Privacy Sandbox Progress Report

Q1 Reporting Period - January to March 2025
Prepared for the CMA, 29 April 2025

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 developer documentation which provides overviews for the core private advertising features and cookie changes, along with API implementation and status information. Key updates are shared on the developer blog along with targeted updates shared to the individual developer mailing lists.

Updated Timing Expectations

In April 2025, Google published a blog post on Next steps for Privacy Sandbox and tracking protections on Chrome, announcing that Google has made a decision to maintain the current approach to offering users third-party cookies in Chrome, and will not be rolling out a new standalone prompt for third-party cookies. Users can continue to choose the best option for themselves in Chrome's Privacy and Security Settings. In light of this update, we understand that the Privacy Sandbox APIs may have a different role to play in supporting the ecosystem. We'll engage with the industry to gather feedback and share an updated roadmap for these technologies, including our future areas of investment, in the coming months. No updates were made to the Privacy Sandbox Timeline in Q1 2025.[1]

[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

Taking into account observations made by third parties

Glossary of acronyms.

ARA	Attribution Reporting API
CHIPs	Cookies Having Independent Partitioned State
DSP	Demand-side Platform
FedCM	Federated Credential Management
IAB	Interactive Advertising Bureau
IDP	Identity Provider
IETF	Internet Engineering Task Force
IP	Internet Protocol address
openRTB	Real-time bidding
OT	Origin Trial
PA API	Protected Audience API (formerly FLEDGE)
PatCG	Private Advertising Technology Community Group
RP	Relying Party
RWS	Related Website Sets (formerly First-Party Sets)
SSP	Supply-side Platform
UA	User-Agent string
UA-CH	User-Agent Client Hints
W3C	World Wide Web Consortium
WIPB	Willful IP Blindness

General feedback, no specific API/Technology

Feedback Theme	Summary	Chrome Response
User Choice	It is unclear what Google's updated approach to elevate user choice will look like, how it will be presented to users, and the anticipated opt-in/opt-out rates. Further information is required to distinguish this from third-party cookie deprecation.	In April 2025, Google published a blog post on Next steps for Privacy Sandbox and tracking protections on Chrome, announcing that Google has made a decision to maintain the current approach to offering users third-party cookies in Chrome, and will not be rolling out a new standalone prompt for third-party cookies. We will provide further updates as available.

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.

Fingerprinting	Google has shared no information with publishers or marketers about how they can rely on any alternatives to Google's Ad Systems without using more risky consumer identity as a common match key (ie fingerprinting).	We've highlighted several, non-Google Ad Systems that are offering solutions to publishers and marketers which are built in part on Privacy Sandbox APIs. This includes non-Google Ad Systems across markets and channels. Further details and case studies are available in the Business Resources section of privacysandbox.com here.
Privacy Sandbox	The Privacy Sandbox APIs would replace internet data ingredients with Google's own finished products. Since Google's alternative is an API, it is offering access to a product that it owns and controls, and one that is subject to terms and conditions that Google has discretion over. That is not a substitute for components that are used by others to make their own finished products.	The Privacy Sandbox APIs have been developed and implemented following extensive engagement with regulators and a wide range of ecosystem stakeholders. As with other platform technologies, Privacy Sandbox APIs must take into consideration that they will be used as components in others' finished products and we welcome ecosystem efforts to develop additional technologies to work alongside the Privacy Sandbox APIs.
User Choice	Request for information on whether Google's updated approach to 3PCs on Chrome will meet certain regulatory requirements, which may impact stakeholders consent management platform experience.	In April 2025, Google published a blog post on Next steps for Privacy Sandbox and tracking protections on Chrome, announcing that Google has made a decision to maintain the current approach to offering users third-party cookies in Chrome, and will not be rolling out a new standalone prompt for third-party cookies. We will provide further updates as available.
Privacy Sandbox Timeline & Adoption	Ad techs have paused Privacy Sandbox API testing and are seeking stronger reasons to reinvest in these technologies for product and marketing activities. Their reinvestment decisions are heavily influenced by the need for greater clarity on the User Choice timeline, as well as concerns around Protected Audience API (PA	In April 2025, Google published a blog post on Next steps for Privacy Sandbox and tracking protections on Chrome, announcing that Google has made a decision to maintain the current approach to offering users third-party cookies in Chrome, and will not be rolling out a new standalone prompt for third-party cookies. We will provide further updates as available. Chrome PA API auctions are 35% faster year-over-year. On top of that, we've seen a significant increase in usage of parallelized

	API) latency and the B&A roadmap. Additionally, there are concerns about the upcoming CMA Commitments review, particularly regarding Google's role as the primary driver of Privacy Sandbox technologies without relying on 3P identifiers, and the overall future direction of the initiative to inform investment strategies.	auctions, which provides an even larger win for those auctions. Our current B&A roadmap is available here.
Privacy Sandbox Timeline	What was updated in the Privacy Sandbox Timeline page?	An overview for the Topics API was recently added to the Privacy Sandbox Timeline page.
Privacy Sandbox	Are there any research papers on Privacy vs. Utility to help understand the impact of Privacy Sandbox on revenue?	Relevant Market Case Studies which address these questions are available here and results from Privacy Sandbox APIs testing are available here.
Privacy Sandbox Adoption	An early adopter reported initial challenges with the Privacy Sandbox APIs due to slow adoption by larger companies, impacting test launches. However despite this, the Privacy Sandbox team's collaborative approach and responsiveness to feedback was appreciated.	We appreciate the early adopter's feedback. We are committed to collaborating with early adopters and we will continue to engage with the ecosystem and gather feedback as we evaluate the role of the Privacy Sandbox technologies in supporting the ecosystem.
Chrome Testing	Concern over the ability to continue Privacy Sandbox testing effectively after the removal of testing labels highlighting significant difference in traffic quality between Chrome with 3PCs disabled (Mode B) and users who have personally disabled 3PC in Chrome settings.	Our response is similar to previous quarters: The Privacy Sandbox team understands that companies would like to continue using the cookie deprecation labels. The process to extend the availability of the labels is similar to extending an origin trial. Support for the labels has been extended on several occasions. We envisage proposing further extending support for cookie deprecation labels and will share updates on blink-dev as available.

Enrollment & Attestation

No feedback received this quarter.

Show Relevant Content & Ads

Topics

Feedback Theme	Summary	Chrome Response
Opting In/Out	Will Google's confirmation that Google Search will not use a site's decision to opt-out of the Topics API as a ranking signal restrict Google from using a site's decision to opt-in to the Topics API as a ranking signal?	Our response is similar to previous quarters: The Privacy Sandbox team has not coordinated or requested from the Search organization that they use page ranking as an incentive for websites to adopt the Topics API. Google Search will not use a site's decision to support (or not support) the Topics API as a ranking signal.
Usage Observability	Requesting an observability mechanism for an SSP or general ad tech to be able to see if their implementation of the Topics API is being used on the web.	We are evaluating support for this functionality, and we welcome additional feedback from the ecosystem if this feature is a high priority.
Privacy	Questions about consent and re-identification potential.	We are currently discussing this issue here and welcome additional feedback.

Protected Audience API

Feedback Theme	Summary	Chrome Response
PA API & GAM/AdX	Google will not send any GAM/AdX demand to a publisher who wishes to rely on a rival publisher ad server. Google should enable rival publishers to choose alternative top-level PA API auction sellers to control the final auction. Information from PA API will be available	**Chrome Response:** The PA API standard is designed to be flexible and allows different parties to run the top-level auction. This choice depends on the specific implementations and capabilities offered by the publisher's ad server (whether GAM or another) and other participating companies in the ecosystem. The PA API's privacy-centric design limits granular reporting for *all* participants

	to GAM but restricted for rival SSPs. As a result, publishers are not able to compare the performance of PA API sourced demand in GAM, such as from AdX or from SSPs integrated into PA API.	consistently. The specific data *reported from* the PA API auction itself is subject to the same API-defined, privacy-preserving rules and limitations for all participants, including any SSPs. Publishers use the PA API's aggregate, privacy-preserving reports to evaluate performance. This allows assessment of the overall contribution of demand sourced via PA API and enables comparison against other demand channels, consistent with the API's privacy-by-design principles. **Response provided by Google Ad Manager:** Publishers are not required to use GAM's ad server functionality in order to access AdX demand. In addition, PA API is agnostic to who initiates an auction both in single seller and multi-seller designs.
Top Level Seller	The Top-Level Seller (TLS) has access to information that none of the other component sellers have access to, raising concerns about unequal access to information. While any entity can be the TLS, in order to access AdX demand, publishers are required to use GAM as the publisher ad server. This creates an incentive to use GAM as the publisher ad server, creating a competitive advantage for Google.	**Chrome Response:** The design of PA API does not dictate which entity can act as a TLS. The TLS role requires coordinating the auction and accessing related auction information per the API's structure. **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 PA API auctions, we intend to keep our promise and not share the bid of any auction participant with any other auction participant prior to completion of the auction in multi-seller auctions. To be clear, we won't share the price of the contextual auction with any component auction, including our own, as explained in this update. Moreover, we do not use information about component auction configurations, including signals provided by buyers to SSPs, as part of our own auction.

		Furthermore, as stated above, GAM does not require that publishers use its ad server functionality in order to access AdX demand. Finally, as noted previously in Google's Q2 / Q3 2024 report, Google's buyside platforms – Google Ads (formerly AdWords) and DV360 – do buy impressions from non-Google exchanges, including via the PA API.
PA API & GAM/AdX	It is difficult for publishers to understand activating PA API on 100% of inventory as the labelling of the option does not make the purpose clear. For SSPs, whose primary means of accessing inventory is often through a multi-level auction with GAM acting as the TLS, there is effectively no way to conduct tests or monetize via PA API without being subject to GAM.	**Chrome Response:** The PA API standard defines technical roles (like TLS and component seller) and the auction process, allowing flexibility in which platforms perform these roles. Operational activities—such as configuration, coordination, and agreements—are managed by the implementing parties (publishers, SSPs, TLS providers) to facilitate participation using the PA API framework. **Response provided by Google Ad Manager:** As described in our Help Center, Ad Manager offers publishers a control to enable testing with non-Google component sellers, such other SSPs, on 100% of a publisher's inventory where the API is available to use (overriding any sampling or throttling that GAM might apply). If a publisher enables this control, then whenever a non-Google component seller provides an auction configuration, GAM will attempt to run a top-level auction with the provided component auction included, provided that the publisher has obtained the necessary user consent to do so. GAM makes it clear to publishers that this control may impact performance, so that the publisher can make an informed decision.
Server-side vs. On-device	Server-side solutions, such as Bidding and Auction (B&A), have the potential to solve for traffic-shaping while maintaining privacy. Server-side solutions are the	Privacy Sandbox aims to support both server-side (B&A services) and on-device auction solutions, providing options to meet different ad tech needs and use cases.

	only viable path forward and Google should abandon on-device solutions.	
Auction Security	Attacks on PA API bids are fundamentally disqualifying for on-device bidding and auctions, this issue is not considered resolved by stakeholders and they continue to request technical guarantees to ensure PA API bids are not tampered with as well as an exhaustive debug mode to provide real-time incident detection and efficient debugging.	Ensuring PA API auction integrity, including mitigating potential attacks, is a key Privacy Sandbox focus. The API's design incorporates integrity measures, and we welcome further technical discussion on specific concerns. We presented and discussed a detailed list of potential attacks on PA API and our mitigations during the W3C Anti-Fraud Community Group meeting in May 2024. We welcome further discussions and feedback on what potential 'attacks on PA API bids' are of concern.
Cookieless Traffic	Will there be a way to enable PA API only on cookieless traffic for testing or other purposes?	Ad techs can identify whether 3PCs are present or not. This is explained in further detail here.
Seat ID	In regards to the Seat ID proposal, seat ID knowledge is essential for most bid requests which brings concern about tying seat ID to creative registration. Furthermore, would it apply only to the "main ad" or also to component ads?	The BuyerAndSellerReportingId proposal addresses the concern about the lack of buyer's Seat ID during creative registration for the main ad. This identifier aims to communicate the buyer's Seat ID to the seller. We are evaluating the support for component ads.
Monitoring and Reporting	Feature request for Real-Time Monitoring (RTM) for (1) sending RTM reports for cancelled auctions as well as (2) new browser-populated buckets to make clear what kind of cancellation happened.	RTM does not appear to be a suitable solution for investigating participation rate. RTM is designed, as a low latency monitoring API, to catch critical, sudden, temporary outages. In contrast, participation rate does not require low latency reporting and is not a critical, sudden temporary outage. Concerns about participation rates are most effectively answered by the sellers with whom buyers collaborate, and not by buyers investigating via the browser. Moreover, as cancelled auctions are extremely common, if the browser would generate RTM reports from each cancelled auction, it could

		drown out RTM reports for actual outages.
Documentation Clarification	Report of a documentation discrepancy in the PA API explainer that states that the nonce should be a UUID string, but it actually returns a promise.	A clarification is proposed here.
Frozen Context	When working with frozen-context, what options are available to address issues and challenges related to (1) bundling, (2) external libraries, and (3) unsupported data types?	We have provided a response to this question here.
Specs	The Private Aggregation API added a generic contributeToHistogramOnEvent operation. As a consequence, the definition in PA API became an overloaded operation, and Web IDL operations "must not be overloaded across interface, partial interface [...]", so that definition is now invalid.	This issue points out a temporary inconsistency between the PA API and Private Aggregation specs while we merge similar changes in both. We have merged a pull request to address this.
Interest Groups	Request for guidance on the recommended and resource-efficient method for ending an Interest Group's (IG's) bidding participation when a campaign stops.	Here are some suggestions we can provide: We believe the lowest latency, least permanent, but also least resource releasing mechanism is using the real-time bidding signals to inform their `generateBid()` to stop bidding. The second option that uses fewer resources would be setting a negative priority for that IG in the real-time bidding signals response, as this would stop `generateBid()` from even getting invoked. The third option, that uses even fewer resources, would be removing the ads from the IG. IGs without ads don't have their `generateBid()` invoked.

		The fourth option, that uses even fewer resources, would be removing the `biddingLogicURL` from the IG. At this point the IG can still be updated/rejoined so as to reactivate it. Further options revolve around leaving the IG, either via `leaveAdInterestGroup()` or `clearOriginJoinedAdInterestGroups()` or via the IG expiring. As highlighted above, different options have different latency implications and resource consumption. Ad techs can pick the option that has the best tradeoff for their specific use cases.
Audiences	Request for a mechanism to run logical operations on audiences built (e.g. ability to target an intersection of IG A & B)	With PA API, running logical operations on audiences from the same site is achievable today. Logical operations of audiences across different sites are not supported today for privacy considerations as explained in our privacy model. We are continuing to conduct research in this area and will share any updates along the way.
Feature Request	Proposal to remove restriction on additional bids requiring the TLS to be known in advance.	We are currently discussing this proposal here and welcome additional feedback.
Updated approach to 3PCs on Chrome	Will Privacy Sandbox APIs such as PA API remain generally available to all Chrome Stable users, or would the APIs (or a subset of APIs) only be available to users who have declined 3PCs?	We do not intend for a user's decision to decline 3PCs to have an impact on the availability of the Privacy Sandbox APIs in Chrome Stable.
Enhanced Signaling	Are there any plans to add functionality that indicates whether the TLS intends to run a PA API auction?	We are evaluating support for this functionality. We will share further details on timing when available and we welcome additional feedback on this request.
Deal ID	Concern that the KV server requirement in the Deal ID proposal may be an	The Deal ID proposal allows SSPs to query metadata of the selected deal IDs from the key-value server during PA auctions, so that

	expensive and time-consuming server-side process.	they don't need to preload all deal-related metadata onto the device. This proposal is being developed in response to requests from SSPs, and we welcome additional ecosystem feedback here. We understand that there's work required to set up the key-value server, but overall still think this is a net benefit for ad tech companies. We continue to welcome feedback and suggestions on making this process easier.
Cross-IG Frequency Capping	Request for cross-IG frequency capping via PA API.	Cross-IG frequency capping has challenging privacy characteristics that we've been unable to find solutions for. We welcome additional feedback from the ecosystem if this feature is a high priority.
Deal IDs & Seat IDs Reporting	Requesting ability to get deal or seat IDs into aggregate reporting.	The reporting ID functionalities we are working on here will make the reporting of deal and seat IDs possible. selectedBuyerAndSellerReportingId is provided to reportResult(), so the easiest way to report it would be via event-level reporting (i.e. encoding the Deal ID into the URL passed to sendReportTo()). If aggregated reporting were to be used, that can also be done. The reporting ID feature is currently live for 10% of Chrome Stable channel traffic. We are evaluating expanding the launch to 100%.
Interest Groups	Use the same order of priority in both IG selection and evaluation and use that order of priority in all evaluation modes.	We are currently discussing this here and welcome additional feedback.
Interest Groups	Suggestion to use audience activation and delegation as ways to increase Privacy Sandbox API adoption.	We are aware of this request from multiple stakeholders and are researching a solution. We welcome additional feedback from the ecosystem.
Interest Groups	Challenges around creating PA API IGs, specifically	We have received the request to support more advanced IG delegations from multiple

	around delegation and ownership when acting for multiple buys or on behalf of publishers.	stakeholders, and we see the added value of SSPs contributing to this process. We are conducting research to find the best solution that allows different parties to participate in the audience extension process. We welcome additional feedback from the ecosystem.
Client-side Performance	Request for guidance on easing client-side caching of trustedBiddingSignals to optimize infracost and latency.	We are currently discussing this here and welcome additional feedback.

Protected Auction (B&A Services)

Feedback Theme	Summary	Chrome Response
K/V Services	How are requests from the browser to the seller's KV server batched? For a seller, what will the request from the browser look like - a GET or POST request? Additionally some clarification is needed around k-anonymity requirements.	For v1, Chrome sends a GET request to the Seller's KV service to fetch `trustedScoringSignalsURL` with the signals in the query parameters of the request. The parameters would include the `hostname`, `renderUrls`, `adComponentRenderUrls`, and `experimentGroupId`. We are currently experimenting with some extensions for sending additional information for creative scanning, but that has not yet launched. When setting `maxTrustedScoringSignalsURLLength` to 0 then Chrome could potentially batch all of the signals into a single request (possibly exceeding any URL length limit on their server), but it's not guaranteed. Chrome currently chooses to include requests in the same batch if they are ready to be sent within 10ms of each other, though we are currently investigating how to optimize this. When working with trustedScoringSignals, it's useful to remember that Chrome respects caching headers. Headers like the `Stale-While-Revalidate` "Cache-Control" header could reduce the average latency by

		allowing Chrome to use the cached copy (and update the cache for the next auction), effectively removing the signals fetch from the critical path. Finally, regarding k-anonymity, the particular section of the explainer seems to be outdated. Originally we were going to require the trusted signals URLs to be k-anonymous, but that requirement was dropped. We will remove this sentence from the explainer.
B&A Services	Upgrading to the latest version of B&A takes a long time. Faster build times or pre-built images would be beneficial.	Ad techs can build the binaries on their own and validate using the provided hashes. We will consider investigating the possibility of providing pre-built artifacts or improving build times in the future.
API Feature Request	Request for macOS compatibility for Bidding & Auction Services (B&A) build scripts, container images, and invocation tools to facilitate local development and testing.	We currently support amd64 which is sufficient for deployment to the supported cloud platforms (GCP & AWS). We may investigate support for other architectures in the future.
AWS	Is having IAM roles created a requirement for production builds?	Yes, IAM roles are required for proper permissions and communication with Coordinators. The keys are used to decrypt the ProtectedAudienceInput ciphertext that is generated on device as set out here. Additionally, these roles are required to pass server/TEE attestation of production builds with those same Coordinators. This is addressed in further detail in our self-serve guide.
B&A Flags	Requesting definitions of available B&A flags to be listed in documentation given that today these definitions reside in the Terraform code, cc files and proto files but ad techs would benefit from documentation on these flags leveraging it as a source of truth for understanding how to	We are investigating the possibility of documenting the Terraform flags descriptions and welcome additional feedback here.

	customize deployments.	
AWS Bidding Service	Seeking guidance regarding bidding service on AWS and default logging behavior and configuration.	For debugging your bidding services within the TEE (such as Bidding service), we recommend using Ad Tech consented debugging. This allows you to enable detailed logging and capture request/response data for your specific test requests directly from your client to help with debugging.
TEE K/V Documentation	Requesting clarification regarding the beginning of TKV enforcement as stated on the dev site.	We will provide sufficient notice in advance of requiring the use of TEEs. Until then, you can continue to use your own server for real-time key/value signals.
B&A Testing & Analysis	B&A analysis and testing remains costly and does not seem production-ready.	We'd need more information on the cost analysis and the factors leading to the assessment of production-readiness in order to look into it further.
Trusted Server Optimization	Proposal to merge parameters specific to component sellers into one *inputsPerSeller* parameter, using a JSON string for its value.	We are discussing this proposal and welcome additional feedback here.
Security	How are security risks from TKV mitigated by using B&A?	Preventing external calls to TKV is possible. This is fully supported and configurable on GCP today. For AWS, additional support needs to be developed due to the deprecation of AWS App Mesh, which previously enabled this. We welcome additional feedback here.
B&A Services	Requesting clarity on the narrative/comms regarding the value of HTTP Streaming for B&A optimization.	Privacy Sandbox supports streaming capabilities in transferring B&A data to improve latency for ad techs who choose to use it. It is optional performance optimization in case of mixed mode.
Prebid	Request for updates on contributing to the open source Prebid library to enable PA API B&A features for the ecosystem.	In March 2025, Chrome launched the Prebid-preferred optimization in stable as documented in the B&A public roadmap (*see* March 2025).

Traffic Shaping	Request for mechanisms to log contextual signals received by B&A to better understand when IGs are being activated and improve their "intent to bid" logic in contextual response. This enables better usage of network resources to avoid "useless traffic" (a.k.a. traffic shaping).	We are currently discussing a proposal here and welcome additional feedback.
Documentation Clarification	Clarification needed regarding 'Service/Vsock proxy is not reachable' error spotted at B&A test integration setup.	This is due to minimum memory requirements.The AWS configuration explainer has been updated to reflect this requirement.

Measuring Digital Ads

Attribution Reporting (and other APIs)

Feedback Theme	**Summary**	**Chrome Response**
Real-Time Data	The lack of real-time data impacts everyone in the industry. Delaying real-time data is a serious problem for advertisers, buyers move to platforms that have Google Analytics as it is the only place they can get proof of reaching audiences.	The real-time data delays that are part of the Attribution Reporting API (ARA) are implemented as privacy-protection mechanisms to reduce the ability of ad techs to use event-level reports to track users across sites. However, ARA provides flexibility in how attribution reports are delivered, by allowing event-level reports to have a minimum report window of 1 hour and by allowing Aggregate Reports to have an option of being sent instantly to ad techs with no delay.
API Usage	Request for confirmation regarding the correct configuration for a Cross Web App attribution flow, specifically when operating web-to-web and web-to-app attribution in parallel.	When running web-to-web and web-to-app campaigns in parallel, the ad tech should choose only one platform to register each source or trigger, in order to prevent double counting. We strongly recommend using the Operating System (OS) where possible, as the OS has the ability to perform both web-to-web and web-to-app attribution, as long as the web sources and triggers have been correctly delegated. This would mean responding with

		the Attribution-Reporting-Register-OS-Source header for sources and Attribution-Reporting-Register-OS-Trigger header for triggers. The Attribution-Reporting-Support header can be used to identify whether there is Chrome and/or Android-level support. The Attribution-Reporting-Info header is useful when there is no Attribution-Reporting-Support header in the request, in which case the browser will make the platform registration decision based on the availability of the platform support on the user's device.
API Spec	Seeking clarification about the Attribution-Reporting-Support HTTP request header set by the Attribution Reporting API and whether it is intended for the header to contain both web and os keys, regardless of the platform.	The Attribution-Reporting-Support header is subject to the browser adding "GREASE" parameters, to ensure that servers use a spec-compliant structured header parser. For this header, only structured-dictionary keys should be interpreted. The values and parameters are currently unused. See here for an example.
3PC-based reporting	Requesting guidance on how to troubleshoot discrepancies in measurement between ARA and 3PC in ads campaigns.	ARA supports two types of debug reports that can be used to troubleshoot and debug discrepancies. Attribution-success debug reports can be used to easily compare ARA results against results from other measurement technologies, and Verbose debug reports can be used to receive more information and troubleshoot potential issues in the attribution registrations.
API Usage	While testing ARA certain issues were discovered: insufficient granular reporting leading to noisy data and inflexible campaign optimization, high thresholds excluding smaller advertisers, and difficulty comparing campaigns due to inconsistent Key Performance Indicators.	ARA provides flexibility by providing multiple parameters that ad techs can customize to achieve their specific measurement use cases. Event-Level Reports support flexible event-level reporting which allows ad techs to customize their reporting windows, the number of reports they can receive, and the trigger data they want to measure, which can change the impact of noise on their data and allow them to achieve different use cases. Similarly, Aggregate Reports have different ways ad techs can customize their configurations such as the number of dimensions they track, their batching frequency,

		and their use of contribution budget to change the impact of noise and achieve different use cases as well.
API Spec	Question about the dependency of ARA on 3PCs, specifically regarding whether it remains in a testing phase requiring these 3PCs.	ARA is enabled independent of 3PCs, but 3PCs need to be enabled to allow ARA transitional debug reporting to compare ARA results with cookie-based attribution results.
API Usage	Inquiry about registering sources for app-to-web attribution on older Android versions (11, 12, and 13) using ARA.	ARA is currently supported on Android S and above (12+).
API Usage	Request for ARA opt-in rates and distribution details.	Our response is unchanged from previous quarters: “We have no plans to share this information with the ecosystem. Developers are welcome to call the APIs where they have code deployed today to estimate availability of the Privacy Sandbox APIs”
API Availability	When ARA is enabled, are 3PCs enabled or disabled?	When ARA is enabled on the users’ browser, it does not have any effect on the users’ cookie settings. It is possible for ARA to be enabled and for the user to have cookies either enabled or disabled.
Reporting	Is there a predefined list of values we can receive in the "Attribution-reporting-support" header?	As set out in our guidance, the value is a structured header dictionary, whose only currently defined semantics is the presence or absence of the OS and web keys. All other parts of the header should be ignored. In other words, parsing requires using a structured header parser, not simple string matching.

Aggregation Service

Feedback Theme	**Summary**	**Chrome Response**
Feature Request	Feature requests for Aggregation Service:	We are evaluating these requests and will share further details when available.

	Server-to-Server integrations, Cross-device measurement, Ease multi-touch attribution and contribution reporting, omnichannel attribution, and support for advanced ML optimization loops (e.g., Private Model Training).	We welcome additional feedback from the ecosystem on whether these requests are a priority.
Feature Request	Request to set the EBS delete_on_termination parameter to True in the terraform environment, in order to mitigate concerns about the reset when updating the aggregation serviceset.	We are evaluating this request and will share further details when available. We welcome additional feedback from the ecosystem on whether this request is a priority here.
Documentation Clarification	Requesting guidance about what can be changed (e.g. monitoring thresholds) and what should stay untouched.	We are evaluating publishing additional documentation and guidance on the available customizations for the aggregation service.
Deployment	Request for clarification regarding new deployment failing at bazel command.	Deployment failing can happen due to the bazel version used in the environment. Documentation will be adjusted to cover debugging on Terraform failures as well as indicating the required bazel version.

Private Aggregation API

Feedback Theme	Summary	Chrome Response
API Usage	Request for guidance on some implementation challenges such as potential data loss due to reported Shared Storage limitations, difficulties with high cardinality requiring complex Aggregation Service allowlists (wildcard suggested), and slowed testing caused by the Aggregation Service's "no	Concerning the Shared Storage limitations, the 20 contributions limit (detailed here) is per execution, not per month. Additionally, API callers can override this limit. The limit is in place to help manage the cost of processing reports in the aggregation service and not to limit the reporting utility. Concerning wildcard queries, we are evaluating this request and will share further details when available.

	duplicates" rule.	Concerning the “no duplicates” rule, in order to enable testing, we temporarily support debug mode for the purpose of bypassing this rule. This is set out here in more detail.
Filtering ID & Buckets	Is it possible to request to the aggregation service the same bucket with two different filtering IDs in two separate aggregation runs, i.e., can the filtering ID act as a supplementary partitioning of domains?	Yes, this feature is supported. When performing an aggregation, only contributions with a filtering ID matching the list in the job parameters will be processed, and the rest will remain available to process in separate run(s).
Multi-touch attribution	Requests for clarification regarding Multi-Touch Attribution (MTA) implementation: 1) Is there a limit to the number of contributions if the aggregation value does not exceed 2^16? 2) Is there a limit to the number of unique aggregation keys (buckets) that can be stored for a given context? 3) How does the Aggregation Service process summary reports when each user agent (browser) has a unique aggregation key, as is likely in MTA?	1) We have put in place default contribution limits, but there are options for the API caller to override them as explained here. The purpose of the limits is to help API callers manage the cost of processing reports in the aggregation service. 2) There is no such limit, although ad techs should consider the granularity of the aggregation keys to improve signal-to-noise ratio, as further explained here. 3) Please see this guidance, especially the signal-to-noise guidance addressed above under item 2).

Limit Covert Tracking

User-Agent Reduction/User-Agent Client Hints

Feedback Theme	Summary	Chrome Response
Feature Request	Request to add Sec-CH-UA-Robot to User-Agent Client Hints (UA-CH) as it would allow servers to identify automated traffic for content adaptation, security, and analytics.	This is an important use case that is being discussed in other standards groups (see here for further details), and we would recommend interested parties to participate by providing their feedback. However, we consider that UA-CH might not be the appropriate solution, given that HTTP request headers can be easily manipulated by automated traffic.

IP Protection (formerly Gnatcatcher)

Feedback Theme	Summary	Chrome Response
IP Address Privacy	Leaving IP addresses available for Google to use contradicts its stated privacy goals. Even though Google says that it anonymises data through IP Protection, users must be logged in to Chrome to use IP Protection, so Google still learns their identities.	The reasons for login are for anti-fraud and abuse purposes, primarily rate-limiting access to the proxies. Furthermore, to protect users' privacy in the context of the authentication requirement, our token design is blind-signed meaning the token issued during login is different from the token that is used during the proxying therefore the tokens issued cannot be linked to a user's Google identity later on. This means Google does not know who the user is when that user's traffic is proxied in incognito mode, despite the authentication requirement for anti-fraud reasons.
IP Address Privacy	The use of IPs is a step in the wrong direction. They cannot be deleted from the browser, like cookies, and users don't have the same transparency controls as they do with cookies. If cookies go away, the industry will move to using IPs as an alternative solution, prioritising self-preservation over	As a platform, Chrome aims to provide users with features that improve their browsing experience on the web. For Chrome users who choose to browse in Incognito, that means providing enhanced protections against cross-site tracking by limiting the availability of IP address information in third-party contexts.

	privacy.	
Masked Domain List	What is the selection criteria on the Masked Domain List (MDL)?	Chrome developed criteria to identify which domains should be on the MDL and therefore receive masked IP addresses in a third-party context. Google has partnered with Disconnect.me, a prominent internet privacy leader who also collaborates with other web browsers. Chrome will leverage Disconnect.me to identify domains that align with Chrome's established criteria. Additionally, Chrome has developed a methodology to identify widely used JavaScript functions that provide consistent outputs from stable and high-entropy web APIs and can therefore be used to construct high entropy probabilistic identifiers. These functions are then detected when they are loaded on websites in a third-party context, resulting in a list of domains that serve scripts with these characteristics that become part of the MDL and are therefore proxied. The detection pipeline that looks for these patterns of API misuse considers all domains, including Google's own domains.
Fraud Prevention	Feedback on Probabilistic Reveal Tokens (PRTs) that the proposed 24-hr reveal delay and reveal rates impede real-time fraud detection. Request for shorter delays (1-hr delay) and higher rates (at least double-digits). Further suggestions involve enabling differential rates based on risk signals (VPNs, automated browsers), and allowing targeted reveals of specific tokens.	Most developers we talked to provide hourly reporting to their customers, and several update IP blocklists throughout the day. A shorter delay period enables more frequent updates, and under an hour, would re-enable IVT measurement in hourly stats, but it also potentially increases the likelihood of re-identifiability of users. We are open to exploring reducing the delay periods and changing the reveal rate based on ecosystem studies, and feedback from stakeholders and welcome additional feedback here.
Masked Domain List	Question regarding domain's inclusion on the MDL despite not having an advertising use case. Concern that this could enable "IP-bridging" to create profiles based on IP addresses.	We recognize the importance of implementing an appeals process for our list-based approach. Appeals permit companies to make a claim that their domain on the MDL does not meet the inclusion criteria and ought to be removed, thereby allowing that domain to continue to receive users' original IP addresses in a third-party context in Incognito mode.

		We have now launched the appeals process to provide domain owners sufficient time to seek an appeal and receive a decision prior to the launch of IP Protection in Incognito mode in Chrome Stable. Further details regarding the appeals process are available here.
Masked Domain List	Feedback that publishers are investigating the implications of their partners being included in the MDL. They were reassured by the GeoIP provisions within the IP Protection Explainer.	Chrome recognizes the importance of supporting geo-based use cases. The proxy will assign IP addresses that represent the user's coarse location, including country. Further information is available in the IP Geolocation Explainer.
Masked Domain List	Question regarding the MDL whether or not country-level targeting is still available.	Chrome recognizes the importance of supporting geo-based use cases. The proxy will assign IP addresses that represent the user's coarse location, including country. Further information is available in the IP Geolocation Explainer.
Fraud Detection	Concerns about impact of IP Protection on fraud detection systems. Will users see proxy IPs or a header? Will SSPs and DSPs see the same proxy IP address for a given use? Inconsistencies could affect fraud detection and OpenRTB.	Users browsing in Incognito mode with IP Protection enabled that make requests to domains on the MDL will receive a proxy IP address based on a defined geofeed. Organisations may request PRTs to be passed as an additional header on proxied traffic, where a small sample of original IPs can be revealed after a delay period. We suspect many SSPs will pass their proxied IP address in server-side bid requests to their demand partners, but winning DSPs are not guaranteed to see the same proxy IP address at impression time.
Fraud Detection	Questions about the update frequency of the IP geolocation file, the update timing for details on reporting fraudulent behavior and PRTs, and how ad tech should detect fraudulent activities.	The PRTs explainer is live, as is the list of proxy IP addresses and their mapped geo regions. We recommend periodically checking this file for updates and changes, as IP addresses will rotate over time. The public email address to report abuse will be announced closer to launch.

Geolocation	Request for public list of IP addresses used for proxies.	The file mapping IP addresses to rough locations for IP Protection is available here. Please note that this file is updated periodically.
API Usage	Assertion that IP Protection seems to be on by default and users are not given the option of opting out.	IP Protection will be available for users in Chrome's Incognito mode, on Android and Desktop platforms. Users will have the ability to disable IP Protection. For enterprise-managed versions of Chrome, IP Protection can be enabled, but it will be off by default.
API Usage	Query regarding the availability of an experiment flag to enable and test IP Protection in Chrome Canary and Beta releases.	Currently, we do not have an experiment flag available to test the full IP Protection feature. The functional experiments we are conducting only proxy traffic going to Google domains.
IP Address Privacy	How do 3PC prompt settings work when a browser moves into Incognito mode?	3PCs are blocked by default in Incognito mode.
Incognito Mode	Seeking clarification on whether IP Protection functions in Incognito mode when the user is not signed into Chrome.	IP Protection is not active if the user has not logged in to Chrome ahead of launching Incognito mode. The reasons for this are for anti-fraud and abuse purposes, namely rate-limiting access to the proxies. IP Protection will use client authentication to limit the ability of bad actors to leverage the proxies to amplify attacks on services on the MDL. Therefore, IP Protection will only be available to users that have been authenticated using the Google account they're signed in with in the Chrome browser prior to opening a new Incognito window.
Incognito Mode	Requests to assess impact of IP Protection ahead of launch, including: (1) Proposal to use a browser state flag or aggregate API reporting to quantify Incognito mode usage; (2) Sending an IP Protection header for a period before enabling the feature; and (3) Shipping the feature to a small, known percentage of traffic for extrapolation.	We understand the ecosystem's interest in being able to understand and measure the scale and impact of IP Protection. However, Chrome works towards making a user's choice to browse in Incognito mode private. Chrome does not expose a method to detect users browsing Incognito, and has taken steps to limit other signals that may reveal the user's browsing mode. We are considering ways to facilitate this testing without impacting the privacy of users browsing

		in Incognito mode and welcome additional feedback from the ecosystem.

Bounce Tracking Mitigations

Feedback Theme	Summary	Chrome Response
Compliance	Google's unwillingness to authorise use of the Bounce Tracking Mitigations (BTM) technique that is compliant with data protection legislation has no legal basis and renders the Privacy Sandbox appeals process meaningless.	As we explained in our previous feedback report, compliance status has no relation to the application of BTM and Google does not make any decisions regarding compliance in implementing BTM. BTM, like other Chrome privacy protections, is instead focused on furthering users' control over whether and how their data is shared. The third-party managed appeals process referenced in the CMA's Q2/Q3 Report is specific to areas where Google is making decisions about individual companies' inclusion or exclusion in lists.
Compliance	Discussion about how browsers ensure compliance with legally consented actions in the context of GDPR highlighting scenarios where browsers might suppress actions (like redirects or cookie setting) that users have explicitly consented to, creating a conflict between legal consent and browser privacy settings.	The browser does not have visibility into the nature of the relationship between a user and a website. Additionally, with current BTM behavior, there already exist workarounds for a user to give explicit consent to bounce tracking from a given site. Further information regarding compliance is available in our Privacy-related compliance FAQ.
Dual-Use Sites	Seeking clarification on whether transitions from WebView or app-to-web (Chrome) will be considered "dual-use sites" under BTM?	The browser does not have visibility into whether a bounce chain began via a transition from WebView or app. Hence, BTM does not give those flows any special treatment. Instead, it interprets the flow as a cross-site bounce beginning from "about:blank" and proceeds with standard behavior.

Strengthen cross-site privacy boundaries

Related Website Sets (formerly First-Party Sets)

Feedback Theme	Summary	Chrome Response
API Usage	Concerns about potential for abuse of RWS in conjunction with IP Protection. Exposing IP addresses to organizations within an RWS set could incentivize organizations to join multiple RWS sets to gain access to portable IP Address data for tracking Incognito users.	The set requirements for associated sites, service sites, and sets as a whole, enforced by automated validations, mitigate any potential incentive to attempt joining multiple sets. Joining user activity across sets via IP addresses would require inclusion of an MDL domain in a set, which requires coordination between the set owner and the domain owner. This same risk applies for single sites (i.e. no RWS involved) coordinating with MDL domains. We have responded to this question in further detail here.

Fenced Frames API

Feedback Theme	Summary	Chrome Response
Native Advertising	Feedback that Fenced Frames, as currently designed, is incompatible with their native advertising business model, which requires ads to flexibly adapt to surrounding content.	We continue our assessment of the ecosystem needs and the current Fenced Frames offering. In any case, as previously stated, Fenced Frames will be required no sooner than 2026.

Shared Storage API

Feedback Theme	Summary	Chrome Response
API Bug	Report that Chrome logs an error when the Shared Storage API's budgeting mechanism prevents the selectURL operation from running, even though this is expected behavior. Request	The change has been implemented and included in Chrome M134, available since 4 March 2025.

	that Chrome downgrade the logging level from error to warning or info, as the error is not actionable for the caller.	

CHIPS

Feedback Theme	Summary	Chrome Response
API Documentation	Clarification needed regarding the security protections offered by partitioned cookies compared to SameSite=Lax/Strict cookies. Suggestion that the documentation should explicitly state that partitioned cookies do not provide the same level of protection against XSS and CSRF attacks as SameSite=Lax/Strict cookies.	We will update the explainer and specification to clarify the semantics and protections offered by partitioned cookies.

FedCM

Feedback Theme	Summary	Chrome Response
UI & Security	Feedback that the FedCM UI is too similar to Google's previous one-tap login, it's hard to quantify FedCM performance due to lack of passive presentation tracking, and a recommendation for stronger documentation language regarding PKCE.	We are actively engaging with stakeholders to address their feedback. Areas of ongoing discussion include ways to provide better metrics to IdPs to allow them to track FedCM performance, and possible enhancements to address new use cases for FedCM around subscription use cases.
API Usage	When a user refreshes the page and calls navigator.credentials.get to login, a pop-up window appears, requiring the user	RPs can use their own cookies to store the token. RPs can then check their own cookies to determine if a user is logged in before invoking navigator.credentials.get. We have addressed this in further detail here.

	to click to continue, which introduces a delay impacting user experience. Could Relying Parties (RPs) cache the token returned by navigator.credentials.get to improve user experience?	
Multi-IdP Selection	How would the browser display the login options for multiple identity providers (IdPs) in FedCM?	The developer documentation has information on how multiple IdPs would be displayed. Stakeholders can experiment with this functionality by enabling the fedcm-multi-idp flag in chrome://flags.
Browsers & IdPs	Is it possible for a browser, such as Chrome, to act as an IdP itself? Browsers could use their stored account and profile data as a trusted source of authentication.	Due to the fact that browsers can be modified (e.g. via extensions), any claims of email verification made directly by the browser cannot be trusted without additional server-based verification. As such, a purely-client-based solution is not recommended. We have discussed this issue in further detail here.
API Spec	Discussion around whether the parameter for the IdentityCredential.disconnect() algorithm should be required or optional.	This is now fixed. More details can be found here.
API Security	Concerns around token leakage in FedCM login process if a RP has an XSS vulnerability. An Attacker could execute navigator.credentials.get in malicious code to obtain the token.	FedCM does not create new XSS risks; these risks are inherent in web applications and existing auth protocols. To mitigate these risks, RPs should verify the aud claim in ID tokens and only accept assertions issued in their own origin. As discussed here, there are widely established best practices to secure this token exchange that exist today and are available for use with FedCM. Additionally, the Storage Access API can be used with FedCM, and Storage Access API calls are automatically granted when there's a prior FedCM call. This should enable the embedded redirect flow discussed on the GitHub issue.

API Spec	The client_metadata_endpoint is a required field in the config endpoint response for FedCM. An empty object is a valid response, and Chromium silently ignores a 404 response, suggesting that the endpoint is treated as optional in practice.	We agree that the specification could be changed to reflect this and make the client_metadata_endpoint an optional field.
API Usage	Concerns regarding the difficulty of testing FedCM implementations due to browser-controlled user interfaces that are not accessible through the DOM.	We support the browser automation APIs for regression testing, which may address these concerns. These APIs are documented here.
API Spec	The login_url parameter, which is a required part of the response of the config endpoint, was not documented in Section 3.2 of the specification.	We have submitted an update to the documentation to include the login_url parameter in Section 3.2.
API spec	Concern around a potential tracking vector in FedCM. An IdP could insert IDs as path parameters into the endpoints specified in the config endpoint response (accounts_endpoint, client_metadata_endpoint) and use these IDs to correlate the account and client metadata requests.	While we do not have evidence of IdPs inserting IDs into these endpoints, we are actively considering mitigations to address this issue here.

Fight spam and fraud

Private State Token API (and other APIs)

No feedback received this quarter.

Google Ads Roadmap for Effectiveness Testing of the Privacy Sandbox Proposals

Google Ads is engaged in integration and testing of the APIs and providing feedback to the CMA and the ecosystem. Google is conscious of the importance of transparency for the ecosystem, so that they can plan their investments and forecast participation in future tests, and as such has included Google Ads' testing updates below:

Chrome-facilitated testing:

- On March 28, 2025, Google Ads published Google Search and YouTube Ads Measurement testing results without 3PCs. The results are available here.

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 CMA has not notified Google of 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.

Stakeholder concerns

Competition Feedback – The CMA has shared stakeholder feedback that Google's behaviour in standard-setting organizations is an abuse of dominance, as Google is using its influence to develop proposals that could potentially harm competition. In line with the Commitments, Google takes into consideration a wide range of stakeholder feedback when making decisions regarding Privacy Sandbox and to this end actively participates in standard-setting organizations. In addition to the W3C, the Internet Engineering Task Force 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. Google's collaboration with the web standard community allows for industry experts of all kinds to guide the designs of Google's Privacy Sandbox proposals. These forums are open to anyone who wants to actively participate in the design and development of the technologies. Google's long-term goal remains to create interoperable standards that multiple browsers broadly support and that provide effective, privacy-enhancing solutions for targeting and measurement use cases.

The CMA shared stakeholder feedback that Google's designs for Privacy Sandbox have not made sufficient progress towards widespread implementation and adoption and that Google's efforts to comply with antitrust laws have shifted the burden to its competitors, requiring dedication of significant resources without progress. The stakeholder considers that there is a disconnect between the current state of the Privacy Sandbox APIs and Google's stated mission 'not to harm the open internet', and that, despite years of work with the industry, Google remains in the requirements gathering phase, with gaps still unaddressed. If Google intends to release these APIs while in the design stage then 'iterate' with the industry, the result of that interim iteration period could potentially harm the ad tech ecosystem.

Google has been actively engaging with the ecosystem and regulators to develop the Privacy Sandbox APIs and to ensure that the Privacy Sandbox tools are designed and implemented in such a way that maximizes utility while preserving privacy, and to ensure Google's continued compliance with competition and privacy laws. As with any new technology, each company is responsible for ensuring that its use of the Privacy Sandbox complies with the law. The relevance and measurement APIs have been generally available in Chrome since 2023 as announced in our blog post Shipping the Privacy Sandbox relevance and measurement APIs. Google has dedicated substantial efforts and resources to encourage testing of the APIs, including through collaborating with the CMA to publish guidance for testers and making 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. Ecosystem participants are not required to adopt the Privacy Sandbox APIs and may choose to adopt alternative privacy-preserving technologies. We welcome efforts to use the Privacy Sandbox APIs alongside other, non-Google privacy-preserving technologies to evolve existing solutions and create new ones.

The CMA has shared stakeholder feedback that Google's announcement in July 2024 was not sufficiently clear and led to competitors incurring further costs. In April 2025, Google published a blog post on Next steps for Privacy Sandbox and tracking protections on Chrome, announcing that Google has made a decision to maintain the current approach to offering users third-party cookies in Chrome, and will not be rolling out a new standalone prompt for third-party cookies. Google is continuing to discuss the Privacy Sandbox project with regulators. We look forward to continuing to collaborate with the ecosystem on this project and we will share updates as they become available.

The CMA shared feedback from a stakeholder that Google should also introduce the new user choice mechanism on its owned and operated ("O&O") properties to incentivise Google to design the Privacy Sandbox proposals in an effective way. As explained above, Google announced in April 2025 that it will no longer introduce the new user choice mechanism. Regardless, Google's O&O properties are already – and will continue to be – subject to the same rules as third parties.

The CMA shared feedback from a stakeholder that Google has not yet provided a timeline for when its own SSP or DSP would shift to using its Privacy Sandbox technologies, which raises doubts as to why any competitors should continue testing a solution that Google itself does not consider fully ready for its own systems. In addition, without a guarantee that Google Ads will operate using only Privacy Sandbox technologies, there is a risk that Google will not fully utilize the technologies. Google has committed to design and implement the Privacy Sandbox in a way that does not distort competition by self-preferencing Google's own business, and to take into account impact on competition in digital advertising and on publishers and advertisers, regardless of their size. As with any ecosystem participant, Google Ads is not obliged to use the Privacy Sandbox APIs, and to the extent that Google Ads chooses to make use of the Privacy Sandbox APIs, it will be subject to the same conditions as third parties.

Testing – The CMA shared feedback from a stakeholder that Google should provide Service Level Agreements and warrants associated with its proposed Privacy Sandbox Ad Systems to ensure Google invests in the server infrastructure required to keep their solution fit for purpose. Google has invested significant resources in the development and testing of the Privacy Sandbox technologies, including the server infrastructure, and will continue to engage in future innovation in collaboration with the ecosystem.

TEEs – The CMA shared feedback from a stakeholder that Google's lack of guarantees for private cloud TEEs, or lack of development of a program to authorize private cloud TEEs in Chrome, raises competition concerns. We continue researching potential approaches to secure the privacy of Chrome users in an On-Premise TEE. We welcome feedback from the ecosystem, in order to collaborate and refine any possible solutions.

IP Protection – The CMA shared feedback from a stakeholder that Google has restricted IP addresses, URLs and User-Agent string data, as well as 3PCs, which are the four key data components used by websites to offer users services worldwide, and that ad tech software engineers use to create publishing and advertising technology. Therefore, Google has allegedly increased the value of Google Ads and limited innovation. As noted above, Google has taken a decision to maintain the current approach to 3PCs on Chrome. Aside from 3PCs, there are numerous signals and technologies that enable effective targeting and measurement of online advertising, including solutions that facilitate cross-site tracking independent of 3PCs. Third parties have developed solutions based on signals such as publisher-provided information and contextual information. Information available through the User-Agent string continues to be available. The only difference is that some of this information is accessed through UA-CH, rather than from the User-Agent string directly. Ultimately, there is ample opportunity for developers to build privacy-enhancing technology solutions for cross-domain and cross-device targeting and measurement on top of the building blocks we're offering as well as non-Privacy Sandbox building blocks.

Customer Match – The CMA shared stakeholder feedback that Customer Match uses covert tracking methods to exchange personal data across organisations, and Google has only given guarantees that it will not use browsing history data. However this does not cover real-time browsing data, authentication data from Google's Account Data and other information that Chrome sends back to Google, such as x-client-data. This stakeholder feedback misstates how Customer Match works. First, Customer Match allows advertisers to upload their online and offline first-party data to Customer Match to reach and re-engage with their (potential) customers across different inventories. As such, Customer Match does not use covert tracking methods to exchange personal data across organisations: it uses data provided by third-party advertisers upon their request for remarketing purposes. Second, as to the scope of the data commitments, as explained in past reporting, we have engaged in detail with the Monitoring Trustee and Technical Expert as well as with the CMA over the course of the past three years with respect to the data covered by these commitments and the technical mechanisms to ensure that this data is not used in contravention of the Commitments.[2] The concern is therefore misplaced.

Governance – In light of Google's decision to maintain the current approach to offering users third-party cookies in Chrome and not roll out a new standalone prompt for third-party cookies, we are currently re-assessing the role of the governance framework, and considering whether any changes or updates will need to be made to our approach. We will provide updates to the ecosystem as available.

User Choice and User Experience – The CMA shared feedback from a stakeholder that Google's consent notice screens for RWS, ARA and PA API rely on 'consent sludge' as well as consent shaming, by presenting the prompt 'Got it' for PA API and ARA. According to this feedback, Google's revised prompt language for PA API, 'site-suggested ads' is misleading to Chrome users because paid ads are not 'suggestions'.

To the extent we can identify them, the surfaces referred to are intended to provide information to users and not to gather user consent, so the feedback does not seem applicable. The term "suggest" in the "Site-suggested ads" notice is used to indicate that sites can suggest related ads based on a user's activity.

The CMA shared feedback from a stakeholder according to which, in order to ensure that competitors to Google can more easily determine privacy preferences of users, the output of any dialogue choices should be sent to all ecosystem participants, rather than being retained exclusively for use by Google's Ad Systems. The stakeholder considers that this is important given Google's suggested solutions do not address all of the online users' concerns regarding retargeting. We note that all developers are able to understand whether an API is enabled or not. Additionally, the feedback appears to be based on the misconception that Google Ads has some kind of exclusive access to Privacy Sandbox API data, which is incorrect.

The CMA shared feedback from a stakeholder according to which Google is interfering with website users exercising their choices then allowing the use of cookies for websites that they choose to access and allow access to their data for, and this does not improve end user privacy. The stakeholder believes that this results in replacing or substituting end user choices with outcomes determined by Google, which would negatively impact consumers' options. The basis for this feedback seems unclear on the face of it. In any event and to clarify, Chrome has long provided users with controls over whether to enable the use of 3PCs at browser level. Users may also use Chrome settings to enable 3PCs for specific sites of their choosing. Furthermore, choices users are making on individual sites are typically related to compliance obligations of the site and not specific to 3PCs.

[2] See Google's Q1 2024 Progress Report.

Privacy Feedback – The CMA shared with Google feedback that Google's conduct is not improving privacy or user choice regarding the use of personal data for advertising, and that Google has never explicitly defined the 'privacy' it aims to improve with its Privacy Sandbox proposals. Google has published a number of materials detailing the goals of the Privacy Sandbox project, which include limiting the scope of cross-site tracking of users online, and providing the ecosystem with more privacy-conscious alternatives to existing technology. More information and resources can be found here.

The CMA has also shared feedback from a stakeholder that Google's privacy principles have not remained consistent. These changes can potentially create uncertainty in the industry and create a system in which industry participants are required to invest resources in projects that may never materialize, or risk being unprepared. Furthermore, the fact that Google can make changes to their privacy principles on short notice creates stakeholder concerns about Google's overall commitment to privacy and the health and wellbeing of the open web. The CMA has also shared stakeholder feedback that Google's December 2024 announcement that it will allow IP addresses to be used for user identification and targeting within their ad products alters its own privacy principles and underlines the industry's doubts about Google's overall commitment to privacy and the health of the open web. Google remains committed to its goal of creating technologies that both protect people's privacy online and give companies and developers tools to build thriving digital businesses. We continue to iterate with the ecosystem to maximise utility while protecting user privacy. We have set out in detail how the Privacy Sandbox APIs provide improved user privacy while enabling key advertising user cases, in our blog post on 'How Privacy Sandbox raises the bar for ads privacy'.

FedCM – The CMA has shared feedback from a stakeholder according to which Google's notices to consumers who authenticate with its Sign In with Google or FedCM do not yet provide meaningful information for consumers or choice that their consent for authentication does not extend to other uses of their personal data. As we have made clear in our API documentation and Privacy Sandbox developer guidance, when developers and sites use FedCM it is their responsibility to determine whether they need user consent for their specific use case, and how best to provide users with the relevant information about their use of personal data.

Status Meetings

The Commitments provide for Google and the CMA to schedule regular meetings at least once a month to discuss progress on the Privacy Sandbox proposals. In line with this requirement, Google and the CMA hold meetings to discuss a variety of topics relating to Privacy Sandbox and Google's Commitments to the CMA, including technical, legal and procedural issues to assist the CMA in carrying out the regulatory scrutiny and oversight foreseen in the Commitments. Google and the CMA collaborate on the agendas for each meeting to ensure that adequate attention is given to each topic.

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 applicable at this time, as Google has not entered the Standstill Period.

Compliance statement

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

[redacted]

COMPETITION AND MARKETS AUTHORITY
Case 50972 - Privacy Sandbox
Compliance Statement

I, Renée M. DuPree, Director, Competition Compliance of Google LLC confirm that for the three months to 31 March 2025, 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