Google

Privacy Sandbox Progress Report

Q2 Reporting Period - April to June 2025
Prepared for the CMA, 29 July 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.

Google Ads is engaged in integration and testing of the APIs and providing feedback to the CMA and the ecosystem. There are no updates concerning Google Ads' testing in Q2 2025. 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.

Updated Timing Expectations

In April 2025, Google published a blog post concerning Next steps for Privacy Sandbox and tracking protections in Chrome, which announced that the current approach to offering users third-party cookies (3PCs) choice in Chrome will be maintained, and that Google will not be rolling out a new standalone prompt for 3PCs, as previously announced in July 2024.

This decision was taken in light of the considerable changes that have taken place in the digital landscape since the announcement of the Privacy Sandbox initiative in 2019, such as increased adoption of privacy-enhancing technologies, new AI-driven safeguards and evolving global regulations. Google will continue to enhance tracking protections in Chrome's Incognito mode, which already blocks 3PCs, including with the launch of IP Protection, planned for Q3 2025.

Additionally, Google is engaging with stakeholders across the ecosystem to understand the role the current Privacy Sandbox APIs could play going forward as well as potential future areas of investment. Google anticipates providing an updated roadmap in the coming months.

Google's latest expectations for the individual Privacy Sandbox proposals are set out in the Privacy Sandbox Timeline.[1] The summary below includes all Q2 2025 updates, covering the period from April 1 to June 30, 2025.

Privacy Sandbox Q2 2025 Timeline Updates	
April Timeline Updates	● No changes
May Timeline Updates	● No changes
June Timeline Updates	● No changes

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)

[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.

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
Future of Privacy Sandbox	In light of the announcement to not proceed with the introduction of a user choice mechanism for 3PCs, some APIs are more useful than others when 3PCs are present and others would need to evolve in order to be useful. There are additional potential areas for investment for Chrome beyond the Privacy Sandbox APIs.	We appreciate the feedback and we are continuing to engage with stakeholders in order to evaluate the role the Privacy Sandbox APIs can play going forward, as well as to explore new areas for future investment, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Privacy Sandbox	Some ecosystem participants are disappointed by the announcement to not proceed with the introduction of a user choice mechanism for 3PCs, but are proud of the work accomplished, they appreciate the technical challenges within Privacy Sandbox, and have emphasized the value of their collaborative working relationship with Chrome and the utility of the Market Testing Grant.	We appreciate the feedback and agree that Chrome can and should collaborate with developers to create technologies that improve online privacy while preserving an ad-supported internet.
Browser Data Sharing	Browser-mediated data sharing is a compelling technology with a potential to address market inefficiencies and trust	We appreciate the feedback and agree that Chrome can and should play a role helping developers with creating technologies that enhance trust between collaborating developers and users.

	issues. The browser has value as a third-party execution context for collaboration.	
Chrome Traffic	What is the share of cookieless traffic on Chrome and the share of traffic for Incognito mode?	As noted by the CMA in its "Notice of intention to release commitments", Incognito mode only affects a very small fraction of browsing activity. In each of the UK and the EEA, Chrome Incognito mode represents: less than 10% of navigations on devices running on the Android operating system; and less than 10% of navigations on devices running on the Windows operating system. These metrics refer to navigations only on Chromium-based Chrome in the UK and EEA. We do not share data about browsers who block 3PCs. Developers may determine when cookies are partitioned using Storage Access Headers and use available mitigations accordingly.
Chrome Testing Labels	What is Chrome's plan for 1% of cookieless traffic that was enabled for testing in 2024?	We do not have plans to share at this time, but we intend to share them publicly as soon as available.
Chrome Testing	Does the current testing label setup include a treatment for scenarios where both 3PCs are available and Privacy Sandbox APIs are enabled?	The current testing label setup includes treatment for both 3PCs and Privacy Sandbox APIs in the form of Mode A.
Privacy Sandbox	Some advertisers find Privacy Sandbox APIs complex and are experiencing apathy due to previous readiness exercises, questioning how to quantify the advantage for early adopters, and are looking for education about the effects of retargeting, prospecting and measurement.	We appreciate the feedback and understand the sentiments about technological complexity and readiness exercises. Regarding understanding the performance of the current Privacy Sandbox technologies, our testing results indicated that ecosystem participation is a critical factor in understanding the performance of the Privacy Sandbox solutions. Testing at low volumes could not reproduce the marketplace dynamics and incentives of using the technologies at scale.

Enrollment & Attestation

No feedback received this quarter.

Show Relevant Content & Ads

Topics

Feedback Theme	Summary	Chrome Response
Performance and Utility Interest in the Topics API with Enhancements	Feedback from buy-side stakeholders indicates that the Topics API is a valuable signal and results in Cost per Impression data (CPM) that is competitive with that for 3PC audiences, for advertiser campaigns. Some publishers view the Topics API's signal as being of greater quality than standard open web signals. Given this feedback on the Topics API's utility, stakeholders are requesting enhancements, such as improving taxonomy fidelity, consistency, and expanding publisher controls to drive wider adoption.	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Usefulness for different types of stakeholders	Because the Topics classifier currently uses only the page hostname to define the corresponding topics, large sites with diverse content are contributing generic topics while small sites are contributing niche topics with more advertising value.	Our response is similar to previous quarters: As with 3PCs, there is a difference in the value of information contributed by different sites. Niche-interest sites are inconsistent in their value contribution: not all niche-interest sites have commercially-valuable content, and therefore contribute less value. These are the sites which will benefit from the Topics API. We have considered the possibility of page-level rather than site-level classifications, however, there are a number of significant privacy and security concerns with such a classification.
Topics taxonomy not granular	The Topics API does not provide sufficient granularity	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox

enough	for news publishers with diverse content sections within a single domain, potentially limiting the API's usefulness for ad targeting.	APIs will play going forward, in light of Google’s April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Classifier Improvement	Allow publishers to give Chrome permissions to classify topics based on page content (e.g., head, body).	We are considering this request and welcome additional feedback here.
Policy	Request for clarification on the guidelines regarding the use of the Topics API in conjunction with 3PC information.	There are no difficulties with using both the Topics API and 3PCs, as the Topics API provides a subset of the functionalities of 3PCs.
Observe-Browse-Topics Header	Request for clarification on the implementation of the Observe-Browse-Topics header, specifically whether continuously returning the header would cause issues.	Continuously returning the `Observe-Browse-Topics: ?1` header will not cause any technical issues. The browser handles this signal efficiently, simply noting that the page visit is eligible for topic calculation without causing duplication or errors. While not required on every page, sending it as a standard header on all top-level documents is a valid and simple strategy.
Taxonomy Categories	Request to update the latest Topics taxonomy with new topics.	We are considering this request and welcome additional feedback from the ecosystem here.
Null Values	Request for guidance on improving the Topics API's performance and understanding the reasons behind the null responses, such as filtering or sensitivity.	For clarity, `null` or empty responses from the Topics API are an expected privacy feature, not an error. A `null` response can be caused by: • **Privacy Rules:** A 5% random `null` chance, or because your script has not "observed" the user on sites related to that topic. • **User State:** Insufficient browsing history, use of Incognito mode, or the user has opted out in Chrome's ad privacy settings. • **Technical Errors:** Publisher sites must send the `Observe-Browse-Topics: ?1` header, and any calling iframes require the `allow="Browse-topics"` permission.

		To investigate, use the **`chrome://topics-internals`** debugging page to see what topics your browser has calculated and why. While the privacy features prevent a 100% fill rate, you can improve performance by: • **Working with Publishers:** Ensure your partners correctly send the `Observe-Browse-Topics: ?1` header on their sites. • **Verifying Your Code:** If you use iframes, confirm the `allow="Browse-topics"` policy is in place.

Protected Audience API

Feedback Theme	Summary	Chrome Response
PA API Adoption Hindered by Cost and Complexity	Adopters are deprioritizing or rolling back Protected Audience API (PA API) integrations, citing operational costs, a lack of advertiser demand, and low inventory volume from exchanges. Some feedback included benefits of PA API's potential, such as its ability to deliver durable audiences and superior reach due to a high match rate.	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Cross-platform functionality	Cross-platform functionality should be supported by utilising PA API across platforms to unlock greater retargeting and audience targeting capabilities. Google should enable Interest Groups (IGs) registered in Chrome to be accessible when serving ads in native environments or	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.

	within webview, and interest groups registered in Android should be available in Chrome auctions.	
directFromSellerSignals	By limiting the amount of information available in the contextual auction, auction participants are always routed through Google's ad server. A publisher must call all of its exchange partners first, then Google Ad Manager (GAM) second to run the contextual auction and finally allow GAM to invoke IG auctions. Without knowing the contextual auction's result in real time, no competitor can fairly orchestrate a top-level decision. The directFromSellerSignals feature within PA API may lack transparency regarding auction information, potentially hindering the ability to access necessary data. Google should either remove directFromSellerSignals or update it so it cannot be used to hide the ad server's auction clearing price. For example, the contextual price could be passed through Chrome via a transparent, immutable, signed field that all auction participants (and the publisher) can access and verify.	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 PA API to understand any of the information their technology providers are passing into PA auctions, they can ask those technology providers for this functionality. **Google Ad Manager response**: 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.
Reporting	Request to add an	We are discussing this request here and

	analytics/reporting entity to enable centralized reporting.	welcome additional feedback.
K-Anonymity on buyerReportingId	Ability to discard bids based on the k-anonymity of the “buyerReportingId” to facilitate audience curation and reporting obligations with third-party data providers.	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google’s April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Improved Debugging in generateBid Script	Requesting a mechanism to rapidly identify the specific stage or “breakpoint” within the generateBid script where the process is failing.	We are aware of the desired usage of Real-Time Measurements as a breakpoint-setting mechanism for on-device auctions. We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google’s April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Event Listeners for Monitoring runAdAuction State	Proposal to add event listener support to PA API's navigator.runAdAuction function to improve monitoring of the ad auction lifecycle.	We are evaluating this request and welcome additional feedback from the ecosystem here.
API Usage	Request to clarify how PA API and Attribution Reporting API (ARA) can support web advertising use cases in the absence of 3PCs, particularly for users who have opted out of 3PCs but not out of Privacy Sandbox APIs, and in scenarios involving failed cookie syncs and WebView?	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google’s April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Latency	Latency associated with PA API could hinder adoption, as publishers may choose to disable PA API if latency is too high.	Several improvements to on-device latency were made in the past few quarters. Bidding and Auction (B&A) services building and scaling continues as necessary. Our latency best practices guide was updated to include more information on how to take advantage of these features. We are also exploring development of new latency improvements, some of which can be consulted here.

Logging Behavior in B&A (Test vs. Production)	Clarification regarding the differences in logging behavior between test and production modes for B&A services. Specifically, the availability of cloud logs and the impact of production mode on logging.	First, it's important to distinguish between **prod vs. non_prod builds** and the separate TEST_MODE parameter, which simply enables a hardcoded test encryption key. The below explanation focuses on the build types. In **non_prod builds**, B&A servers feature a configurable verbosity level for logging. These detailed logs are written to the standard stdout/stderr streams. On Google Cloud Platform, these are accessible through the native logging interface, and on Amazon Web Services, they can be found in the attached-console logs. For **prod builds**, the logging behavior is more restricted. The verbosity level is fixed and cannot be changed. While some non-privacy-relevant logs, such as server startup messages and most crash errors, are still printed to stdout/stderr, no request-specific logs are available through this channel. The only per-request logs from a prod build are for requests containing a consented debugging token, and these are exported exclusively via OpenTelemetry. It's important to use consented debugging sparingly, as heavy traffic can degrade server performance and lead to health-check failures. Regarding **metrics**, all are exported via OpenTelemetry. Non-privacy-sensitive metrics are always exported as-is, without any "noising". Conversely, privacy-sensitive metrics are always "noised" when exported from a server running in prod mode. The specific telemetry configuration determines whether these privacy-sensitive metrics are exported as noised, un-noised, or both.
Include Full Page Path in Trusted Bidding Signals for Brand Safety	Request for an update to PA API to include the full URL path of the top-level page, in addition to the hostname, in the fetch request for trustedBiddingSignals. The primary use case is to enable more granular brand	We are currently discussing this issue here, after extensive prior discussions, that can be consulted here, and we welcome additional feedback. However, we want to clarify that we are only considering adding this information when the trustedBiddingSignals fetch is going to a server running inside a Trusted Execution Environment

	safety controls. Advertisers often need to block ads from appearing on specific sections of a domain (e.g., news-site.com/politics) while being comfortable with the domain in general. As these blocklists can be millions of entries long, they must be evaluated on the server-side. The current specification, which only sends the hostname, makes it impossible for the trustedBiddingSignals server to perform this necessary path-level evaluation, limiting brand safety capabilities.	(TEE).

Protected Auction (B&A Services)

Feedback Theme	**Summary**	**Chrome Response**
Testing Availability	Information regarding the availability of Key/Value (KV) v2 for testing in both Chrome and B&A environments.	KV v2 is available both on B&A and Chrome. Additional guidance is available here.
KV Server Implementation	Request for clarification on the usage of the KV server, specifically concerning mapping creative render URLs to request data, the necessity of coordination between SSPs and DSPs for defining parameters in the render URL, and the availability of documentation outlining required coordination and data storage in KV mode.	The KV service uses the renderURL as a key. If the URL is new, it's stored. If it exists, its value is returned for use in scoreAd. The return format depends on the setup: "Bring Your Own Server" (BYOS) allows any value, while the Trusted KV service requires a User-Defined Function. While not always required, coordination with DSPs is essential for features like macro replacement (e.g., ${AD_WIDTH}) in the renderURL, which enables dynamic ad customization and verification. We recommend starting with a simple test with one DSP to determine the necessary level of coordination. We are also in the process of updating our KV documentation and will share it publicly once available.

BYOS for B&A	Why doesn't B&A offer BYOS mode similar to KV's BYOS mode?	B&A requires a TEE, preventing a BYOS model, because it handles highly-sensitive data combinations which require the enforcement of privacy mechanisms, as explained below. For **DSPs**: B&A processes publisher context (potentially the full URL if explicitly sent by the seller via auctionSignals / perBuyerSignals) combined with detailed user IG data. The TEE is essential to securely process this combination and to prevent potential user re-identification. In KV BYOS, the full URL cannot be sent. For **SSPs**: Even just knowing the combination of participating IGs (and their DSP owners) in an auction can generate an identifying signature. This is where the chaffing solution comes into play, which requires the use of a TEE. Therefore, the secure processing of these combined sensitive signals and the enforcement of privacy mechanisms mandate the controlled, attested environment of a TEE.

Measuring Digital Ads

Attribution Reporting (and other APIs)

Feedback Theme	Summary	Chrome Response
Noise Policy	The implementation of ARA has been valuable for some market participants and Google should continue to maintain event-level reporting. Google should consider relaxing the noise policy in scenarios where both ARA and 3PCs are available. Performance advertisers are increasingly using the current 'value' field implementation of the ARA	This mechanism is a foundational part of the ARA's design, which is meant to protect user privacy by preventing individual tracking. We are taking into consideration the feedback about the reporting challenges caused by noise, as we continue to evaluate the role the Privacy Sandbox APIs will play going forward, as well as any potential future enhancements, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.

	flex event, and a less restrictive noise policy would help reduce delays and inaccurate reporting.	
Roadmap and Long-Term Support	Requesting a product roadmap for ARA, as well as confirmation of long-term investment and support given the announcement to not proceed with the introduction of a user choice mechanism for 3PC.	The Privacy Sandbox team is engaging with the ecosystem to understand the role the Privacy Sandbox APIs will play going forward and to evaluate any future investments.
Cross-Environment Measurement (App-to-Web)	Request for a solution that involves utilizing ARA to facilitate cross-environment measurement, offering a cleaner and more reliable data flow, enhancing the ability to connect user interactions across different platforms.	App-to-Web on the same device is already supported by ARA. You can find more details on the cross app and web measurement solution here and here.
Cross-Browser Attribution	A unified, cross-browser approach to ARA would dramatically improve the ability to measure ROI on the open web and provide a stable alternative ahead of potential regulatory shifts. Chrome should collaborate with the Safari team on a solution like this.	We are already exploring an interoperable API with other browser vendors in the PATCG and PATWG groups within the W3C. Noting that this work is preliminary, stakeholders are welcome to consult our progress here.
Cross-Device/Offline Measurement	Inability to support cross-device conversion measurement within ARA is a significant limitation. Measuring online-to-offline conversions is also significantly important, and the browser could play a role in collaborating with measurement vendors.	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Multi-Touch Attribution	Request to allow advertisers to use Privacy Sandbox data	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox

	as an unbiased "ground truth" to validate and calibrate their existing attribution models. This can be achieved by using ARA's browser-provided data as a reliable calibration signal, creating a baseline of truth.	APIs will play going forward, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Consentless/Opted -Out Traffic Measurement	A privacy-preserving solution, such as Interoperable Private Attribution, would enable measurement for consentless traffic. This would allow for a more comprehensive understanding of campaign performance by including data from users who have opted out of tracking, addressing a major gap in measurement created by consent requirements.	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Server-to-Server Attribution	Request to allow ad techs with sophisticated server-side infrastructure to integrate with ARA in a more flexible way, accommodating use cases that are difficult to manage purely on the client side, while maintaining user privacy.	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Multi-Domain Enrollment	Seeking clarification on limitations and caveats when enrolling multiple domains with ARA, particularly concerning the aggregation service and cross-origin attribution.	Below are the key limitations when using ARA with multiple domains: • **Attribution is scoped to a single origin.** You cannot match a click from one of your domains to a conversion on another. Attribution is sandboxed to the same origin for both the source and trigger. • **The Aggregation Service does not support multi-origin batching.** Reports from different origins must be batched and processed separately. We are exploring ways to support

		this in the future. Briefly, while multiple domains can be enrolled under one entity, all ARA functions, such as attribution and aggregation, must currently be handled on a per-origin basis.

Aggregation Service

No feedback received this quarter.

Private Aggregation API

Feedback Theme	Summary	Chrome Response
Limits and Noise Levels	Concerns regarding limitations on aggregation key sizes and aggregation values within the Private Aggregation API.	Aggregation key and value sizes were chosen to have high granularity while limiting network and storage costs. We also recommend using hashing when assigning keys to maximize flexibility. While there are other factors protecting user data, adding noise is an important piece of the Private Aggregation API's privacy protections. We are taking into consideration the feedback and will continue to evaluate the appropriate parameter choices alongside our consideration of the role the Privacy Sandbox APIs will play going forward, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.
Privacy vs. Utility	The Privacy Sandbox's approach may prioritize privacy over utility, potentially hindering adoption. Suggestion to allow more granular data sharing with user consent to improve measurement and ad personalization.	Aggregation key and value sizes were chosen to have high granularity while limiting network and storage costs. We also recommend using hashing when assigning keys to maximize flexibility. We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in

		Chrome will be maintained.

Limit Covert Tracking

User Agent Reduction/User Agent Client Hints

Feedback Theme	Summary	Chrome Response
Spam Detection	If the first request from a website that uses a spam detection system relies on client hints, the tracking or detection system could fail to identify or properly categorize the request.	Use cases that rely on having access to User-Agent Client Hints (UA-CH) on the first request should make use of critical client hints.
API Feedback	Consider deprecating Sec-CH-USA-Wow64 as it is no longer relevant for the modern web.	We are considering this request and welcome additional feedback here. We have also received feedback that it would be useful to extend wow64 beyond Windows.

IP Protection (formerly Gnatcatcher)

Feedback Theme	Summary	Chrome Response
Controls	Request for IP Protection toggle for sites to use selectively outside of Incognito mode.	We appreciate the feedback and we welcome additional input on this issue here.
Misconduct	Will Probabilistic Reveal Tokens (PRTs) resulting in a NULL value prevent perpetrator identification when police request IP address disclosure for platform misconduct?	If a domain is used exclusively for fraud and abuse detection, it's likely not included in the Masked Domain List (MDL) and therefore not impacted by IP Protection. Consequently, PRTs would not be needed for those domains. If a domain is included in the MDL, PRTs are currently the only way to learn the original IP address for a proxied request. As PRTs are specifically designed to support aggregate analysis, not individual identification, it is true that PRTs will not contain an IP address in most cases. We expect this to have limited impact in the described scenario, however, as IP Protection applies only in the third-party

		context, meaning that publishers will continue to receive un-proxied IP addresses for first-party interactions, such as users visiting the site of an online platform.
Anti-Fraud	What are the specifics of Google's anti-fraud measures for IP Protection, including details on rate-limiting access to proxies and authentication token issuance, and what are the specific use cases for PRTs ?	We confirm that rate-limiting and authentication tokens in IP Protection are designed to prevent bots from performing ad fraud by over-accessing proxies, as detailed in the anti-fraud and anti-spam strategy. Further use cases for PRTs are outlined in the PRT explainer documentation here.
Incognito Mode	Is IP Protection in Incognito mode still planned for Q3?	There are currently no changes to the Q3 timeline for IP Protection launch in Incognito mode.

Bounce Tracking Mitigations

Feedback Theme	Summary	Chrome Response
API Feedback	Chrome should block cookie/storage access rather than partitioning them when applying Bounce Tracking Mitigations (BTM), citing unintended behavior and confusion from Safari's "partitioning" method.	We welcome this suggestion. Currently, BTM does not involve cookie/storage partitioning and instead deletes it after a grace period. If there are any later designs to BTM that involve immediate action towards cookies, we intend to prefer blocking cookies over partitioning them.

Strengthen cross-site privacy boundaries

Related Website Sets (formerly First-Party Sets)

No feedback received this quarter.

Fenced Frames API

No feedback received this quarter.

Shared Storage API

Feedback Theme	Summary	Chrome Response
API Feature Request	Request to append ad views and clicks in Shared Storage.	We are taking this feedback into consideration as we evaluate the role the Privacy Sandbox APIs will play going forward, in light of Google's April 2025 announcement that the current approach to offering users 3PCs choice in Chrome will be maintained.

CHIPS

Feedback Theme	Summary	Chrome Response
API Question	Request for clarification on how Chrome's 3PC controls interact with CHIPS, specifically whether non-partitioned cookies are converted to partitioned ones when 3PCs are disabled, and if partitioned cookies remain active.	Non-partitioned cookies will not be stored, retrieved, or sent in a third-party context when 3PCs are disabled. Partitioned cookies, however, will continue to be stored, retrieved, and sent in a third-party context, as their functionality is not impacted by browser settings that disable 3PCs.
Privacy Concern	Concern that an embedded party with a persistent identifier, such as for Single Sign-On, might still enable both embedding and embedded parties to gain a global digital identifier, even with partitioned cookies.	While an embedded party may have a persistent identifier, this identifier, when stored in a partitioned cookie, is only accessible on the site where the cookie was set by the embed. Cross-site joining of this identifier would require a login action, which already allows for the exchange of an identifier in the form of an authentication token, even without the use of

		partitioned cookies.

FedCM

Feedback Theme	Summary	Chrome Response
API Usage	Silent mediation failing for users with multiple accounts with no specific error.	The silent mediation behavior is a by-design feature, as it is intended for a very specific case with just one available account. The recommendation is to use the “optional” mediation instead, in which FedCM falls back to presenting the user with an account chooser if silent mediation is not possible.
API Usage	`navigator.credentials.get` returns generic errors, preventing capture of specific rejection reasons like user dismissal or cooldown periods.	The inability for developers to distinguish between the user dismissing the FedCM dialog vs. a network error vs. FedCM being in a “cooldown period” due to the user having previously dismissed the dialog is also a by design feature, meant to preserve the user’s privacy. The concern is that such a capability would allow websites to infer the user’s login state on different Identity Providers (IdPs).
Sign-in	Inconsistent account selection behavior with multiple signed-in accounts was observed.	It is unclear whether the intermittent inability to select a specific account in a multiple-signed-in-account scenario is an intermittent bug in FedCM or some issue involving the testing system. We are working with the reporter to resolve this issue, and have asked for further details in order to better understand the issue.
API Usage	If the user dismisses the dialog while authorising with FedCM, the fact that they are in the cooldown state is not reported via a catchable error.	Yes, that would be the case and this would produce the generic error code in order to preserve user privacy.

API Usage	Why does FedCM go into a 10-minute quiet period after a successful “auto-reauthentication”?	Given that auto-reauthentication happens without a user-initiated action, if the user wanted to go back to the website but sign in with a different account, they would need a period of time when FedCM does not auto-reauthenticate them. The “quiet period” provides the opportunity for users to manually sign in using a different account. This blog post has further details on this “quiet period”.
Lightweight FedCM	Concerns that the Lightweight FedCM proposal introduces additional complexity for IdPs due to the need for supporting two incompatible implementations (FedCM vs. Lightweight FedCM).	Lightweight FedCM is compatible with traditional FedCM. IdPs can choose which implementation method to use and will not be required to support both. Lightweight FedCM is a push mechanism for FedCM. If an IdP chooses to use this feature, they can push the account information to the browser when the user logs in, so that, when a Relying Party (RP) invokes FedCM, the account would be retrieved from the browser, instead of the IdP’s accounts endpoint.
Lightweight FedCM	Concerns about the exposure of personal user data such as name, email, and profile picture to the RP in the Lightweight FedCM proposal.	The proposal for Lightweight FedCM has been updated since receiving this feedback, to remove the name, email, and profile image from the method response.
Lightweight FedCM	Managing multiple signed-in accounts appears to be too rigid in the Lightweight FedCM proposal. The proposal does not currently support individual session lifetimes or nuanced login states per account.	Expiration is currently tied to the IdP within the credentials object. We have noted per-account expiration as an open question and will take this feedback into consideration for future developments.
Lightweight FedCM	The distinction between "signed in" and "available for selection" is not clearly defined, which could impact the user experience for the Lightweight FedCM proposal.	We do not currently support the ability to distinguish if an account is logged in or logged out in the FedCM User Interface (UI). Logged out accounts should not be listed. If an account is logged out and listed, and a user selects the account that is not actively logged in, the Continuation API can be used to have the user log back in.

API Usage	Inconsistency between the `given_name` field in `getUserInfo` and its usage in the FedCM UI.	This issue was discussed further with Mozilla here, in order to align on how `given_name` should be treated in `getUserInfo`.
API Usage	Not all fields used in the UI from `IdentityProviderAccount` are provided to `getUserInfo`, specifically `tel` and `username`, suggesting a need for synchronization.	The discussion with Mozilla and other FedID Community Group members is progressing on the issue of reconciling which fields from `IdentityProviderAccount` get sent to `getUserInfo.`
Enterprise FedCM	Request for FedCM support for Enterprise IdP use cases.	The key issue is the need for a *trusted* mechanism for IdPs to signal to browsers that administrators have pre-consented to allow the user to access specific RPs that cannot be mimicked and/or abused by Web trackers. This was discussed in the 22 April FedID CG meeting (please find here notes of the meeting) and combinations of browser extensions and Enterprise Policies (for managed devices) were put forth as potential solutions. We welcome additional feedback on this issue here.

Fight spam and fraud

Private State Token API (and other APIs)

No feedback received this quarter.

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 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.

Stakeholder concerns

The CMA has raised a number of stakeholder 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.

Google’s April 2025 announcement regarding next steps for Privacy Sandbox and tracking protections in Chrome – The CMA shared feedback from a stakeholder that Google’s announcements regarding Privacy Sandbox may encourage competitors to invest in solutions that Google might not implement, and that some market participants have invested significant resources and dedicated considerable effort to engineering, product development, analytics, and infrastructure for the Privacy Sandbox. Google has always sought to keep the ecosystem updated regarding developments related to Privacy Sandbox in a timely manner, and Google’s most recent announcement reflects the changes and advances that have been made in the ecosystem since Google announced the Privacy Sandbox initiative in 2019 and entered into a formal engagement with the CMA and ICO in 2022. Google’s updated approach to Privacy Sandbox takes into consideration the evolving needs of the ecosystem as well as ongoing ecosystem engagement and regulatory and technological developments to provide the best experience for Chrome users while continuing to support advertising on Chrome.

The CMA has also shared feedback that Google’s April 2025 announcement does not protect digital markets from its conduct. The stakeholder concerned considers that Google could unfairly direct users to Incognito mode, which restricts the data sent to third parties, but not to Google, and that Google has used misleading language, non-transparent consent designs, and other dark patterns in its choice screens. In May 2020, almost two years prior to the adoption of the Commitments, Chrome announced that it would start blocking 3PCs by default within each session in Incognito mode. Google does not plan to promote Incognito mode as an alternative for users’ day-to-day needs. In addition, Google’s research regarding UX and UI for Privacy Sandbox on Chrome has been carried out under the supervision of the CMA and ICO which have reviewed relevant changes ahead of their implementation to ensure that all changes are aligned with the Commitments.

The CMA has shared feedback that the title of Google's announcement, "*Next steps for Privacy Sandbox and tracking protections in Chrome*", exemplifies the ongoing harm caused by Google's announcements. The stakeholder considers that this title does not commit to making changes to Google's alleged interference with third-party publishers' use of data for advertising purposes. Google has never suggested that all potential stakeholder concerns would be addressed in a single blog post. The purpose of this blog post is to update the ecosystem regarding Privacy Sandbox and in particular, Google's decision to continue supporting 3PCs on Chrome. For clarity, Google's decision makes it clear that 3PCs will continue to remain available on Chrome, thereby significantly reducing any perceived risk of Google interfering with publishers' use of data. The title of the blog post is not intended as a commitment or comprehensive statement, but rather a reference to Google's overarching online privacy-enhancing plans and goals.

Proposal for introduction of a User Choice Mechanism – The CMA has shared feedback from stakeholders concerning Google's announcement in July 2024 that it would not deprecate 3PCs on Chrome, and instead proposed to introduce an updated approach to elevate user choice on Chrome. As set out in further detail below, in light of Google's announcement in April 2025 that Google will not be rolling out a new standalone prompt for 3PCs on Chrome, feedback regarding the proposed introduction of a user choice mechanism is no longer applicable. However, for completeness we have addressed this feedback below.

Certain stakeholders suggested that the user choice mechanism should not be rolled out without a comprehensive market testing phase, that it should not be deployed until potential competition concerns were addressed and that the governance framework should be implemented prior to its introduction. Stakeholders also considered that Google would be abusing its market position if it were to impose terms that override the choices freely expressed when users access specific websites and that Google's proposed user choice mechanism did not facilitate users to exercise choice, because consumers visit a website and freely agree to its data usage terms. Stakeholders also offered comments on the Commitments in light of Google's user choice mechanism proposal, including regarding their scope, testing requirements, Standstill period and duration.

As previously explained in Google's Q1 2025 Progress Report, Google has invested significant resources in the development and testing of the Privacy Sandbox technologies, and has encouraged their testing including by publishing guidance, in collaboration with the CMA, and by making grant funding available for engineering and testing related work. Moreover, Google wishes to reassure the ecosystem that, as set out in Google's Q4 2024 Progress Report, the proposed user choice mechanism was being discussed in detail with the CMA and the ICO prior to Google's subsequent announcement in April 2025 about its plans. Therefore, any well-founded competition or privacy concerns with the user choice mechanism would have been addressed by means of substituted commitments, if offered and accepted. As indicated in the CMA's Q2/Q3 2024 Update Report, the CMA's view was that "*Google's proposed* *governance framework could resolve a range of outstanding issues once finalised and provided it is implemented effectively*".

Competition Feedback – The CMA has shared feedback from stakeholders arguing that Google has market power as a browser owner, and that publishers wishing to offer content free of charge are required to rely on Google's advertising services due to its market position in browsers and search. These stakeholders also consider that Google has used its Chrome browser to self-preference its own products and that Google is bundling its advertising services with Chrome and discriminating in favour of its own products and allegedly restricting competing publishers from effectively operating with third-party ad tech providers and restricting functionality for third-party ad tech providers while retaining this functionality for its own advertising services.

As with any ecosystem participants, publishers are not obliged to make use of the Privacy Sandbox APIs, nor to engage Google's advertising services in order to facilitate advertising on their inventory in the Chrome browser. Publishers can make use of multiple technologies and engage a range of third-party providers of ad tech services available on Chrome, and Google actively works to support third-party providers of ad tech services on Chrome. Moreover, as set out in further detail below, Google announced in April 2025 that the current approach to supporting 3PCs on Chrome will be maintained, further reducing any perceived reliance which publishers may have on Google's advertising services. However, for completeness, under the Commitments, Google has undertaken to design and implement the Privacy Sandbox proposals in a way that does not distort competition by self-preferencing Google's own business, and to take into account impact on competition in digital advertising and on publishers and advertisers, regardless of their size.

First-party data – The CMA has shared feedback from a stakeholder that Google insulates itself from any financial impact to its advertising services by relying on its "first party" exemption. The stakeholder considers that Google has not justified this approach, which in its view distorts digital markets by preferencing vertical integration over decentralized competition, without any privacy benefit. As set out in further detail below, Google announced in April 2025 that the current approach to supporting 3PCs on Chrome will be maintained, and third parties will continue to have access to 3PCs for advertising use cases. Notwithstanding the extensive measures which Google has put in place through the Commitments and associated monitoring process under the supervision of the CMA, ICO and the Monitoring Trustee, in any event, Google considers that the stakeholder's concern cannot arise in these circumstances.

Privacy risks of 3PCs – The CMA has shared feedback from a stakeholder claiming that Google is suggesting that all 3PCs pose significant privacy risks to users, and that such concerns are unfounded since data stored in cookie files is not necessarily personal data subject to the EU's General Data Protection Regulation. The stakeholder considers that advertisers go to considerable lengths to protect data and deidentify user information, through contractual and technical safeguards. The aim of Privacy Sandbox is to develop new ways to strengthen online privacy while ensuring a sustainable, ad-supported internet. While Google has sought to ensure that the Privacy Sandbox APIs enable compliance with applicable legislation, and have engaged with regulators in their development, we don't consider the basic legal requirements to be a cap on what we can offer to the industry and to users. More information and resources concerning the privacy goals of Privacy Sandbox are available here.

Protected Audience API – The CMA has shared feedback with Google that the design of Privacy Sandbox could strengthen Google's position in ad tech services. According to this feedback, Chrome's use of the directFromSellerSignals feature in the PA API allows Google's ad server to not disclose the contextual auction price to publishers and their partners. The stakeholder considers that competitors require access to the contextual bid price to compare bids from multiple sources in real-time and that directFromSellerSignals ensures that only GAM sees the publisher's highest contextual bid, while publishers and ad exchanges do not receive this information. However, Google's ad server can choose to not share its own price using directFromSellerSignals in order to protect commercially-sensitive information. The CMA has also shared stakeholder feedback that although Google stated in its Q4 2023 Progress Report that it will "*not share the bid of any auction participant with any other auction participant prior to completion of the auction in multi-seller auctions*", in line with its commitments to the French Competition Authority, according to the stakeholder this commitment was made to prevent Google from having unequal access to data when casting an AdX bid or sharing that ability with paying Google Open Bidding integrations. The stakeholder objects that Google is now presenting this commitment as an inability to pass its own bid to other auction participants.

Our response remains unchanged from previous quarters:

"*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.*"

User-Agent Client Hints – The CMA has shared a range of stakeholder feedback regarding UA-CH and the corresponding obligations under the Commitments. As set out in further detail below, in light of Google's announcement in April 2025 that Google will maintain the current approach to supporting 3PCs on Chrome, the CMA considers it has reasonable grounds for believing the Commitments are no longer necessary, and launched a consultation on releasing Google from the Commitments. Notwithstanding this, for completeness, we have addressed this stakeholder feedback below.

The CMA has shared stakeholder feedback that Google's email announcement of 25 February 2025 to the IETF HTTP Working Group indicates that the first request to a site might be missing critical client hints. According to the stakeholder, this lack of critical data being passed on results in websites receiving incomplete information on the initial page load. The stakeholder considers that this is a breach of Google's non-discrimination obligation under the Commitments as Google has immediate access to critical user data, through x-client data, that other websites do not have access to and is self-preferencing its own products and services.

In Google's email announcement itself, Google proposed two mitigations to resolve this issue. First, if a website needs a specific set of client hints in their initial request, they can use the Critical-CH response header, as explained in further detail here. Second, a new ACCEPT-CH Frame has been proposed, which is an alternative mechanism that carries Client Hint preference for the servers. This ensures the information is available to the user agent when it makes the first request. Further detail regarding the ACCEPT-CH Frame is available here.

In respect to Google's alleged access to critical user data via x-client data, as set out in Google's Q1 2025 Progress Report, 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. The concern is therefore misplaced.

The CMA also shared stakeholder feedback that a claimed inability/failure to pass on critical hints on the initial page load breaches the Commitments, which require Google to allow publishers, advertisers and ad tech providers to make unlimited requests for UA-CH, so that all the information available in the User-Agent string would remain accessible during the period prior to the removal of 3PCs.

In any event, there has been no breach of the Commitments. As stated in Google's Q4 2022 Progress Report, "*all the information currently available in the User-Agent strings is recoverable via UA-CH*". Moreover, the CMA confirmed the same in its Q4 2022 Update Report, stating that "*Based on the evidence provided to date, we are satisfied that all the information in the UA-String will remain available in UA-CH, as required under the Commitments*". For completeness, we recognise that the first request to a site may potentially be missing critical hints, because high-entropy UA-CH headers are sent by browsers only after a request from the server, for the purpose of limiting the fingerprinting of users. Indeed, UA-CH allows access to the full set of User-Agent data, in a more privacy-preserving way, only when servers actively declare an explicit need for specific pieces of data. However, Google's email announcement of 25 February 2025 to the IETF HTTP Working Group sets out two mechanisms to resolve this issue, as described above.

The CMA has shared feedback that websites function sub-optimally during the initial page load, resulting in a degraded user experience and impacting publishers' ability to generate revenue, and that UA-CH results in increased initial navigation time and inconsistent behavior. The stakeholders concerned consider that this is a breach of the Commitments.

Keeping latency to a minimum is a key design goal of the Privacy Sandbox APIs. Google has carefully assessed and worked on resolving the potential latency issues related to UA-CH for the past several years. Google published detailed metrics and latency measurements in its Q4 2022 and Q1 2023 Progress Reports, which showed a modest latency impact resulting from User-Agent Reduction (UAR) and the introduction of UA-CH. We continue to monitor and make improvements to reduce latency and welcome further feedback from the ecosystem here. In light of the holistic assessment envisaged by the Development and Implementation criteria, and the circumstances just described, we consider there is no basis for claiming a breach of the Commitments.

The CMA has shared stakeholder feedback that Google's implementation of UA-CH constitutes a violation of the anti-circumvention requirement under the Commitments and that by proceeding with a change that creates an anti-competitive advantage, particularly through its integration within the Chrome browser, Google has effectively bypassed the intended safeguards set out in the Commitments.

The introduction of UA-CH and the roll-out of UAR was carried out under the close supervision of the CMA. As noted above, to address potential concerns and increase transparency, Google published detailed information regarding UAR in its Q4 2022 and Q1 2023 Progress Reports. Indeed, adopting a cautious approach regarding latency and ecosystem dynamics, Google initially limited the envisaged increase of Phase 6 UAR to 5% rather than 10%. In any event, Google's obligation under the Commitments regarding UA-CH requires that "*before the Removal of Third-Party Cookies Google will allow publishers, advertisers and ad tech providers to make unlimited requests (and receive responses) for User-Agent Client Hints, so that all of the information available in the user-agent string as of the Effective Date would remain accessible during the period prior to the Removal of Third-Party Cookies.*" It is clear from the CMA's confirmation as set out above that Google has not breached this obligation.

Trusted Execution Environment – The CMA has shared stakeholder feedback regarding TEEs. As set out in further detail below, in light of Google's announcement in April 2025 that Google will maintain the current approach to supporting 3PCs on Chrome, the CMA considers it has reasonable grounds for believing the Commitments are no longer necessary, and has launched a consultation on releasing Google from the Commitments. Notwithstanding this, for completeness, we have addressed this stakeholder feedback below.

The CMA has shared feedback from a stakeholder according to which Google incorrectly claims that TEEs do not involve the collection and processing of personal data because, without a contract with the data controller (e.g., media owner), Google retains both the technical and organisational ability to reidentify the data it receives, and accordingly such data still qualifies as personal data. Another stakeholder states that Google's claims regarding the privacy benefits of TEEs lack sufficient evidence to justify the potential harm the proposed browser changes will have on competitors and argues that Google intends to require ecosystem participants to use TEEs despite the absence of any privacy improvements. A stakeholder also argues that the design of Google's TEE adds unnecessary latency, cost, and complexity that may negatively impact the digital advertising ecosystem. Another stakeholder states that Google's designs exempt the use of identity-linked personal data as a common match key for advertisers to share their data if ecosystem participants use TEEs, and that Google restricts real-time communication of input data from its competitors, while retaining this functionality for its own auction services, which is an alleged breach of the Commitments.

This claimed comparison with Google's own auction services is addressed in relation to Customer Match below.

In line with Google's announcement in April 2025 that the current approach to supporting 3PCs on Chrome will be maintained, any perceived potential adverse impact of the introduction of TEEs should no longer be a concern, because ecosystem participants can continue to rely on 3PCs. As always, they remain free to choose the best solution adapted to their own needs and are not required to make use of the Privacy Sandbox APIs.

The CMA shared feedback from a stakeholder that Google's own CMA submissions contradict its privacy claims. In Google's Q2 and Q3 2024 Progress Report, Google stated that "*there is currently no TEE technology which fully protects user data from a potentially adversarial operator. Therefore, we include multiple requirements to validate the trustworthiness of the cloud provider*". The stakeholder considers that this undermines Google's assertions regarding the privacy benefits provided by the design of its TEE. This statement made by Google refers to the fact that, currently, there is no on-premise TEE solution that could fully protect user data from a potentially adversarial operator unlike public cloud providers. Google has sought to address this issue and engaged in extensive research regarding potential approaches to secure the privacy of Chrome users in an on-premise TEE. Google will share any updates with the ecosystem in this regard as they become available.

Customer Match – The CMA has shared stakeholder feedback according to which Google's designs exempt the use of identity-linked personal data as a common match key for advertisers to share their data, to improve the monetization of Google's own ad inventory. The stakeholder considers that the Commitments state Google will only use such data transfers for its own benefit and exclude any benefits to rival publishers, and that removing competing publishers' technical ability to rely on deidentified match keys while promoting the use of identity-linked match keys is a breach of the Commitments. 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. Moreover, in light of Google's announcement in April 2025 that Google will maintain the current approach to supporting 3PCs on Chrome, the CMA considers it has reasonable grounds for believing the Commitments are no longer necessary, and has launched a consultation on releasing Google from the Commitments. The concern is therefore misplaced.

Moreover, this stakeholder feedback misstates how Customer Match works. As explained in Google's Q1 2025 Progress Report, Customer Match is a helpful feature for all advertisers, as it allows them 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 simply uses data provided by third-party advertisers upon their request for remarketing purposes. Advertisers in any event collect and use such first-party data for similar purposes as Customer Match.

Search ranking and latency – The CMA has shared feedback from a stakeholder that Google's position in Search and use of latency as a ranking factor means Google can design the Privacy Sandbox APIs to disadvantage competing publishers' rankings in organic search results if they choose to engage third-party advertising services. The CMA has also shared feedback from a stakeholder that, while Google has confirmed that when rival publishers opt-out, their choice will not be used directly by Google as a ranking signal of their links in Search, Google has not stated that it will not use this choice indirectly, given the impact to latency in the Privacy Sandbox API designs and its published use of this factor in its search rankings.

In line with Google's announcement in April 2025 that the current approach to supporting 3PCs on Chrome will be maintained, any perceived potential adverse impact of the introduction of the Privacy Sandbox APIs should no longer be a concern because ecosystem participants can continue to rely on 3PCs. They remain free to choose the best solution adapted to their own needs and are not required to make use of these tools. In any event, as set out in 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.*"

Privacy Sandbox on Android – The CMA has shared stakeholder feedback regarding Privacy Sandbox on Android. This feedback argues that certain Privacy Sandbox APIs are available through Android and that Google's Commitments include personal data collected or processed via Google's Android operating system. It is said that Google's control over the Android OS could enable Google to preference its own advertising services; and that interfering with real-time communication between web and app-based software reduces interoperability and creates challenges for advertisers and competing publishers operating across both environments.

First, we note that Privacy Sandbox on Android is not within the scope of Google's Commitments to the CMA. The Commitments refer to Android only to the extent that Google's data usage commitments with respect to tracking users to target or measure digital advertising on ad inventory on websites not owned and operated by Google, after Chrome ends support for 3PCs, refer to personal data from, among other sources, Google's services available on the Android operating system as deployed in smartphones, connected televisions or other smart devices. Thus the feedback received relates to a workstream that is outside the scope of the Commitments.

Second, Privacy Sandbox on Android remains in Beta mode and to date, Google has not removed any signals or identifiers from Android as part of Privacy Sandbox on Android and will provide substantial notice to the ecosystem ahead of any future changes in this regard. The APIs for Privacy Sandbox on Android are merely one alternative, amongst other signals and technologies, for targeting and measurement of online advertising. Ecosystem participants remain free to choose the best solution adapted to their own needs.

Third, as we have already stated in our Q1 2024 Progress Report, we agree that it's desirable to support app and web interoperability and have launched cross app and web attribution measurement and are exploring web-to-app targeting solutions.

Updated approach to 3PCs on Chrome

As mentioned above, in April 2025, Google announced that the current approach of supporting 3PCs on Chrome will be maintained, and that Google will not be rolling out a new standalone prompt for 3PCs, as previously announced in July 2024. This decision was taken in light of the considerable changes that have taken place in the digital landscape since the announcement of the Privacy Sandbox initiative in 2019, such as increased adoption of privacy-enhancing technologies, new AI-driven safeguards and evolving global regulations. Google will continue to enhance tracking protections in Chrome's Incognito mode, which already blocks 3PCs, including with the launch of IP Protection, planned for Q3 2025.

Throughout the development of Privacy Sandbox we have engaged extensively with the CMA and ICO, in order to ensure that changes to Chrome continue to support competition and privacy in digital advertising. We are in discussions with the CMA on our updated approach and the consultation on releasing Google from the Commitments, launched by the CMA in June. Google will continue to gather feedback and work with the ecosystem on determining how the Privacy Sandbox APIs can best serve the industry and consumers. An updated roadmap for the Privacy Sandbox APIs will be shared with the industry in the near future.

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 30 June 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