead to even more optimized supply paths.
Auction design	Protected Audience shifts to a model where SSPs are rarely the 'last' auction run on the page but are forced into this model by the API design.	We disagree. The early adopter implementations we've seen actually make it so SSPs participating in component auctions can beat the output of the contextual auction, which occurs before the Protected Audience auction runs. SSP component auction outputs in Protected Audience are considered last, after a full contextual auction is run.
Auction design	Contextual auction may only be relevant to provide data signals about the auction opportunity to inform Protected Audience auction.	We expect contextual auctions will remain relevant for myriad reasons like deals, non-first-party audience targeted campaigns and loads of contextual scenarios. It's also valuable when there are no IGs present or the bids in Protected Audience fail to reach floors or abide by ad quality rules.
Traffic shaping	DSPs are operating at fixed QPS. Fitting Protected Audience auctions will decrease the utility of legacy infrastructure.	As we understand it, the thing that is changing with regard to queries per second is that many SSPs use cross-site IDs as a feature for determining whether or not to send a DSP a request. This would be true whether the publisher wants to run a Protected Audience auction or not. We explored traffic shaping with many SSPs and found solutions including caching and contextual-based filtering. Over time we expect developers to take advantage of Private

		Aggregation to further aid understanding of DSP bidding preferences and to filter accordingly. Ultimately, some legacy infrastructure built around cross-site identifiers will no longer be useful.
Available signals	Lack of clarity on the full range of signals available when auctions occur and how sequencing with the contextual auction disadvantages that.	Generally speaking, for bidders, information can be supplied when an IG is created, from the contextual auction and from a real-time key-value lookup. For scorers, information can be supplied when the auction is configured, including contextual information about the page and the contextual auction, as well as from a real-time key-value lookup on ad renderUrls.
(Reported in previous quarters) Video Rendering	Support for video rendering using Protected Audience and Fenced Frames.	Our response is unchanged from previous quarters: “Protected Audience API supports video rendering using a mechanism that relies on iframes. However, we haven't yet designed a solution 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 would be lacking for that partner.”
Video Rendering	PA API support for video in iframes is limited to HTML5 video, and does not support the widely used VAST standard.	It is possible to implement VAST-based ads using the iframe rendering mechanism available in Protected Audience today. Google acknowledges that doing so requires new engineering on the part of buyers, sellers, and publisher ad platforms, and we will continue to work to ease the transition from the way VAST has worked in the past.
(Reported in previous quarters) Top-Level Auctions	Ability to use Google's publisher ad server without also giving Google Ad Manager control of the top-level PA API auction.	Our response is unchanged from previous quarters: “**Response provided by Google Ad Manager:** Google Ad Manager's plans for the Protected Audience API do not include supporting Google's publisher ad server without the control of the top-level Protected Audience auction, for the following reasons.

		In order to properly serve our customers in the publisher ad serving market, Google's publisher ad server needs to retain control of the top-level Protected Audience auction. As a publisher ad server, our role is to provide publishers forecasting so they can negotiate direct sold campaigns without overbooking, and to pace and deliver their direct reservations optimally. Doing this requires running the final auction to compare all eligible direct and indirect demand. Forecasting and pacing are core functionalities that publishers expect from an ad server. Without accurate forecasting, publishers may end up overselling their inventory, which puts their business reputation at risk. Pacing is also critical, as being unable to fulfill reservation contracts with advertisers also risks damage to the publisher-advertiser direct relationship, which could result in significant impact to a publishers business. In short, therefore, we do not view a publisher ad server's activity of running the top-level Protected Audience auction as distinct from the other activities of the publisher ad server."
(Reported in previous quarters) directFrom SellerSignals	directFromSellerSignals allows Google Ad Manager to prevent the publisher from seeing the price of its contextual auction.	Our response is unchanged from previous quarters: "**Chrome response:** Information passed into runAdAuction() is not known to come from the seller unless the seller calls runAdAuction() from its own iframe. In a multi-seller auction it becomes impossible to have all sellers create the frame calling runAdAuction(). directFromSellerSignals addressed this issue by loading content from a subresource bundle loaded from a seller's origin. This ensures that the authenticity and integrity of information passed into an auction from the seller-auctions configurations cannot be manipulated. If publishers want to use Protected Audience API to understand any of the information their technology providers are

		passing into Protected Audience auctions, they can ask those technology providers for this functionality. **Response provided by Google Ad Manager:** 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. For Protected Audience auctions, we intend to keep our promise by leveraging directFromSellerSignals, 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 our own component auction either, as explained in this update.""
(Reported in previous quarters) K-anonymity value	How will the value "K" to "k-anon" be decided and when will it be published?	We published the K-anonymity value in December 2023. After the 3PCD process begins, we will raise the k-anonymity threshold to the final value of 50 (k=50) and set the update period to 1 hour (p=1). The K-anonymity value of 50 was assessed as providing the optimal balance between utility and privacy. This value is sufficient to thwart basic bot attacks and maintain differential privacy, while also being low enough that the API continues to be useful for its intended use cases.
(Reported in previous quarters) forDebuggingOnly	Potential for forDebuggingOnly.reportAdAuctionWin to be misused if it remains post-3PCD.	We have shared our proposal on how to continue supporting the debugging use cases long term here. We welcome additional feedback on the proposal.
(Reported in previous quarters) Same-origin policy	Request for relaxing the same-origin policy to allow for subdomains.	This request is under consideration and we have discussed this here.
(Reported in previous quarters)	Increase the number of ad components from 20 to 40.	We have been discussing this request during the Oct 4 WICG call and in this GitHub issue and

Ad Component size		plan to address it by the end of Q1 2024.
(Reported in previous quarters) Key Value Server Key Expiration	Discussion on removing server keys once the corresponding IGs have expired.	Managing TTL is better done outside TEE to reduce the complexity, although we welcome additional feedback here.
InterestGroup Triggers	Can a single IG trigger multiple generateBids within a single (component) auction?	Every time the browser is calling the generateBid() function of an IG, that IG is allowed to return a bid value. It is possible that e.g. in a multi-seller auction an IG is called multiple times, each time in one of the component auctions. Nothing needs to be done explicitly by the owner of the IG to activate/support this behavior.
Compliance questions	What is the scope of consent being collected via a user's Chrome browser?	Please refer to "How is Privacy Sandbox approaching privacy-related compliance in Chrome?" in the Privacy-related compliance FAQs for details.
Multi-tag auctions	How to accommodate multi-tag auctions?	We are evaluating this request and welcome additional feedback here.
IP Protection Availability	What is the impact on Protected Audience feature timelines such as Fence Frame enforcement and removal or removal of Event Level Reporting if IP Protection isn't ready by the announced dates?	As mentioned here, we believe Protected Audience timelines should be linked with the release timelines of other privacy protection features.
modelingSignals	Request for a new field in addition to modelingSignals that can only encode display and click information.	We understand the utility gains provided by this and we are evaluating the request and welcome additional feedback here.
Negative IGs	Would it be possible to allow normal IGs to specify a negative IG name?	Currently this is not possible per the explainer but we welcome additional ecosystem feedback on why this is a requirement.
API usage	Generate an aggregated report at generateBid() level	Private Aggregation can be invoked inside of generateBid.

	passing.	
Macros	Route signals from perBuyerSignals via macros in IFrames to 3Ps.	We are discussing this use case here and welcome additional feedback.
API usage	If Trusted Scoring Signals fetch returns error will scoreAd() still be called?	ScoreAd() should still run if the fetch call did not succeed.
API usage	Writing metadata.shard_num in riegeli files for delta/snapshot files.	We're adding support for shard_num right now to unblock. Riegeli is not as well adopted as for example Avro but it is not abandoned. Since TEE has much more constraints and overhead we made the tradeoff to prioritize performance over user experience. We are considering providing a gRPC service to create files from requests. We may also evaluate other formats like Avro on their performance impact.
API testing	How will PA API and Measurement APIs support incrementality testing?	Privacy Sandbox does not have a way to measure incrementality with a counterfactual pre-auction. You can use Shared Storage and Private Aggregation, but the counterfactual would only be after the auction.
API usage	Is using biddingWasmHelperURL for daily updates impacting the k-anonymity threshold?	As k-anonymity is no longer considered for IG updates, biddingWasmHelperURL can be updated without impacting the threshold.
API usage	Are we able to receive error notifications for PA API?	We welcome ecosystem feedback on what sort of error notification they would need to troubleshoot PA API issues.
Ad sizes	Ad sizes are not visible in the auction nor reporting possible.	We are addressing the issue with this pull request.
API usage	Is the update IG endpoint called for the IG if it is not participating in this auction?	Yes. The updateURL is called for all IGs of a given owner, even if they didn't bid in that particular auction. The only requirements are: - the owner must be included in a given auction (i.e., included as a buyer within the auctionConfig) - the given owner's interestGroup must not have been updated within the last 24 hours.
Prebid in PA API	What version of Prebid.js will	According to our technical documentation, the

	be required for the testing phase?	version should be >= 8.9.0.
First-party data activation in PA API	How can they activate their own first-party data for the definition and usage of IGs?	It is possible to use "Permission Delegation" and "negative interest groups" for this task.
PA API and server-side tagging	How does PA API work with server-side tagging?	The base tag on the user's browser will need to redirect the API call to the rest of the tags on the server side, which would allow them to also register the call.
Chrome testing (mode a/b)	Is the expectation that SSPs will also pass these labels in RTB bid requests and if so how?	Yes, the expectation is that the labels will be passed from the SSP to DSP. Entities are encouraged to access the label and to share the value unmodified with partners via this Device extension.
Data storage and usage	Do you have more information on how the data is stored and where data is transferred?	We will not be providing legal guidance, but more so our approach/general thinking around data storage, retention, and other privacy issues. See here privacy-related compliance FAQs that you may find helpful.
API safety	Concerns about malicious client-side code manipulating the return value of generateBid() function.	We have discussed the issue here and some of the feedback has been incorporated into the Private Aggregation proposal.
Custom destination	When using custom destination reportEvent calls do you happen to know if a custom reporting origin (not to buyer nor to seller) pre-registered as part of an IG in allowedReportingOrigins requires to be declared by the DSP in reportWin using registerAdBeacon?	No, it doesn't need to be registered again in reportWin and can directly be used in reportEvent as documented here.
API restrictions	IG Size during creation and update.	The update size has been updated to 1 MB, matching the new 1 MB cap (from 50 KB) for IG creation.
K-anon restrictions	K-anon for ads containing different sizes.	We published the K-anonymity value in December 2023 which states K-anonymity will start checking ad size "sometime after 2025".

		There isn't a way around excluding size because it can be a cross-site tracking vector, as described in the Oct 11 WICG call.
API safety	Can a malicious player falsify the "hostname" of a page?	The API supports a subkey set to publisher hostname. Since the browser is setting the key it seems difficult to circumvent this mechanism.
API usage	ForDebuggingOnly functions shouldn't be recommended for production use.	We are about to reassert to the ecosystem that the forDebuggingOnly functions are not suitable at all for other than troubleshooting post-3PCD.
More debugging tools needed	ForDebuggingOnly is insufficient to understand issues that may happen before scoreAd().	We are collecting more feedback on this gap and welcome additional input here.
Permanent Opt-Out of Interest Groups	Request for allowing users to permanently opt-out of creation of special IGs.	Our strategy has been to not let users opt out at an IG level as the semantics are not understandable to users as things stand.
Improve documentation	Use same capitalization for renderUrls parameter in spec and explainer.	We appreciate the feedback and will follow up on updating the documentation.
Protected Audience deal support	Request for additional options for Protected Audience Deal Support.	The Chrome team is currently assessing what we can do to support this by 3PCD.
Macros	Macro support needed to keep the size of IGs under max IG size.	A recent update to the explainer partially addressed this request.
event-level ReportLoss API	Request for event-level ReportLoss API.	While event-level loss reports pose a severe privacy risk, we believe the underlying goals of this request can instead be met with suitable modifications to the Private Aggregation API. We welcome additional feedback here.
API usage	How does forDebuggingOnly methods behave if no bids score > 0?	If score <= 0, then that's an automatic loss. So, reportAdAuctionloss will be invoked.
Standardization	No alignment between users of PA API generateBid() function input/output value.	We would recommend all partners raising this (or similar) issues to IAB Tech Lab. This group is specifically working on industry standards for APIs like Protected Audience.
API safety	What data from our IGs can	K-anonymity relies on strong privacy

	Google see?	protections to avoid leaking user sensitive data to any party, including Google. Google also is developing a third-party implementation (Fastly) of this layer to minimize this risk.
Chrome testing (mode a/b)	Can "k-anon" restricted users be excluded from testing?	We expose the k-anonymity status in reporting, as explained here.
Brand Safety	Support Brand Safety use cases where ads are not served depending on the list of blocked sites or keywords.	Such brand safety use cases should be already possible with the PA API. For an ad campaign to negatively target some set of domains, they can either store the domain blocklist in the IG itself, perhaps using a Bloom filter if listing each one would take up too much space. Or they can return the allow/deny decision from their Key Value server, using a UDF that looks up the answer based on the combination of the key that identifies the ad campaign and the domain name that is included in the Key Value request. The Protected Audience API also allows both the SSP and DSP to pass into the auction any information about the page context. This could include, for example, a list of sensitive topics or keywords on the page. The DSP's bidding logic can compare this information with any stored information about where the ad should not appear, and choose not to bid when appropriate. We welcome feedback from the ecosystem on any specific use cases that they believe are not possible.
Permission delegation	How does permission delegation work?	We have shared documentation on permission delegation here.
Batch Requests	Use POST request for some PA API URLs in order to support Batch Request.	We welcome the proposal and welcome additional feedback here.
Improve API	Fields that probably should not be used (such as X-fledge-bidding-signals-format-version).	We are discussing the issue and welcome additional feedback here.

Improve API	Request for passing GDPR consent to third-party ad serving & measurement Vendor.	This functionality is supported using the deprecatedReplaceInURN macro replacement API, as explained here.
Dynamic Creative optimization	How does Protected Audience support dynamic creative optimization?	We are discussing this use case and shared potential solutions here.
Improve API	Request for third party ad serving URL being able to get IG context primarily IG name corresponding to the IG that won the auction.	Such requests may increase tracking risk for users. We are discussing this issue and welcome additional feedback here.
API safety	Concern that the size of "IG blob" will leak information about the IGs that were selected.	As mentioned in the privacy considerations section of the Chrome B&A API explainer, the blob size does not depend on any of the inputs to navigator.getInterestGroupAdAuctionData(). It just packages all IGs on the device. This ensures that the blob size is relatively consistent on a page and limits the ability to leak cross-site information. We designed it this way for exactly this reason.
Chrome testing (mode a/b)	What are the other SSPs' stance on missing the first load with regards to setting cookies and Chrome-facilitated Testing?	We haven't heard any significant concerns (though others have acknowledged this situation), but we welcome ecosystem feedback if this is a significant issue.
A/B Testing support	Request support for PA API A/B testing.	We discussed this request in the November WICG meeting and welcome additional feedback here.
Ad sizes	Who chooses the size for a Protected Audience auction?	This question is answered in this FAQ.
Improve API	Request to configure the key-value service to accept /bidding-signals/v1/getvalues path.	We have added support path prefixes in this pull request.
API usage	How can a publisher create the IG with their code if they are supposed to be in the advertiser's base, so that the advertiser can bid on them?	The answers must come from some ad tech partner — a DSP or SSP that wants to participate in Protected Audience auctions and builds a way for those audiences to come from an outside source. We have discussed this further in this GitHub issue.

Improve API	Request for possibility to link Negative IGs to ads in "Positive Interest Groups".	We are considering this request and shared a potential proposal on how to support it here.
Number of Shards	Request for support on passing "shard_num support" in metadata.	Following this feedback, we have added support for shard_num.
API usage	Request for estimation of overhead of keys in K/V server.	We have shared our thoughts and welcome additional feedback here.
K-anonymity	Request for clarification and enhancement of K-Anonymity counter granularity.	We have provided clarification on K-Anonymity counter granularity here.
Debugging	Request to improve PA API debugging capabilities following the recent proposed changes to forDebuggingOnly.	We are discussing the request here and welcome additional feedback here.
Ad size	Request for Ad Slot size as an additional BTS signal.	We have shared a proposal for supporting this request and welcome additional feedback here.
API safety	Is it possible to restrict "runAdAuction()" usage based on an origin?	We have shared a detailed response here.
IG lifetime	Request for extending the lifetime of IGs from 30 to 90 days.	We are considering the request and welcome additional feedback here.
API usage	Is it possible to run a Protected Audience auction in parallel to Header Bidding and publisher's ad server call?	We are discussing this request and welcome additional feedback here.
Debugging	Request for better support of Chrome PA API debugging extensions talking to DevTools.	We are supportive of providing more debugging tools and welcome additional suggestions here.
API usage	Loss notifications not getting triggered if no bids from component sellers make it to the top seller.	We have explained the rationale behind this here.

Improve API	Request for support of TextEncoder in Protected Audience bidding worklet.	We are considering this request and welcome additional feedback here.
API usage	Network calls and running logic in the client can block the main thread and cause JS execution challenges that can impact SEO.	We are discussing this issue and welcome additional feedback here.
API usage	Is it possible for DSPs to use their current server side bidding funnel to evaluate and send the ad-candidates as part of perBuyerSignal to be used for on-device auctions?	We are discussing this question and welcome additional feedback here.
Extend bid opportunity data	Request for extending the bid opportunity data passed by the browser to the SSP with a list of unique origin domains of the active IGs in the browser.	We are discussing this request and welcome additional feedback here.
ORTB	Request for two new hooks for auctionConfig and generateBid response adaption in ORTB.	We are reviewing this issue and welcome additional feedback here.
Previous Win	Request for IG defining a prevWinsTransformer, that takes in the previous wins of the IG and outputs a serializable thing.	We are reviewing this issue and welcome additional feedback here.
Content Types	Strategy for evolution of content types, e.g. JSON to something like CBOR.	We are reviewing this issue and welcome additional feedback here.
Prebid in Protected Audience API	Request for a sample publisher page that uses prebid in order to run an end-to-end flow for Protected Audience auction.	We are considering this request and welcome additional feedback from the ecosystem on why this should be prioritized. We have also seen ecosystem participants producing sample publisher pages that are available for others in the ecosystem to demo.

Protected Auction Services

Feedback Theme	Summary	Chrome Response
Trusted Execution Environments (TEEs)	More expensive to run Trusted Execution Environments in public clouds as opposed to on-premise ad tech data centers?	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. 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.
(Reported in previous quarters) On-premise TEE	What are the requirements for someone to become a TEE provider?	Our response is similar to previous quarters: “While we are continuing to explore support for options beyond public cloud-based solutions, including considering which deployments would be acceptable from a security perspective, 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 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."
Limits of Key/Value Server	Limits of keys per auction per server	We are discussing this issue and welcome additional feedback here.
K-anon restrictions	Confirmation that K-anonymity will not be enforced in the future on K/V keys.	We have no current plans to enforce k-anon on keys of K/V server requests as we are aiming to move K/V servers into TEE in future.

Building K/V service	Does Google have pre-built artifacts available for the K/V service?	We currently do not have any pre-built artifacts for the Protected Audience Key/Value server, though we may consider providing them if we are hearing strong demand for it from the ecosystem.
EgId support in B&A	Request for supporting field experimentGroupId in Bidding & Auction code and in request to KeyValue service from BuyerFrontEnd	B&A currently doesn't have the support for experimentGroupId, but aims to roll this out by Beta 2 (currently scheduled for February 2024). We have shared additional information here.
API usage	Request coalescing in HTTP can help protect against on-path attackers, but the operator of the TEE will learn sizes.	We are discussing this request and welcome additional feedback here.
Improve documentation	The specification is unclear how the k-v server will be addressed.	We are discussing this issue and welcome additional feedback here.
API usage	What is the purpose of "Ad-Auction-Result" and adAuctionHeaders?	We are discussing this issue here and welcome additional feedback.
Improve documentation	Unclear if v2 design has been propagated into FLEDGE.md.	FLEDGE.md talks about how Chrome sends requests to BYOS-KV. The v2 protocol design is limited to TEE-KV only and not currently supported by Chrome.

Measuring Digital Ads

Attribution Reporting (and other APIs)

Feedback Theme	**Summary**	**Chrome Response**
Cross-environment measurement	How does Chrome plan to support cross-environment measurement in the interim phase where 3PCs have been removed from Chrome mobile, but the Privacy Sandbox for Android is not yet available?	On the Android side, we're working on expanding PSB/ARA coverage - Attribution Reporting API (ARA) is available on Android 13 and 14, and we plan to begin expanding to Android 11 and 12 later this year, although that is subject to change. We won't be able to expand to Android 10 or older, but we expect the percentage of Android devices still on Android

		10 or below to be lower at 3PCD and naturally decrease over time as users upgrade. We welcome additional feedback from the ecosystem on this request.
Filtering	Filtering "conversions" from creative scanning.	We have reached out to this stakeholder to better understand their request, and welcome additional feedback from the ecosystem on this issue.
Third-Party Ad Servers	How will PA API and ARA work with Third-Party Ad Server tags?	Similar to how pixels work with impression and click tags today, an ad server can either set source and trigger registrations for ARA on their own (including from Protected Audience auctions), or they can set up redirects to pass and accept source and trigger registrations for ARA.
DCM	Support of attributionsrc by DCM and other third party ad servers.	This is a DCM related issue and has been addressed by the DCM team in this GitHub issue.
Hierarchical Aggregation Key	Is it necessary to split all the contribution budget into all these hierarchical keys?	We have discussed and provided an answer to this stakeholder. When using a hierarchical key structure the ad-tech must consider that the contribution budget is shared across all keys output for an impression.
Use different Sub-Domains	Make attribution reporting to work with sources and triggers registered on different sub domains but the same eTLD+1?	We have discussed this question with the stakeholder and proposed the following solutions. They can either change their URL setup to have the same reporting origin on source and trigger, or redirect from their current URL to a common URL before performing their registrations. We are open to additional ecosystem feedback if the proposed solutions do not work for their use case.
(Also reported in previous quarters) Production Support	What levels of service are available to support partners using ARA?	Our response is unchanged from previous quarters: "Google provides a range of channels to allow ad techs to report technical issues and enable any necessary escalations to resolve such issues. In addition, Chrome expects to further build and scale a process to resolve technical issues and escalations affecting the health of

		the ecosystem. Chrome is committed to ensuring resources for this effort. Please see our developer post for more information on the public and private forums for feedback and escalation."
(Also reported in previous quarters) Timeline	Will Google have "Phase 2 Full Flexible Event-Level" ready by the beginning of CMA Quantitative testing?	Phase 2 Full Flexible Event-Level is expected to be available in Chrome in Q1 2024. You can track the status here.
(Also reported in previous quarters) Conversion funnel	Report multiple domains that were used in conversion.	This use case is possible since the addition of multiple destinations. We welcome additional feedback.
Reporting testing labels	Will the reporting capabilities allow testers to report which group the user (Chrome browser) is part of (Mode A/B)?	We are working on publishing a testing guide for capturing Chrome testing labels in ARA.
Documentation	The documentation for Attribution-Reporting-Register-Source states that expiry will be rounded to the nearest day, how will it be rounded?	Rounded to the nearest day would mean 1.5 days will be rounded to 2 days.
Use different Sub-Domains	Request to receive Attribution Reporting API reports in a different subdomain as the source and trigger registration.	This is not possible. HTTP redirects can be applied but there's no setup for this. We welcome additional feedback from the ecosystem on why this request is useful.
Event-level reporting delay	7-day attribution and reporting window but due to event level reporting delay, it may take longer than 8 days for all reports to come through.	We acknowledge the feedback and welcome additional input from the ecosystem on whether this delay in event-level reporting is an issue or not, especially with the move from fixed to flexible event reporting windows.
Conversion triggers	Conversions triggers that occur between the end of the first event_report_window (1h) and the expiry time (1Day) won't generate reports.	We have introduced flexible event-level configuration which moves from fixed to flexible event reporting windows.

Noise	Are event-level reports noisy fake conversion as described on the GitHub explainer?	Yes, noise is applied to event-level reports and is representative of all possible output states, including different trigger_data, not reporting anything at all when a trigger actually occurred, or potentially reporting multiple fake reports for the event. The noise % is open sourced and can be made flexible via flexible event level configurations.
Filtering	Using filtering with Attribution Reporting API would still consume the contribution budget even though it does not record the aggregation key.	This is working as intended since aggregatable_trigger_data only supports filtering on the trigger key pieces themselves, not on the values / keys. Top-level filters can support filtering the keys themselves, but this is shared by event + aggregate so it's not applicable here. We welcome additional feedback from the ecosystem here if filtering on keys is necessary.
Storage Limit	Request to introduce a storage limit that also considers the reporting origin.	An increase from 1024 to 4096 of this limit will be effective from M120 and we welcome additional feedback from the ecosystem here.
Direct Attribution	How to get metrics for situations where a user visits an advertiser directly without going through a publisher, since the standard attribution reporting process does not cover this scenario?	ARA is only designed to recover cross-site information (i.e. the join of information across publisher/advertiser sites). If there is no cross-site information required, then ARA will not help you. We are discussing this issue and welcome additional feedback here.
Report Time	Get scheduled_report_time the time from a timeserver instead of using the local machine time.	We currently do not have any plans to use a timeserver, and we have not heard much demand for it from Ad Tech. We would be interested in hearing additional feedback from the ecosystem on whether this would be a useful feature.

Aggregation Service

Feedback Theme	**Summary**	**Chrome Response**
(Also reported in previous quarters)	Can the Aggregation Service be deployed in on-premise	While we are exploring potentially supporting options beyond cloud-based solutions, it is not

On-premise solution	data centers?	currently feasible to support on-premise TEEs given on-premise security limitations that would require a time-consuming evaluation for Privacy Sandbox. Given Privacy Sandbox security requirements and the significant challenges presented by on-premise deployments, we believe that continuing to expand and improve cloud-based deployments (e.g. supporting GCP in addition to AWS) is the most beneficial for the ecosystem. However, we welcome additional feedback here on why such a requirement is necessary.
Enclave	If the enclave is not up or suddenly receives an error, how is it handled by the Aggregation Service API?	We will use retries if the enclave fails at startup and autoscaling to bring up new instances if an instance is seen as unhealthy. Adtechs can also investigate failures using logs. To debug enclave failures on AWS, ad techs can check the status of their EC2 instance by logging into their AWS Console Manager. Ad techs can also log in to the Nitro Enclave host instance and check the enclave status with the nitro-cli tool. If there are any errors/failures, they can use the AWS command line interface to view the logs and investigate further. To debug enclave failures on GCP, adtechs can check the status of their instance via the Cloud Console. They can also check for errors using the list-errors-command.
Use different Sub-Domains	Request to register multiple (sub)domains to use multiple instances of Aggregation Services, both in dev and prod environments.	Site enrollment has been launched so ad techs can register multiple subdomains of the same site on one AWS account or GCP project. They will also be able to register the same domain on multiple AWS accounts or GCP projects. We welcome feedback from the ecosystem.
Privacy Budget	How to better debug privacy budget exhaustion related issues?	Currently we are looking into solutions to provide more details on the exhausted budget and also improving our documentation to outline strategies adtechs can use to minimize occurrences of this error. We will update the Aggregation Service GitHub page once we have a proposal.
Epsilon value	Request to increase epsilon	The Aggregation Service's epsilon value will be

	value.	kept as a range of up to 64, to facilitate experimentation and feedback on different parameters during 3PCD. We will provide advanced notice to the ecosystem before the epsilon range values are updated.
Binaries	Publish a more complete set of binaries for Aggregation Service releases.	We are reviewing this request and welcome additional feedback.
API usage	Sharing data with Coordinators, in light of the Coordinator Terms of Service.	We are seeking clarification on this issue and welcome additional feedback.

Private Aggregation API

Feedback Theme	Summary	Chrome Response
Debugging	Enable additional options for debugging during Mode B testing.	As shared in this Github issue, we are moving forward with allowing debug mode in Mode B. This eligibility is changing in M121 Beta at 50% of Mode B traffic starting on 1/31. We will provide notice before ramping up to Stable.

Limit Covert Tracking

User Agent Reduction/User Agent Client Hints

Feedback Theme	Summary	Chrome Response
ChromeOS	Support User-Agent Client Hints for the bitness of Chrome OS.	We have shared a response to this request here.

IP Protection (formerly Gnatcatcher)

Feedback Theme	Summary	Chrome Response
Abuse	Google may be able to view user's browsing data through	IP Protection tunnels traffic through two proxies (one run by Google, one by another company).

	IP Protection.	That ensures that Google cannot see browsing data. All traffic is encrypted between Chrome and the proxies, so the Google proxy has no information about what websites are being browsed. Additionally, the system uses blinded authentication tokens to minimize access to user identifiers at the proxies. All the Google proxy will see is that an unknown client at a specific IP is using the proxy system. No information about websites visited or ads loaded is available.
Headless Mode support	How will bots using plugins and headless mode be managed?	Mitigating abuse of IP Protection is a key priority for the team. We have carefully considered these scenarios (amongst many other potential threats as well) and are working on options that will help reduce the likelihood abuse or fraud is successful. While we cannot provide more details at the moment, we expect to provide them in the near future and look forward to continuing the discussion.
Existing proxies	How will IP Protection work with existing proxy settings on Chrome?	Existing proxy configurations will remain supported. Users will be able to configure their own custom proxies as before.
Abuse Reporting	How will abuse reporting be handled?	We will have more details to share in the near future, but we plan to have a mechanism for organizations and users to share reports and evidence of abuse.
Regulations	How will IP Protection follow local laws and regulations?	Google is committed to complying with local laws and regulations, and circumventing such country-level blocks may not be allowed. This feature is not intended for circumvention.
Limiting capabilities	Will IP Protection block our cyber response?	We strive to strike a balance between protecting users from being tracked across the web based on their IP addresses while minimizing disruption to the normal operations of servers, including the use of IP addresses for anti-abuse. While we cannot provide more details at the moment, we expect to provide them in the near future and look forward to continuing the discussion.
Timeline	If this is going to be enforced before the end of 2024, it will	Chrome will initially launch IP Protection as an opt-in setting for users in specific regions,

	be nearly impossible to prepare for it.	understanding that this could be a significant change for how some companies rely on IP addresses, and seeking to minimize disruption as the ecosystem adjusts. IP Protection will transition to default on no sooner than 2025.
API usage	Will a user be given a choice to toggle IP Protection the first time they open Chrome?	We plan to provide users the choice on whether they want to use IP Protection or not. The mechanics of presenting this option to users is still being developed.
API usage	How much data is logged and for how long that data is retained?	We will have more details to share in the future, but we plan to log minimal amounts of data.
Negative feedback	Users can use VPNs if they prefer to use them. No need for PS APIs.	The goal of IP Protection is to prevent the usage of IP addresses for the purpose of cross-site tracking, it is not intended to be a VPN service.
API safety	How to prevent first party to access IP address and forward info via parameter of header?	We're initially focusing on third parties as we see that as having the most impact. We will continue to monitor the ecosystem to determine whether we need to evolve our approach to prevent scaled circumvention.
API usage	Confirmation needed if understanding of API usage is correct.	IP Protection uses a list-based approach to identify which third-party traffic goes through the proxies. Origins that are on the list but are accessed in a first-party context will not be proxied through this service for those connections. For example, if an analytics company is on the list of domains and a user navigates directly to the site, that site will still be able to observe the user's IP address instead of the proxied IP address. However, if that domain on the list makes a network request in a third-party context, the connection will be proxied and the user's original IP address will not be visible to the site. Our ultimate goal is to prevent cross-site tracking of users across the web. We are working through some details before sharing more information about which third-party domains we plan to focus on initially.

VPN	Concern that Google's proposal could be disadvantageous for other VPN providers.	The goal of IP Protection is to prevent the usage of IP addresses for the purpose of cross-site tracking, it is not intended to be a VPN service.
Timeline	What is the IP Protection timeline?	IP Protection will be opt-in initially. This will help ensure that there is user control over privacy decisions and that Google can monitor behaviors at lower volumes. IP Protection will roll out in a phased manner and will transition to default on no sooner than 2025. Like all of our privacy proposals, we want to ensure that we learn as we go and we recognize that there may also be regional considerations to evaluate. We are using a list-based approach and only domains on the list in a third-party context will be impacted. We are conscious that these proposals may cause undesired disruptions for legitimate use cases and so we are just focused on the scripts and domains that are considered to be tracking users.
Limiting capabilities	User's IP addresses cannot be looked up in WHOIS anymore.	Our position is that the IP address is a stable identifier whose use can have privacy implications for users, including the use of metadata associated with it such as ASN. With IP Protection we're trying to strike the right balance between privacy and supporting a helpful user experience on the web, for example with our approach to IP geolocation. If this metadata isn't sufficient for your use case, we are open to discussing that further.
HTTP Referer	Will the original HTTP Referer be preserved?	There are no plans to alter the Referer header as part of IP Protection, as discussed here.
Open source	Will IP Protection source codes be open source?	The majority of the software here is open-source as part of the Chromium and Envoy Proxy projects, but some components are closed-source, as explained here.

Bounce Tracking Mitigation

Feedback Theme	Summary	Chrome Response
Storage deletion	Does Bounce Tracking Mitigation (BTM) delete Shared Storage and Attribution Reporting storage?	We did not intend for BTM to delete Privacy Sandbox API storage (ARA, PA API, Shared Storage, Private Aggregation, Topics). BTM should only delete storage types which have privacy risks if accessed in a third-party context. A bug fix is in progress.
API usage	Which Chrome version will BTM activate? Will redirect/bounce tracking after 10 seconds be considered as Bounce tracking by BTM or not?	In M116, BTM rolled out to 100% of users with 3PCs blocked. Currently a redirect after 10 seconds is not considered a bounce.
Sign in use case	Automatically synchronize/maintain sign-in state across multiple domains, without being punished for tracking-like behavior?	We are discussing this request here and welcome additional feedback from the ecosystem.
User journey	Currently BTM results in complicated user journeys.	We are discussing the issue and shared our thoughts on this here.
Storage Access API	BTM in Chromium will honor 3PC grants from storage access API (SAA).	We have discussed this issue with ecosystem participants at TPAC 2023 and welcome additional feedback here.
Impact on ads reporting	Bounce Tracking Mitigation may lead to smaller companies in the ecosystem relying on other Privacy Sandbox APIs like ARA to carry out ads use cases.	Bounce tracking mitigations are intended to prevent circumvention of 3PCD. ARA is one of many alternative measurement solutions companies will have available after 3PCD, but no company is required to use it.

Privacy Budget

No feedback provided this quarter.

Strengthen cross-site privacy boundaries

Related Website Sets (formerly First-Party Sets)

Feedback Theme	Summary	Chrome Response
(Also reported in previous quarters) Related Website Sets (RWS) domain limit	Request for expanding the number of associated domains.	At present, we do not expect to increase the numeric limit. The limit was established based on user privacy considerations, feedback from ecosystem stakeholders in the W3C, and consideration of comparable implementations in other browsers. For additional information, please see our blog posts (1, 2). We recommend examining use cases that require cross-site cookie access beyond the numeric limit, and consider leveraging our guidance for identity use-cases, authenticated embeds, and advertising use cases.
Scope of cookie access	Concern that all domains in a RWS will have granted access to read and write all cookies from all domains.	Membership in a RWS does not result in members being able to access each other's cookies. Instead, this would allow members to access their own cookies when embedded on other same-RWS sites (after a Storage Access API invocation).
(Also reported in previous quarters) RWS + CHIPS integration	Request for RWS + CHIPS integration in order to support use cases such as A/B testing	We continue to solicit use cases and requests for this feature here. For now, we are weighing the need for this feature against cross-browser interoperability risks.
API usage	What if a user manually removes sites from their Chrome settings locally?	We currently do not have a way for a user to manually delete a site from a group. The user can instead choose to turn off the "related sites" feature using the toggle below "Block third-party cookies"; or "Block all third-party cookies" on the new Tracking Protection settings panel.
Cross Domain communication	Will RWS allow cross domain communication?	We are currently running an Origin Trial to expand access to some types of unpartitioned storage (including localStorage and Broadcast Channel) via Storage Access API that will enable this communication. This capability is available in all supported configurations of Storage

		Access API, across the same RWS, and also across non-RWS sites. This blog post has additional information.
requestStorageAccessFor	Can document.requestStorageAccessFor(origin) return a promise that resolves with origin's cross-site cookies?	This is not possible. Since the invocation happens from the top-level origin (which is different from the origin passed in as the argument), doing so would violate the Same Origin Policy.

Fenced Frames API

Feedback Theme	**Summary**	**Chrome Response**
(Also reported in previous quarters) Native Advertising	Fenced Frame support for Native Advertising.	We previously shared that some Privacy Sandbox technologies will be required in the future to further strengthen privacy protections. For example, for Protected Audience, we'll require use of Fenced Frames for ad rendering, and transition away from event-level reporting, no earlier than 2026. We've provided "no sooner than" dates for each of these future requirements, so the industry has clarity on the intended evolution of the APIs. The additional time allows us to continue working with the industry to design and implement support for a broader range of critical use cases. For example, we will evolve Fenced Frames ahead of their requirement in 2026+ to maintain support for video and native ads with Protected Audience API. Per our Commitments, the CMA will be consulted on such changes, and we will continue engaging with feedback from the ecosystem ahead of implementing those "no sooner than" requirements.
Size difference across platforms	Reports that the size of content displayed in the Fenced Frame looks different between desktop and smartphones.	We are looking into the issue and welcome additional feedback here.
Render adComponent	Provide sample codes on how to render adComponents in Fenced Frame?	We will be looking to provide documentation on how to use navigator.adAuctionComponents(numComponents) inside the Fenced Frame to display an ad

		composed of multiple pieces.
Improve API	Provide more signals to FencedFrames (improve e.g. brand safety).	We welcome the proposal and welcome additional feedback here.

Shared Storage API

Feedback Theme	Summary	Chrome Response
Anti-abuse / Anti-fraud use case	Potential of using Shared Storage for fraud or anomaly detection.	We discussed the possibility here and welcome additional feedback.
Frequency Capping	Provide a way for cross-site frequency capping outside of PA API.	We appreciate the feedback that cross-site frequency capping outside of PA API is a valuable use case. At this time, Privacy Sandbox remains focused on its current set of APIs for 3PCD. However, we welcome additional feedback from the ecosystem on this use case here.

CHIPs

Feedback Theme	Summary	Chrome Response
Popup/Redirects	How will CHIPs support embedded authentication use cases involving pop-ups and redirects?	We recently shared some guidance on checking the impact of the 3PC phaseout on your sign-in workflow and we welcome additional feedback here.
Partition limit	Reduce overall per-site per-partition limit to 1 KiB.	We are considering this request and welcome additional feedback here. We will continue to monitor feedback as we continue rolling out 3PCD and developers adopt CHIPs and provide feedback.
Cookie migration	Recommended process for migrating a web app to issue cookies as partitioned which does not break ongoing cookies/sessions?	We proposed a potential scheme for migration in our response here; but the developer was able to formulate an alternative solution that worked better for their configuration.

API usage	Is the access to partitioned storage disabled when a user does not opt-in to the Ad Privacy APIs setting?	Partitioned storage and partitioned cookies (CHIPs) are enabled even if a user does not opt-in to the Ad Privacy APIs setting ; since they do not enable any cross-site transfer of information. As a general principle, cross-site transfer of information will be subject to limits, checks, or user opt-in; but these currently do not apply to CHIPS.
API usage	What is the rationale for eventually blocking unpartitioned cookies, rather than the browser just "silently" partitioning them?	This is not possible in the short and medium term, as explained here.

FedCM

Feedback Theme	**Summary**	**Chrome Response**
API usage	Unable to serve 'well-known file' on eTLD+1 within the development environment.	We have updated Chrome Canary to skip fetching the well-known as discussed here.
API usage	Are there any specific user interaction requirements defined to request for third party sign-in permissions or using FedCM?	There are no specific user interaction requirements, as discussed here.
API safety	Are there any plans to have a flow which allows the client to initiate FedCM, but essentially the Tokens are transferred from IdP to a backend-system of the RP?	We are discussing and welcome additional feedback here.
Opt-In	Allow IDP to opt-in to receiving the RP's client ID, so users can decide if they trust the IDP or not.	We are discussing this request and welcome additional feedback here.
API usage	Request for more documentation on FedCM.	We acknowledge this feedback and will continue to improve documentation as we continue to develop this API.

Fight spam and fraud

Private State Token API (and other APIs)

Feedback Theme	Summary	Chrome Response
Documentation	Request for a detailed developer guide on Private State Tokens to assist with testing.	We have published a developer guide for Private State Tokens in Q4 2023.
Age/Gender Verification	Difficult to perform "age & gender" verification of audiences post 3PCD.	Private State Tokens is currently not designed for age and gender verification. We are seeking to understand the use case better, and how this is accomplished today, and welcome additional feedback.

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 plans below:

Protected Audience API for Remarketing:

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

Measurement APIs:

- In Q4 2023, Google Ads published a technical explainer on how third-party ad tech could improve Event and Aggregate-API data from the Privacy Sandbox Attribution Reporting API via optimized configuration.
- In Q4 2023, Google Ads conducted an experiment with the Attribution Reporting API (utilizing both Event-level and Aggregate-level reports) on Chrome Desktop and Mobile Web utilizing General Availability traffic from a subset of Google Owned and Operated properties. The results have been shared with the CMA.
- In Q1 2024, Google Ads plans to continue the experiments with the Attribution Reporting API (utilizing both Event-level and Aggregate-level reports) on Chrome Desktop and Mobile Web utilizing General Availability traffic from an expanded set of Google Owned and Operated properties and also from non-Owned and Operated/Display.

Chrome-facilitated testing:

- In Q1 2024, Google Ads plans to conduct an experiment to test privacy-preserving solutions and Chrome's Privacy Sandbox APIs in combination (Topics, Protected Audience and Attribution Reporting) via Chrome-facilitated testing on Desktop and Mobile Web with traffic from the Google Display Network. We encourage authorized external parties (Demand Side Platforms aka DSPs and Supply Side Platforms aka SSPs) to participate in this experiment with us.

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.

Experiments and Testing - Google has engaged with the CMA to help the ecosystem prepare for experiments and testing. To facilitate testing, as of 4 January 2024, Google has disabled third-party cookies for 1% of Chrome Stable browsers (see the dedicated Google Ads section above). Google has also published a blog post to help users understand the changes to the Chrome browser to facilitate this testing. Chrome is also offering a third-party deprecation trial which allows embedded sites and services to request additional time to migrate away from third-party cookie dependencies for non-advertising use cases, supplemented by a deprecation trial for top-level sites to help websites mitigate user-impacting problems due to third-party cookie issues of their third-party providers.

The CMA has shared stakeholder feedback that Google is selective about its audience for testing which does not reflect the views of market participants, and that there is a risk that smaller publishers are less likely to get involved in testing than larger publishers, and therefore may be underrepresented in the results. Google does not determine which market participants take part in testing, and encourages all interested market participants to test the Privacy Sandbox APIs. For example, the SSPs who have publicly identified themselves as testing participants - see above - serve a wide range of publisher types and sizes, and can work with their publisher customers to participate in tests. Google worked with the CMA to publish testing guidance for third parties: most recently in October 2023, additional guidance to third parties on testing to provide detail on how market participants should use Google's testing modes in Chrome in order to generate results which are comparable and informative to the CMA's assessment of the Privacy Sandbox APIs.

The CMA has also shared stakeholder feedback that the Market Testing Grants provide financial incentives for market participants to produce positive results. As noted above, Google made grant funding available in order to encourage market participants to test the Privacy Sandbox APIs. However, grantees will undertake their testing in line with the CMA's guidance to third parties on testing, focusing on their own use cases, product strategies and business goals, and will submit their results directly to the CMA. We have been pleased to understand that the CMA is speaking directly with grantees about their testing plans. Grantees have been informed that they are not required to share any insights from their preliminary tests, or Final Effectiveness Test results with Chrome. As noted by the CMA in its Q3 2023 update report, the CMA has "*closely scrutinised the terms of Google's agreements with the funding recipients, and [the CMA is] continuing to engage with Google to make sure [the CMA has] all the details so [the CMA] can have confidence in the robustness of the test results [the CMA receives].*"

The CMA has shared stakeholder feedback that current Privacy Sandbox specifications lack the detail needed by a consuming engineer to understand explicitly how the associated interfaces will operate, including all the restrictions and features of the interfaces, and that testers are reliant on non-specification documents such as developer explainers, GitHub comments, blog posts, and videos. Google has published a large amount of technical documentation which continues to be updated and expanded based on developer feedback. Google also holds Office Hours and provides a dedicated Privacy Sandbox Developer Support GitHub repository which allows for developers to raise developer-specific questions and issues. A number of companies have been able to integrate the Privacy Sandbox APIs, and begin testing based on the documentation available - details of testers who have publicly identified themselves are listed above. Google is also pleased to note that some market participants are publishing their own implementation overviews and anticipates expanded guidance and best practices shared by early adopters, alongside Google's documentation.

IP Protection - The CMA has shared stakeholder feedback with Google regarding IP Protection, and the Intent to Experiment for Phase 0. This functional test allows Google to test its infrastructure and the integrations between various components for bugs, stability and

reliability, while avoiding any impact on other companies. In this initial test, only Google domains are affected.

After this initial functional testing, IP Protection will be released as a beta opt-in feature, giving users the option to enable IP Protection. IP Protection will transition to default on no sooner than 2025. At that time, Google envisions that there will be a setting for users to opt-out of the feature. IP Protection will mask the IP address only for the domains specified on the list. Domains (whether operated by third parties or by Google) that are not on the list will be unaffected, and will be able to see the IP address when users visit their websites. Thus publishers will continue to have access to the IP addresses of users visiting their websites. Google Ads will be subject to the application of IP Protection, and will therefore be unable to access IP addresses in the same circumstances as its competitors.

The CMA has shared stakeholder feedback that after the introduction of IP Protection, internet service providers (ISPs) will no longer have visibility of data via an IP address whilst leaving Google with the ability to monitor and process such data at all times. This is not accurate. In respect of data an ISP could obtain through an IP address, even when IP Protection is enabled by default, the only traffic included will be traffic to third parties identified as potentially using IP addresses for web-wide cross-site tracking. Only domains called in a third-party context will be impacted by IP Protection. In respect of Google's ability to monitor and process IP address-related data, on a technical level, the IP Protection feature is Chrome's proposed solution to prevent a user's IP addresses from being used as a tracking mechanism and to make sure no entity can view a user's IP address and the domain their traffic is being sent to. IP Protection fulfills this by leveraging a two-proxy architecture to route users' traffic. An external CDN will run one proxy while Google runs the other proxy. This implementation ensures that Google can only view a user's IP address but not the destination domain.

The CMA also shared a stakeholder concern that IP Protection might affect the way companies will be able to execute their contracts with publishers in the future, thus creating an anti-competitive barrier in favor of Google's Privacy Sandbox. As mentioned above, after IP Protection is implemented, publishers will continue to have access to the IP addresses of users visiting their websites. Google does not have visibility into, or control over, how publishers subsequently make use of this information, including in respect of how they execute contracts with third parties.

Public fora for stakeholder feedback - The CMA shared a stakeholder query, asking from which public fora, in addition to the World Wide Web Consortium (W3C), is Google actively considering "reasonable views" as required by the Commitments. In addition to feedback received through the feedback form, and W3C, Google enables stakeholder engagement, and takes into consideration stakeholder feedback from a number of public fora.

Each Privacy Sandbox proposal is open to public discussion, where proposal authors and web stakeholders collaborate to answer open questions and clarify implementation details before features are finalized. Explainers and supporting content for each proposal are hosted on

GitHub. This enables all stakeholders with a GitHub account to raise an Issue in the repository to start or participate in a discussion. Proposal authors, including Chrome product managers and engineers, are active in these discussions, and Google takes into consideration feedback received through GitHub. The Privacy Sandbox Developer Support GitHub repository also allows for developers to raise developer-specific questions and issues. Feedback and discussion options for individual Privacy Sandbox proposals can be found in the API status and feature releases.

For Privacy Sandbox proposals which require features to be built in Chromium, every stage of feature development on Chromium is announced to a public mailing list, which encourages further discussion of technical implementation. Proposal developers submit requests to begin each stage of feature development on the public blink-dev mailing list. This mailing list is open to the public which allows interested stakeholders to follow along with the discussion on each milestone and join the list to ask additional questions. Individual features can be tracked on the Chrome Status site. As individual proposals progress through implementation in Chromium, a proposal-specific mailing list may be created to allow for focused communication. This allows for announcements and discussion of origin trial updates, necessary code updates, or known issues that may impact development. As with blink-dev, these lists are public.

Google also enables stakeholder feedback through participation in standards bodies. In addition to the W3C, the Internet Engineering Task Force (IETF) develops open standards for all web platforms. These standards bodies encourage interested parties to discuss and learn about individual standards as well as the web ecosystem at-large. New web platform technologies, like Privacy Sandbox technologies, are proposed and discussed in various forums across these standards bodies. These forums are open to anyone who wants to actively participate in the design and development of the technologies. Proposal authors will often present overviews and progress updates at associated meetings, providing an opportunity to ask direct questions and hear from other stakeholders. Google takes into account stakeholder feedback raised in various forums across these bodies, and meeting minutes for most standards groups are publicly available.

For the sake of completeness, Google also participates in a number of other fora including global industry associations, such as the Interactive Advertising Bureau, the Association of Online Publishers (AOP), and the German Association for the Digital Economy (BVDW). While participation in meetings and presentations to industry associations may require paid membership, these groups often represent hundreds or thousands of stakeholders such as ad tech companies, publishers, advertisers and agencies.

Bounce Tracking Mitigations - The CMA shared stakeholder feedback that Google launched BTM without sufficient industry consultation, as required by the Commitments. Since publishing the BTM proposal in September 2022, Google engaged in a significant amount of industry consultation prior to the launch of BTM. This included seeking feedback via the GitHub repository, as well as from a number of W3C groups including the Privacy Community Group, the Federated Identity Community Group, and the Web Payments Working Group.

Related Website Sets - The CMA has shared stakeholder feedback that limited feedback on Related Website Sets is due to poor knowledge within the ecosystem. Throughout the development of Related Website Sets Google has engaged with the ecosystem and taken into consideration ecosystem feedback in order to improve the proposal, including through the W3C's Privacy Community Group, and the Web Platform Incubator Community Group, including holding public office hours (conducted in multiple languages) presenting at various conferences with thousands of attendees, and posting public videos explaining the proposal. In addition, Google has made a wide range of resources regarding Related Website Sets available on a dedicated GitHub repository, and on our various developer sites. We are processing set submissions in a timely manner while continuing to receive feedback and address questions about the design and usage of the API. We welcome additional feedback and questions on Related Website Sets.

Protected Audience API - The CMA has shared stakeholder feedback that Google has closed feedback to third parties on PA API, but appears to have continued making changes at the request of Google Ads. We remain open to feedback from all parties, and we continue to make changes as a result. During the period of testing on specially-labeled slices of traffic, we are deliberately making behavior changes to those slices only when necessary, to avoid disrupting the ongoing gathering of experimental data.

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 December 2023, Google has complied in the preceding three-calendar-month period with the obligations relating to:

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

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

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

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

Date.....[redacted].....

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