



# Privacy Sandbox Progress Report

Q3 Reporting Period – July to September 2022

Prepared for the CMA, 21 October 2022

## Overview

Google has prepared this quarterly report as part of its Commitments to the 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, details are provided in the [overall "Privacy" blog posts](#) along with the "Progress in the Privacy Sandbox" series published by Chrome's Developer relations team [here](#). In each blog post, the team shares a developer-focused overview of the updates to the [Privacy Sandbox timeline](#) along with news from across the project.

## Updated Timing Expectations

Google's latest expectations for the timing of the Privacy Sandbox proposals are set out in the [Privacy Sandbox Timeline](#).<sup>1</sup> The summary below includes all Q3 2022 updates, covering the period from July 1 to September 30, 2022.

---

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

Privacy Sandbox Q3 2022 Timeline Updates	
July Timeline Updates	<ul style="list-style-type: none"> <li>• <b>Testing Timeline Extension.</b> On 27 July 2022 Google <a href="#">published a revised timeline</a> for the testing and implementation of the Privacy Sandbox APIs and removal of third-party cookies. The revised timeline extends the testing window for the Privacy Sandbox APIs, reflecting consistent feedback from the ecosystem to have more time to evaluate and test the new Privacy Sandbox technologies before deprecating third-party cookies in Chrome.</li> <li>• <b>FAQ updated to include sentence highlighted in yellow:</b> What is the difference between functional testing and effectiveness testing? <ul style="list-style-type: none"> <li>○ When a feature is initially made available for testing, typically through a feature flag, the focus is generally on functional testing. This means that the stability and shape of a feature could change quickly in this period. As development progresses and features become more stable, the focus shifts to wider scale effectiveness testing, often through Origin Trials, to understand the performance of the feature against its intended use cases at scale. Both the functional and effectiveness testing will be done in compliance with our <a href="#">commitments to the CMA</a>. <b>In particular, the commitments set out Development and Implementation Criteria against which the PS technologies must be evaluated through effectiveness testing.</b> Read more about <a href="#">how we collaborate with stakeholders</a> to discuss, test, and adopt privacy-preserving technologies.</li> </ul> </li> </ul>
August Timeline Updates	<ul style="list-style-type: none"> <li>• No updates</li> </ul>
September Timeline Updates	<ul style="list-style-type: none"> <li>• “Bounce Tracking Mitigations” added to the timeline under “Early Phases.”</li> </ul>

# Taking into account observations made by third parties

As part of its commitments to the Competition and Markets Authority, Google has agreed to publicly provide quarterly reports on the stakeholder engagement process for its Privacy Sandbox proposals (see paragraphs 12 and 17(c)(ii) of [the Commitments](#)). These Privacy Sandbox feedback summary reports are generated by aggregating feedback received by Chrome from the various sources as listed in the [feedback overview](#), including but not limited to: GitHub Issues, the feedback form made available on [privacysandbox.com](https://privacysandbox.com), meetings with industry stakeholders, and web standards forums. Chrome welcomes the feedback received from the ecosystem and is actively exploring ways to integrate learnings into design decisions.

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

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

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

Feedback received recently may not yet have a considered Chrome response.

## Glossary of acronyms.

W3C - [World Wide Web Consortium](#)

PatCG - [Private Advertising Technology Community Group](#)

IETF - [Internet Engineering Task Force](#)

DSP - Demand-side Platform

SSP - Supply-side Platform

OT - [Origin Trial](#)

UA - [User Agent string](#)

UA-CH - [User-Agent Client Hints](#)

IP - Internet Protocol address

WIPB - [Willful IP Blindness](#)

IAB - [Interactive Advertising Bureau](#)  
 openRTB - [Real-time bidding](#)  
 CHIPS - [Cookies Having Independent Partitioned State](#)  
 FPS - [First-Party Sets](#)  
 FedCM - [Federated Credential Management](#)  
 IDP - Identity Provider  
 RP - Relying Party  
 TPAC - [Third Party Advantage Conference](#)

## General feedback, no specific API/Technology

Feedback Theme	Summary	Chrome Response
(Also reported in Q2) Usefulness for different types of stakeholders	Concerns that the Privacy Sandbox technologies favor larger developers and that niche (smaller) sites contribute more than generic (larger) sites.	<p><i>Q3 Update:</i></p> <p>Google has committed to the CMA to design and implement the Privacy Sandbox proposals in a way that does not distort competition by self-preferencing Google's own business, and to take into account impact on competition in digital advertising and on publishers and advertisers, regardless of their size. We continue to work closely with the CMA to ensure that our work complies with these commitments.</p> <p>As testing of the Privacy Sandbox progresses, one of the key questions we will assess is how the new technologies perform for different types of stakeholders. <a href="#">Feedback</a> is critical in this respect, especially specific and actionable feedback that can help us further improve the technical designs.</p> <p>We have worked with the CMA to develop our approach to quantitative testing, and are supportive of the CMA publishing a note on experiment design to provide more information to market participants and an opportunity to comment on the proposed approaches.</p>

(Also reported in Q2) Documentation requests	Requests for more resources detailing how to manage testing, analysis, and implementation	<p><i>Q3 Update:</i></p> <p>We appreciate that developers have found our current material helpful, and are committed to providing more material over the coming weeks and months so developers can continue to understand how the new technologies can work for them.</p> <p>We've also held public developer office hours sessions to share best practices and demos, along with Q&amp;A sessions with product and engineering leads to allow for live discussion/questions.</p>
Cross-browser support	Other browser vendors adopting the Privacy Sandbox APIs.	Other browser vendors, such as Apple, Mozilla, and Microsoft, are active participants in the public forums where privacy principles and browser-based approaches are being discussed. We're encouraged by the collaborative discussions in forums like the recent W3C Annual TPAC meeting and ongoing W3C PATCG forums where we see signs of convergence.
Platform differences	Request to align feature sets across web and Android as much as possible to help reduce resources needed for the transition.	We are working hard to align our approaches across Chrome and Android to avoid creating confusion/fragmentation across the industry. Any differences in our approach will largely be due to necessary technical differences between the web and mobile app platforms that developers will already be taking into account.
Resources to test Privacy Sandbox APIs	Difficulties allocating enough resources to test the Privacy Sandbox APIs given the current economic headwinds.	Google is continuously improving the documentation and support available to testers to ease the complexity and aid in adoption of the APIs. These efforts include: API-specific mailing lists, open office hours, and ongoing updates on <a href="https://developers.chrome.com">developers.chrome.com</a> .
Sandbox API Opt-out Signal	Request to provide a 'user has opted out of sandbox APIs' signal, which ad tech and websites can use.	We have seen many historical cases where web sites react to user choices like "turn off third-party cookies" by pressuring the user to change their settings, sometimes including blocking website access unless they do. An opt-out signal may also be used as an additional signal for fingerprinting. At this

		point in time, Google does not intend to provide an opt-out signal
(Also reported in Q2) Clearer timelines	Clearer, more detailed release schedules	<i>Q3 Update:</i> As explained in the Changes in response to feedback section below, Google updated the Privacy Sandbox timeline in July to give the market additional time for preliminary testing and feedback, as well as more time to test once the Privacy Sandbox APIs are fully launched before third-party cookies are deprecated.
(Also reported in Q2) Third-party cookie deprecation timelines	Requests to avoid further delay for 3rd party cookie deprecation	<i>Q3 Update:</i> In July, Chrome announced an updated timeline for third-party cookie deprecation reflecting our commitment to act responsibly given the complexity of the technologies and their importance to the ecosystem. Feedback from regulators and the industry were taken into account before this change, and we continue to work closely with all stakeholders.
First-party cookies	Are restrictions on first-party cookies also being proposed? Concerns about utility and functionality that would arise if so.	We have not considered any first-party cookie restrictions. The Privacy Sandbox's focus is on deprecating third-party cookies.

## Show Relevant Content & Ads

### Topics

Feedback Theme	Summary	Chrome Response
(Also reported in Q2) Usefulness for different types of stakeholders	Concerns have been raised about the usefulness for sites depending on their level of traffic or how specialized their content is.	<i>Q3 Update:</i> The usefulness of the API will be explored through testing. As required under paragraph 17.c.ii of the Commitments, Google will share with the CMA the results of such tests. Chrome expects the taxonomy and other parameters to evolve based on testing results. The evolution of the taxonomy or

		parameters may not require backwards incompatible changes. Further, Chrome expects feedback to continue influencing the Topics API evolution after third-party cookie deprecation.
Privacy/Policy	Request to remove per-caller topic filtering requirement.	Based on feedback from privacy KOFs, privacy advocates, security experts, digital rights groups, and others in the ecosystem, Chrome chose this design to give access to information only to those that otherwise had such access. The reasons for this included, but were not limited to, limiting incremental cross-side data leakage; ensuring transparency and explainability; adopting an approach that is simple to implement and describe; and limiting the risk of fingerprinting. Publishers and third parties that receive Topics could decide for themselves what information they will share with parties on their site. If third parties do share this information, Chrome strongly encourages them to be transparent to users about such sharing, and offer them controls.
Miscategorized sites	Sites are miscategorized to the wrong topic, which may result in inaccurate ads targeting.	<p>Sites are classified through a combination of a human-curated override list, containing the most popular sites, and an on-device ML model. Chrome continues to evaluate options for sites to contribute to Topics classification. Any utility improvements must be weighed against the privacy and abuse risks. For example, a few of the risks include:</p> <ul style="list-style-type: none"> <li>- sites using self-labelling as a method to encode different (and potentially sensitive) meanings into topics;</li> <li>- sites misrepresenting their topics for financial gain;</li> <li>- sites attacking topics in order to blunt its usefulness for others (e.g., spamming the user's topics with</li> </ul>

		<p>meaningless noise).</p> <p>The public can inspect these components, with tooling available via a <a href="#">chrome://topics-internals</a> or this <a href="#">colab</a>. Through testing, we expect classification to improve over time, and we <a href="#">welcome feedback</a> of examples of sites that may be miscategorized.</p>
Access requirements	Current Topics requirement for DOM entity on-page as a script or iframe in order for access may lead to undesirable behaviors by players in the ads ecosystem.	We have merged a <a href="#">change on the Github explainer</a> . We intend to support Topics in HTTP headers.
Topics taxonomy not granular enough	Current topics classifications are too broad, and does not include more granular topics, such as regional topics.	<p>Improvements to the taxonomy are an ongoing effort, and we expect the taxonomy to evolve with ecosystem testing and input.</p> <p>We are actively <a href="#">seeking feedback</a> on the taxonomy that would be most useful for the ecosystem. In evaluating whether to expand the number of topics or include more granular topics, there are a few considerations including 1) potential privacy implications (e.g. more topics may introduce fingerprinting risk) and 2) ability to retrieve previously observed topics (e.g. with more topics, there may be less of a chance that an ad-tech has seen the chosen topic in the past). Expanding on #2, Google seeks to maximize callers' ability to retrieve previously observed topics, within the existing filtering requirement, with the goal of achieving both utility and privacy.</p>
Topics limit	Three topics per website is too little information for advertisers to serve ads to.	Feedback from the ecosystem, especially testing results from our Origin Trials, will continue to influence the evolution of the API. It is worth noting that Topics is expected to supplement other signals like contextual to help find an appropriate advertisement for

		the visitor. So, there can be more information available to the advertiser beyond topics.
(Also reported in Q2) User controls and safety	Certain topics may be proxies for sensitive groups and users need more controls to prevent negative outcomes.	<i>Q3 Update:</i> Topics represent a significant step forward for user control and transparency. Users will be able to opt out of topics, review the topics that have been assigned to them, remove topics, and understand which companies are interacting with their topics on a given page. In addition, users can also clear their Topics by deleting their browsing history, from which topics are derived. These controls are currently implemented on the Chrome browser at the device level. We welcome continued discussion regarding more advanced user controls, such as those suggested by developers; however we need to make sure that new additions are well calibrated to address the concerns raised and don't result in making piecemeal changes.
Impact on SEO	Publishers adjusting their website's hostnames to better reflect Topics may negatively impact SEO.	We would caution sites against changing their hostnames solely for the sake of Topics. It's true that a site may be able to influence its assigned topics in this way. But the benefits to publishers of doing so are unclear at best, and it would undermine the value of Topics for the entire ecosystem if sites try to "game" the classification model. Topic assignments are also not fixed; we expect the taxonomy to continue to evolve with testing and input. In connection with this testing, we <a href="#">encourage feedback</a> , including any examples of sites that may be miscategorized.
Fraud & Abuse	Have a way for the buy-side party to verify that the topic they see is actually generated by the browser.	We appreciate the suggestion to support a mechanism for ad tech buyers to verify the topics passed by sellers in programmatic advertising auctions. We encourage

		the ecosystem to contribute to the active discussion <a href="#">here</a> . While we are currently focused on other, higher priority improvements, we recognize that this could be an important future addition to the design.
Fraud & Abuse	Allow for public review of parties that are legitimate users of Topics data, through the same kind of public posting and review that a first-party set would be subjected to.	We appreciate the suggestion and agree that public accountability is an important tool for helping achieve the goals of the Privacy Sandbox. Topics API calls are inherently public, since anyone can visit a site and observe a domain's calls to the JavaScript API. Individuals and organizations can therefore view the relevant activity and assess which sites are using Topics and how. We believe that this is a better approach than making assessments of a site's "legitimacy" part of the functionality of the Topics API itself.
Impact on first-party signals	Topics signal may be highly valuable and as a result devalues other first-party interest-based signals.	We believe interest-based advertising is an important use case for the web, and Topics is designed to support that use case. As described above, other ecosystem stakeholders have expressed concerns that Topics may not be useful enough to provide value. In all cases, improvements to the taxonomy are an ongoing effort, and we expect the taxonomy to evolve with ecosystem testing and input.

## FLEDGE

Feedback Theme	Summary	Chrome Response
FLEDGE Auction	How can SSPs format data sent to Google Ads to bid on a FLEDGE auction.	Companies that are participating in testing are encouraged to publish documentation about their testing plans and work together where appropriate.

		<p>We have worked with the CMA to develop our approach to quantitative testing, and are supportive of the CMA publishing a note on experiment design to provide more information for market participants who plan to engage with trialling and an opportunity to comment on the proposed approaches.</p> <p>The Ad Manager team has posted documentation for sellers that are interested in testing FLEDGE with publishers that use Ad Manager as their ad server <a href="#">here</a>.</p> <p>There is additional technical detail outlined <a href="#">here</a>.</p>
FLEDGE in nested Fenced Frames	Fenced frames allow for less restrictive testing, while restricting more in an undefined future. This unknown timeline presents a challenge to the ecosystem.	Companies can test FLEDGE with Fenced Frames today. To provide an easier onboarding option, companies can choose to first implement FLEDGE. After implementing FLEDGE, they can test Fenced Frames with their FLEDGE design.
Data handling policy	What is the data handling policy for interest groups / FLEDGE?	<p>In the FLEDGE design, all data stored in interest groups, or about what people are in what interest groups, remains on-device. None of this data is sent to a Google server.</p> <p>Some privacy protections that Chrome plans for FLEDGE do involve interaction with a Google-run k-anonymity server. That interaction is being carefully designed to avoid sharing information about users, and to run in a trusted execution environment (TEE) to ensure parity of information across the ads ecosystem.</p> <p>Google has committed to the CMA to design and implement the Privacy Sandbox proposals in a</p>

		<p>way that does not distort competition by self-preferencing Google's own business, and to take into account impact on competition in digital advertising and on publishers and advertisers. We continue to work closely with the CMA to ensure that our work complies with these commitments.</p>
Age policies	How does Chrome ensure that audiences created by FLEDGE are complying with age restrictions?	<p>Publishers and advertisers are best positioned to assess whether the audiences they create using FLEDGE comply with applicable law. To further protect users, the Privacy Sandbox APIs will not be active for any users signed in to Chrome if the age associated with their account is under 18 years old, even during the testing period. (For signed-out users, Chrome doesn't collect profile signals that would allow the browser to infer user age.)</p>
FLEDGE Key/Value Services	More clarity on what FLEDGE Key/Value service will allow, such as number of keys and how often they can be updated.	<p>Companies using FLEDGE can have as many keys as they can fit in RAM. For more details, please refer to the explainer <a href="#">here</a>.</p> <p>We are looking at providing a faster path to modify data and welcome suggestions for any requirements.</p>
Testing	Hard to test FLEDGE with Google Ads	<p>Refer to Google Ads <a href="#">onboarding documentation</a> on how to best participate and test in the origin trial.</p>
Bidding and Auction Services API	What is Google's direction for the Bidding and Auction Services API? Will it be prioritized above or below the Chrome browser FLEDGE on device auctions?	<p>We remain committed to the current FLEDGE on-device bidding design. The Bidding and Auction services have been proposed to explore possible solutions to support a subset of use cases where the computational power or network speed of the device may be limited.</p>
Aggregate reporting	Request to support aggregate	<p>We plan to publicly share more on</p>

	reports based on all signals available to generateBid.	this soon.
Contextual Ads	Serving contextual ads with FLEDGE.	We have considered this option and for the reasons explained in this <a href="#">discussion</a> we would not currently recommend using FLEDGE for contextual ads.
Testing in real world	Guidance on how to isolate FLEDGE from third-party cookies for real-world testing.	<p>We are investigating ways to provide test populations.</p> <p>We have worked with the CMA to develop our approach to quantitative testing, and are supportive of the CMA publishing a note on experiment design to provide more information for market participants and an opportunity to comment on the proposed approaches.</p>
Testing FLEDGE and Attribution Reporting API	What is the best way to implement Attribution Reporting API with FLEDGE? Is it a good idea to separate FLEDGE & Attribution or test together?	We'll eventually support testing both FLEDGE and Attribution Reporting API as an integrated solution, but we encourage developers to first test Attribution Reporting API independently and then with FLEDGE when the integration is complete.
Bid price visibility	Request to obfuscate bid prices.	It is possible to set breakpoints within <code>generateBid()</code> or <code>scoreAd()</code> to access bid values from DevTools. The Chrome team has considered the narrow attack vector raised in this feedback on FLEDGE. However, Chrome's security and privacy models consider users trusted to do whatever they want with information on their own device, and consequently there is no feasible way to hide the bid data as requested.
Documentation requests	Documentation and examples for testing in a live ecosystem.	We appreciate that developers have found our current material helpful, and are committed to providing more material over the coming weeks and months so developers can continue to understand how the new

		<p>technologies can work for them.</p> <p>We've also held public external developer office hours to share best practices and demos along with Q&amp;A sessions with product and engineering leads to allow for live discussion/questions.</p>
Private Aggregation API	Request for more information on the Private Aggregation API?	A <a href="#">public explainer</a> is available with the latest information we're able to share at this time. More documentation will be provided as this API is developed and use cases defined.
Data latency	Will the FLEDGE Key/Value server data retrieval be real time?	A small amount of staleness on the order of minutes, not hours may be expected before updated data can be returned by the server for queries, as explained <a href="#">in an open GitHub Issue</a> . We are also looking for <a href="#">developer feedback</a> .
Bidding and Auction services	Will bid prices be hidden from the user if bidding and auction (B&A) services are used?	<p>For the B&amp;A server-side approach, the individual bid price is not visible to the user, since the bid request is made from the SSP auction service directly to the DSP auction service, and therefore not available in the browser anymore.</p> <p>However, the winning bid price will still be visible to the browser (discussed in more detail above, regarding requests to obfuscate bid prices).</p>
Bidding and Auction services	How can we load balance bidding and auction services?	We currently don't have any guidance on load balancing, but it is an important concern from the perspectives of both performance and privacy. We will provide more details in the future.
FLEDGE limits	Request to increase the joinAdInterestGroup duration cap from 30 days to 90 days.	We feel the 30-day data retention timeframe is in line with other Privacy Sandbox advertising APIs, like the 30-day limit in Attribution Reporting and the 3-week look back in Topics. This timeframe addresses both the needs of ad

		<p>tech and users' privacy expectations.</p> <p>However, we welcome further feedback as we continue to discuss the issue <a href="#">here</a>.</p>
Shared Storage in FLEDGE	Is it possible to use the Shared Storage API in FLEDGE?	We intend to support the Shared Storage API in FLEDGE in the future and are working to make this available in an upcoming Origin Trial.
Frequency control by clicks	Is it possible to have frequency capping by clicks (not wins) in FLEDGE?	FLEDGE does specify that a Fenced Frame can call <code>navigator.leaveAdInterestGroup()</code> (with no parameters) to leave the interest group that caused the ad to be shown; this call could be done the first time that a click is received to prevent future bidding, as a form of frequency capping. At present, this solution would not work for capping after more than one click.
FLEDGE in nested Fenced Frames.	Unable to report clicks via Fenced Frame Ads Reporting, if they happen on a nested Fenced Frame.	We have published a proposal to fix the issue <a href="#">here</a> .
Measurement	Need guidance on how to collect latency data on bidders in a FLEDGE auction.	We are working to publish a performance measurement doc soon.
Reporting	How will FLEDGE reporting be handled?	<p>FLEDGE reporting on Win, Auction Result, Event e.g. clicks will be available through FLEDGE APIs such as <code>reportResult()</code>. On reporting with the ad conversion, the integration with Attribution Reporting API will be independent from FLEDGE, but there are ongoing discussions with the ecosystem on possible approaches.</p> <p>The Private Aggregation API can also be used to report auction results from within the isolated execution environments. See explainer <a href="#">here</a>.</p>

Interest group size	Is there any way for ad-techs to check the size of an interest group (i.e. the number of users in the group)?	<p>Interest group membership is stored by the browser, on the user's device, and is not shared with the browser vendor or anyone else.</p> <p>However, an interest group owner can theoretically track every call to <code>navigator.joininterestgroup(...)</code>. Tracking this call does not guarantee the exact size of an IG (as users can leave a group at any time), but it gives the owner an upper limit and an approximation of what the size could be.</p>
Performance	Is Bidding JS/WebAssembly code compiled at every auction?	Bidding JS/WebAssembly code is compiled once during every auction.
Performance	What is the scope of <code>biddingDurationMsec</code> ?	<code>biddingDurationMsec</code> includes compiling script time. It does not include download time, wasm compile time, network time; fetching time from key value server or anything ahead of JS compile.
Customization	Is it possible to update <code>adComponent</code> so that it is customized for the user?	<code>adComponent</code> can be updated when Interest Groups are updated either by the caller when calling <code>joinInterestGroup</code> or when Chrome makes a call to <code>dailyUpdateURL</code> . This allows the caller to update the <code>adComponent</code> based on knowledge of the user from the current site or based on k-anonymous information, respectively. You can find the original proposal of Product-level turtledove <a href="#">here</a> which includes some analysis by RTB House on impact on core metrics for the recommendation use case.
Interest group	Is it possible for an interest group owner to conditionally remove certain users?	Interest group membership is stored only on the user's browser and can only be removed on the user's side (e.g. by clearing site data).

		However, it is possible for an interest group owner to call <code>navigator.leaveAdInterestGroup()</code> (with some conditional logic around it), if the user returns to a page that is under the control of the interest group owner.
Performance	How to measure the performance of <code>generateBid</code> ?	Compile and execute time can be measured with <code>biddingDurationMsec</code> . Download time can be measured with <code>chrome://net-export</code> . In recent versions of Chrome, compile and execute time will show up in the DevTools Performance tab.
Frequency of interest group updates	What will be the frequency of the update of the interest group from the browsers?	For interest groups that have not been updated in the last 24 hours, Chrome attempts to update them when <code>navigator.updateAdInterestGroups()</code> is called or when they have had the chance to participate in an auction. For more details see explainer <a href="#">here</a> .
Aggregation Service Providers	When will other cloud providers be supported on Aggregation Service?	We currently do not have any update on the specific times but will share more once we do. Right now only AWS meets the aggregation service's security requirements.
FLEDGE Testing Timeline	How long will the FLEDGE be testing in BYOS? Will there be enough time to switch from the BYOS model to the TEE-based model?	To ensure that the ecosystem has sufficient time to test, we don't expect to require the use of the TEEs until sometime after third-party cookie deprecation. We will provide substantial notice for developers to begin testing and adoption before this transition takes place. We currently do not have any further updates but will share more once we do. Please find the latest information <a href="#">here</a> .
Data size limit	What is the data size limit for <code>wasm</code> in bidding function.	There is a requirement that interest group updates cannot result in an interest group that exceeds 50kb, as discussed <a href="#">here</a> , but the data size limit for

		wasn't is not yet defined so we would appreciate input on this topic.
Auction signals	Will there be a standardized data structure for auctionSignals?	This is not defined yet, but we are open to feedback.
Querying Ad Tech Servers	Is it possible to query ad tech server data in realtime from a K/V server?	No, K/V server runs in a trust model which enforces "No network, disk access, timers, or logging" to avoid leaking user data. Please see the trust model explainer <a href="#">here</a> for more detail.
Frequency of updating adComponents	Updating the adComponents field (currently only in IG setting) by user's browsing history is currently not possible	The Privacy Sandbox aims to support the needs of the web ecosystem without cross-site tracking, which means preventing access to browsing history. We recommend using alternatives such as Topics.
Auction results	Is there any way for ad-techs to know auction winning rates?	The auction result is reported by calling the reportResult() and reportWin() functions in the auction code provided by the seller and the winning buyer respectively, so each has an opportunity to perform logging and reporting about the auction result.
(Also reported in Q2) Support for negative Interest Group targeting	An API to support negative interest group targeting: showing ads only if a user does not belong to an interest group.	<i>Q3 Update:</i> We have shared a new <a href="#">proposal</a> and are seeking feedback.

## Measuring Digital Ads

### Attribution Reporting (and other APIs)

Feedback Theme	Summary	Chrome Response
OT requirements	Remove Permission-Policy restrictions during / for the OT only.	Please see our <a href="#">announced changes</a> to Permissions-Policy during testing. The underlying stakeholder concern addressed by this change, is allowing DSPs to test the API on a higher amount of cross-origin iframes. Originally, DSPs needed to coordinate with

		Publishers/SSPs to make sure the right permission policy was set in order to test the API on cross-origin iframes, but with this change DSPs will be able to call the API by default and SSPs/Publishers can disable the API if needed during the Origin Trial.
Noise	Feedback that the level of noise is too high and it is impacting the usefulness of the reporting.	We <a href="#">welcome feedback</a> regarding noise, which we will use to determine how to set certain noise related parameters. We are also looking to publish more resources, tools, and other docs to help testers with this.
Cross-domain conversions	How to track the conversions that are cross domain, such as with 2 or more destinations?	We are <a href="#">currently discussing and seeking feedback</a> on this question.
Debugging requirements	Request to allow developers to check the remaining privacy budget when deploying / testing for summary report?	You can track this feature request <a href="#">here</a> .
API usage policies	Feedback suggesting policies for who can use a given API based on restrictions for things like fingerprinting	This is a very interesting idea and something we would be happy to engage in further with both other browser providers and the broader web ecosystem.
Expiry setting in conversion report	Request to support report filter / expiry for less than 24 hours.	Hour-level expiries are a source of privacy concern as it enables ad-tech to know exactly which hour a user visits the advertiser site. Day level expiry will allow ad-tech to filter out invalid impressions without determining which hour the user visited the site.
OT token expiration	Request to extend the validity of the existing OT tokens to reduce operational overhead.	We recognize that tokens must be renewed and are working to make it easier for developers and provide additional notice.
Regional support	Aggregation service currently does not support all regions.	This is a current limitation for beta. We expect to support additional regions as testing progresses, but there isn't yet a clear timeline for this.
Event level reporting delay	The delay of 2-30 days in event	We have shared a proposal <a href="#">here</a>

	level reporting may be too long for certain use cases.	to allow ad techs to control when event level reports are sent via expiry. The default is 30 days, but it can be set shorter.
(Also reported in Q2) Multi-touch attribution	Allow multi-touch attribution, such as cross device or cross apps.	<i>Q3 Update:</i> Current methods of multi-touch attribution require deterministically tying together a user's impressions (and therefore identity) across different websites. As a result, this functionality in its current form does not align with the goals of the Privacy Sandbox, which aims to support key ads use cases without cross-site tracking.
FLEDGE & Attribution Reporting integration timeline	What is the timeline for FLEDGE and attribution reporting API integration?	We currently do not have any updates to share, but will provide more information publicly once we are able to commit to a specific timeline.
Multiple Trigger Types	Request for more flexibility in trigger registration.	We have <a href="#">proposed</a> a deduplication system for aggregate API that will give ad-techs more flexibility in how they control the event-level and aggregatable reports.
Measurement	Request to receive measurement data on whether inventory is performing well.	We appreciate the feedback and are seeking additional clarity on the use case(s) for this request.
Conversion expiry	Request to support conversion expiry on trigger tag instead of just the source tag.	We appreciate the feedback and are seeking additional clarity on the use case(s) for this request.
Batch reporting	Request for additional measurement in batch reporting.	We appreciate the feedback as we continue to think about the impact on aggregation service. We are interested in hearing how ad tech are thinking about batching reports and their expected frequency as well as any feedback on how batching strategy changes throughout the year.
Epsilon	When will the value of epsilon be determined?	We are actively working with ecosystem testers to finalize the epsilon value and how it will be implemented in GA. The value will

		be visible in public, along with the discussion that led to the decision of the value. If you have any feedback, please post it in this GH <a href="#">issue</a> .
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Limit Covert Tracking

### User Agent Reduction

Feedback Theme	Summary	Chrome Response
Deployment Dependencies	Addressing Structured User Agent (SUA) deployment dependencies.	We have rolled out "Phase 4", aka minor version reduction to 100% of Chrome users in versions 101 and above. See update <a href="#">here</a> .
Testing	Request to extend User-Agent Reduction Origin Trial from Meta.	We <a href="#">extended the Origin Trial</a> , and <a href="#">obtained permission</a> to remove traffic limits to accommodate larger sites. The relaxed traffic limits apply to any site, large or small.

### User Agent Client Hints

Feedback Theme	Summary	Chrome Response
(Also reported in Q2) Anti-Fraud / Anti-Abuse concerns	Certain features that might be lost via UA-CH: Click redirect tracker, and fraudulent clicks.	<p><i>Q3 Update:</i></p> <p>We have received positive feedback from companies reporting that they did not see any adverse effects on their anti-fraud pipelines (Results <a href="#">here</a> and <a href="#">here</a>).</p> <p>The team is continuing to investigate these potential issues with anti-fraud and measurement stakeholders.</p>
Permission-Policy	Is Permission-Policy cached?	Permission-Policy is not cached as explained in <a href="#">this Github issue</a> .

## Gnatcatcher (WIP)

Feedback Theme	Summary	Chrome Response
Geolocation use cases	Gnatcatcher may prevent legitimate geolocation use cases from working in the future, such as content personalisation based on geolocation.	We are working with stakeholders to ensure that Chrome continues to support legitimate use-cases of IP addresses.

## Strengthen cross-site privacy boundaries

### First-Party Sets

Feedback Theme	Summary	Chrome Response
Policy	Concern that FPS is not consistent with the CMA commitments' provisions regarding "Applicable Data Protection Legislation," on the basis that GDPR does not impose a limit on the number of sites in a set while FPS envisages a limit of 3.	Google has committed to the CMA to design and implement the Privacy Sandbox proposals in a way that does not distort competition by self-preferencing Google's own business, and to take into account impact on competition in digital advertising, publishers and advertisers as well as impact on privacy outcomes and compliance with data protection principles as set out in the Applicable Data Protection Legislation. The concern expressed does not disclose any incompatibility with GDPR. We continue to work closely with the CMA to ensure that our work complies with these commitments. Further details are included in the "Changes in response to feedback" section below.
Documentation	Request for additional examples and to update existing explainers.	The examples in our explainers are under review, and will clarify or remove any as needed.
Preference sharing	Proposal to make preferences across the same party sets.	We welcome the feedback and are actively discussing the idea <a href="#">here</a> .
Enforcement	Transparent enforcement processes have a risk of abuse by bad actors.	We appreciate the feedback and are actively engaged in

		conversation with stakeholders on GitHub (considering points raised in <a href="#">this issue</a> and looking to incorporate suggestions raised in <a href="#">this issue</a> ) and other forums to assess this risk and identify potential mitigations.
Common ownership	Proposal for machine-readable declaration for common ownership.	Input on our <a href="#">proposal</a> is welcomed and encouraged.
Subdomains ownerships	Should different subdomains with different data controllers, different privacy policies or operated by different entities be part of the same First-Party Set?	Based on feedback, we plan to remove the common eTLD use case.
Abuse Mitigation	Request for more details about the abuse mitigation measures.	The management of the process is under consideration and more details will be shared in the coming months.
Potential attack vector	A deceptive associated set for easily-findable pages could be used to drive traffic to other pages that are deceptively presented as independent.	We are actively gathering public input and investigating potential ways to address <a href="#">this issue</a> .
Set validation	Validating the set via consented common policies.	Various members of the web standards community and broader ecosystem have <a href="#">pointed out it is not feasible</a> .
Domain limit	Request for expanding the number of associated domains.	We are actively in discussion regarding the domain limit in FPS, and would appreciate more feedback from the community on the number of associated domains they require for their use cases.
Subset service interaction	Concern regarding service and associated Subset Interaction.	We appreciate the feedback and will look into making this more explicit in the future specs.
(Also reported in Q2) Improving privacy	Too many sites in the same set could result in similar outcomes to third-party cookies.	<i>Q3 Update:</i> The latest proposal suggests a limit of three domains for the “associated” subset (which does not include ccTLDs and service domains). Chrome is actively engaging with the ecosystem to determine whether this limit is appropriate.

(Also reported in Q2) Common privacy policy requirement	It is infeasible to maintain a common privacy policy across all products, and jurisdictions that need to be part of the same set.	<i>Q3 Update:</i> A common privacy policy is no longer a requirement to be part of the same set.
------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------

## Fenced Frames API

Feedback Theme	Summary	Chrome Response
Why a new element instead of attributes on iframes?	Question regarding proposal Fenced Frame instead of existing iFrame proposals.	We welcome the feedback and are open to ideas on how to converge the current state of things as discussed <a href="#">here</a> .
Intersection observer in fenced frames	Questions regarding the viewability of information inside a Fenced Frame.	This is in active discussion and in the commenting period <a href="#">in this doc</a> and on <a href="#">GitHub</a> . We welcome partners to share use cases with us to better understand how to support.
Support Video & Native inventory	Does Fenced Frames support Video & Native inventory?	In terms of video playing capabilities, Fenced Frames do not differ from iframes and that's why it isn't explicitly called out in any public documentation. If any issues with video ads are being seen, it would be helpful to <a href="#">file feedback</a> in order for us to investigate further.
Web Bundles	Will Ad serving / rendering by Web bundles become a requirement in the future with Fenced Frame x FLEDGE?	The long term goal is to support Web Bundles for rendering ad content in a fenced frame. However, the current implementation of FLEDGE does not support this, and requires rendering an HTML resource retrieved from renderUrl.
Asset dimensions	Request for render_url to support a macro for the slot height and width so that we can respond with an appropriately sized creative	This is actively being discussed <a href="#">here</a> .

## Shared Storage API

Feedback Theme	Summary	Chrome Response
FLEDGE integration	How will Shared Storage & FLEDGE be integrated?	While we are not currently pursuing this, we are interested in exploring this

		idea if we can ensure the preservation of privacy protections. We encourage interested parties to file suggestions for potential use cases this proposal could support in the Shared Storage <a href="#">github repository</a> or the FLEDGE <a href="#">github repository</a> .
Data retention	Clearing Shared Storage reduces utility. Have extensions to the retention period or ability to delete individual key/values been considered as alternatives?	We are always looking to balance user privacy and utility tradeoffs. We are open to feedback on adjustments, and encourage partners to <a href="#">provide more feedback</a> and details as they test shared storage.
Negative Signal	Negative signal from Mozilla regarding the Shared Storage proposal.	We thank Mozilla for their careful review of our proposal. We plan to respond to their feedback in the near future.

## CHIPS

Feedback Theme	Summary	Chrome Response
Partitioned requirement	Add explicit behavior requirement for "Partitioned" attribute on First-Party cookies.	We have discussed this on a PrivacyCG call, and have followed up on the <a href="#">GitHub issue</a> with notes. We are continuing to work with browsers, developers and the privacy community to align on a behavior and specify it.
Authenticated embeds	CHIPS may affect current SSO sign in flow due to different partitioning impacting authenticated embeds.	We are aware of the authenticated embeds use case and are working to explore solutions.
Cookie Partition Limit	Concern that the current 10 cookie limit may not be enough for certain use cases.	We're moving away from a limit on the number of cookies to a 12kb memory limit. Doing so allows us to address concerns on the cookie limit while ensuring

		performance and browser memory footprint is not adversely impacted.
Origin Trial Timeline	Extend OT follow the removal of the hostname boundedness requirement.	We have extended the origin trial deadline following feedback from the ecosystem.
Testing limitations in Chrome	Possibility of testing CHIPS in Firefox due to current limitation in Chrome.	Firefox's implementation is approximately different, Chrome has a lower cookie limit, and CHIPS is an opt-in mechanism, but Firefox is partitioned by default.
(Also reported in Q2) Authenticated embeds	Is sign-on state preserved with CHIPS?	<i>Q3 Update:</i> Signed in state is not currently preserved, but it is not the intended use-case for CHIPS. We are aware of the authenticated embeds use case and are working to explore solutions.

## FedCM

Feedback Theme	Summary	Chrome Response
(Also reported in Q2) Potential attack vectors	Potential attack vectors via link decoration and timing attacks.	<i>Q3 Update:</i> We have worked with Mozilla to arrive at a common understanding of how to address the timing attack problem and the details are <a href="#">here</a> . We are now prototyping this architectural change and expect to be running experiments in the next few quarters.
Identity providers	Account chooser: single identity provider. Request to allow multiple identity providers.	We have worked with Browser vendors and the FedID CG on how to achieve allowing multiple identity providers and have arrived at a formulation that seems worth trying. The description of the proposal is <a href="#">here</a> and we expect to

		develop prototypes and run experiments in the next few quarters.
Known issues with Federation	Request to enumerate cases where federation might run into trouble with third-party cookie deprecation.	The FedID CG has a work item which is to enumerate the ways in which federation breaks <a href="#">here</a> and <a href="#">here</a> . They are also building a decision matrix to map breakages to Web Platform APIs <a href="#">here</a> .
Nounce parameter	Could Nounce parameter affect sign in flow?	This could be considered cross-site tracking, but we are still gathering input and analyzing how to treat such cases.
User consent	Linking different relying parties (RPs) and user consent for each origin.	This spec cannot control how origins within the same domain share cookies. The spec allows idtoken from the IDP origin to the RP origin, but it is up to the RP to choose whether the sign in state of the user should be stored in a cookie locked to that single origin or a cookie shared with origins within the same domain.
IDP account portability	User option to migrate IDPs if they choose when transferring between two IDPs.	That seems like something that the user would need to do directly in the sign up page of their new IDP of choice, not via the FedCM API.
Account deletion	IDP Revocation accounting for account deletion with the IDP.	This <a href="#">feature request is open</a> for input and under investigation.
UI Claim	Claims about browser-specific interface aspects.	See <a href="#">pull request</a> to address this.
IDP Referral Check	IDP checks for referrer of RP.	Added mandatory IDP referrer check to spec. See <a href="#">pull request</a> .
Sign in flow	Request for sign in flows to be customized based on RP preferences.	We welcome the idea and are <a href="#">actively discussing it</a> .

# Fight spam and fraud

## Trust Tokens API

Feedback Theme	Summary	Chrome Response
Fraud & Abuse	Tools to ensure that a bot has not tricked an issuer into giving it a token, that a bot has not taken over a token issued to a real user and to prevent bots from issuing malicious tokens?	While bots may be able to get tokens from an issuer, issuers are encouraged to have limits on how often they issue tokens and robust methods for issuing tokens and updating their issuance logic as malicious actors attempt to circumvent them. Issuers without robust enough logic in issuing tokens will likely become less trusted in the ecosystem as websites prioritize depending on more robust issuers.
Fraud & Abuse	Is there a way for a Trust Token redeemer to be able to specify that they will only accept Trust Tokens from specific entities?	Yes, this is possible. The <a href="#">Trust Token redemption</a> section in the explainer describes how this works.
Fraud & Abuse	Is there a way for a Trust Token issuer to define a list of redeemers and not allow anyone else to redeem tokens?	Not at present, but the team is investigating this use case.
Timeline	When will the Trust Token API be generally available?	As soon as we can commit to a timeline, we will share more information publicly.
(Also reported in Q2) Maintenance overhead	Not clear how long protocol versions will be supported.	<i>Q3 Update:</i> Additional support in the APIs to support multiple concurrent versions is being added to allow for graceful transition between versions, though timeframes for support / deprecation are still being worked out.

# Changes in response to feedback

Published every quarter, the “Taking into account observations made by third parties” is the most authoritative section about ecosystem feedback and Chrome’s attendant responses.

At the CMA’s request, Google describes in more detail below how certain updates it has made to the Privacy Sandbox proposals relate to ecosystem feedback. While updates to the Privacy Sandbox proposals are often based on a myriad of factors, this section is designed to illustrate how this feedback informs design decisions beyond the baseline provided for all feedback in the “Taking into account observations made by third parties” section.

**Update to First-Party Sets proposal and use of the Storage Access API.** In response to ecosystem and CMA feedback, Chrome has updated its FPS proposal with a shift in focus towards addressing specific use cases and surfacing relationships between domains, rather than establishing a single definition of a “First-Party Set”. Google originally contemplated a single definition that would allow the sharing of third-party cookies between a set that satisfied three criteria based on ownership, branding and a common privacy policy. Ecosystem feedback highlighted that, for some organizations that own multiple brands, branding decisions are taken differently per brand and it was difficult to know if they could align those decisions across all websites. There were also concerns about any general requirement for prominent branding on multiple domains and that changing site branding might require legal and other interventions. Publishers highlighted that they often have domain specific privacy policies because of differences in content or target audience e.g. for content for children.

In light of this feedback, Google had contemplated revising its original proposal by simply dropping the common branding and privacy policy requirements, leaving common ownership as the only relevant factor. After extensive discussions with the CMA on the application of the Development and Implementation Criteria foreseen in the Commitments, Google decided not to proceed with this idea. Instead, Google has moved to a proposal that separately addresses certain use cases (which naturally involve common ownership) and also provides for situations where browsers can understand the relationships between domains of multi-domain sites such that they can effectively present that information to the user. The new proposal addresses the ecosystem feedback by not requiring shared branding for all domains, and by not requiring a common privacy policy. Instead, it focuses on users’ understanding of relationships between associated domains, rather than ownership, together with a 3-domain limit.

On technical implementation, Google has replaced SameParty cookies with the Storage Access API to enable cookie access within a FPS. Feedback from the browser community noted that the SameParty cookie approach limited their ability to choose different user interaction models for their own browsers to gate access to the cookie information, which the adoption of Storage Access API facilitates. Many web developers rely on Storage Access API to ensure site functionality on Safari and Firefox. Consistent implementations

across browsers means less incremental work for developers and minimises friction for users.

**Expanding FLEDGE Key/Value server to allow user-defined functions to execute within a sandboxed environment.** To power FLEDGE's on-device ad auction, a limited number of real time signals (e.g. ad campaign budgets) must be made available to Chrome clients. To achieve this goal, a key part of the FLEDGE proposal is the building of a service—the FLEDGE key/value server—to transmit these signals to Chrome clients for usage in on-device auctions.

Initially, Google designed the FLEDGE key/value server to offer advertisers simple lookup functions; those necessary for the server to load data points like ad budgets from services external to the key/value server that must sometimes be updated quickly. Google received feedback from advertisers that have participated in FLEDGE trials indicating that such limited outbound calls may affect their ability to use FLEDGE for more complex ads bidding strategies, such as performing machine-learning model evaluation or dynamically generating budgets.

To better support use cases such as this, Google decided to publish an explainer stating its intent to change the FLEDGE key/value server to support advertiser-defined code executing within a limited-capability sandbox running within FLEDGE key/value servers.

At the same time, Google's goal is to preserve the FLEDGE privacy model of sites not being able to learn new information about a user's interests or browsing history from an ad auction. Google has put in place a number of protections to reduce the risk of data leakage out of the key/value server and plans to limit the metadata that the key/value server passes to user-defined functions from the current auction.

**Testing Timeline Extension.** After consultation with the CMA (see "Status Meeting" section below), on 27 July 2022 Google [published a revised timeline](#) extending the window for testing the Privacy Sandbox APIs. The new timeline envisages expanding the trial population throughout the rest of the year and into 2023, and by Q3 2023 launching the APIs for general availability in Chrome. Following the standstill foreseen in the Commitments, the plan is then to start phasing out third-party cookies in Chrome in the second half of 2024.

The extension of the testing window reflects consistent feedback from the web ecosystem that more time is needed to understand, test, and adopt the APIs. In particular, partner feedback indicates testing will take at least 6-9 months due to a number of factors, including securing resources and ramping up teams, coordinating with other ad techs and customers, and testing multiple APIs separately and in combination. Additionally, many partners have expressed a high interest in testing, but need between 1-3 months to prepare and set up. The new timeline allows for a longer testing period which will enable the collection of more performance data to inform the impact that the Privacy Sandbox APIs will have on publisher monetisation and advertiser utility. Most importantly, this longer testing period should allow for developers to further build and refine models that optimize performance of the APIs.

The revised timeline is also intended to provide greater clarity in an effort to meet requests from the ecosystem for increased transparency around the Privacy Sandbox milestones, so that they can forecast resource allocation for testing and provide feedback on the APIs.

## 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.

The parties have jointly reviewed and streamlined the process by which the CMA reviews Google announcements. For "High Priority" publications, i.e. new (or material changes to) GitHub explainers or blog posts and updates to the [privacysandbox.com](https://privacysandbox.com) timeline, Google shares the draft text with the CMA at least 3 working days before publication to allow for pre-review and comments. For all other modifications to explainers Google provides the CMA with weekly updates. For more routine process documentation, like Blink Intents, Google updates the CMA on a monthly basis.

On 7 September 2022 Google informed the CMA under paragraph 17(a)(i) of the Commitments that it was adding Bounce Tracking Mitigations to the Privacy Sandbox. Google also updated the [privacysandbox.com](https://privacysandbox.com) website to reflect this change. A GitHub explainer for Bounce Tracking Mitigations is available [here](#).

As discussed above in the Response to Feedback section, Google has updated its FPS proposal in response to feedback from the ecosystem and the CMA's intervention under the Development & Implementation Criteria. Regarding Privacy outcomes under paragraph 8(a) of the Commitments, Google has worked to align the designs of FPS with user expectations. This includes use-case specific rules for the inclusion of domains in an FPS (specific to particular use cases). For example, ccTLD and service use cases could have unlimited domains and would require common ownership as an abuse mitigation mechanism, while associated domains would focus on users' understanding of relationships between domains, not requiring ownership but instead have a 3-domain limit to mitigate abuse. Regarding Publisher outcomes under paragraph 8(c) of the Commitments, the 3-domain rule limits the potential for larger publishers to use cross-site cookies to generate advertising revenue, creating a better balance with smaller publishers, who can combine 3 separately-owned domains subject to user expectations.

## CMA concerns

The CMA has not during the relevant period expressed concerns for resolution pursuant to paragraph 17(a)(ii), or notified any such concerns pursuant to paragraph 17(a)(iii).

## Stakeholder concerns

The dialogue with the CMA is informed by feedback provided by stakeholders to the CMA (and to Google) and these points are captured in the table of feedback above. Among the points highlighted by the CMA as part of its discussions with Google (see Status Meetings section below) included the following:

1. Clarifying timelines including for testing and trialling;
2. Detailing design issues including in relation to Topics and Fledge;
3. Ensuring training about the Commitments for all staff working on Privacy Sandbox.

## Status Meetings

The Commitments provide for Google and the CMA to schedule regular meetings at least once a month (before the Removal of Third-Party Cookies), to discuss progress on the Privacy Sandbox proposals. Currently, Google and the CMA typically have one substantial technical meeting a month, updating on progress and addressing an agreed agenda of testing, targeting, measurement, boundaries and user control topics to assist the CMA to carry out the regulatory scrutiny and oversight foreseen in the Commitments, as well as one legal status meeting focusing on legal, procedural, and competition considerations. Google and the CMA collaborate on the agendas for each meeting to ensure that adequate attention is given to each topic. Additional meetings are held to discuss specific issues when the need arises. For example, Google and the CMA discussed the extension of the Privacy Sandbox timeline in detail before it was announced on 27 July 2022. The CMA pointed out that some stakeholders had concerns about Google's overall timetable and the risk that removal of third-party cookies could be delayed further, or alternatively, may come too soon.

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 the notification of concerns during the Standstill Period is not yet applicable, as Google has not entered the Standstill Period.

## Proposals covered by CMA Commitments

To aid transparency, Google sets out below the proposals covered by the CMA Commitments as of September 30, 2022. This list is based on Annex 1 of the Commitments

as accepted on 11 February 2022, reflecting any instances where the development of an API is discontinued, and / or an alternative API is developed (in accordance with Annex 1), including any successor technologies having the same objective as Alternative Technologies listed in Annex 1 (in accordance with paragraph 6 of the Commitments), and incorporating any changes to the Privacy Sandbox that are material to ensuring that the Purpose of the Commitments is achieved, as from the date they are notified to the CMA as part of the dialogue provided for at paragraph 17(a) of the Commitments.<sup>2</sup>

- Trust Tokens API
- Topics API
- FLEDGE API
- Attribution Reporting API
- First-Party Sets API
- Shared Storage API
- CHIPS API
- Storage Partitioning
- Fenced Frames API
- Network State Partitioning
- DNS-over-HTTPS
- Federated Credential Management (FedCM) Web Identity API
- User-Agent Reduction
- Gnatcatcher
- Privacy Budget
- Bounce Tracking Mitigations

## Compliance statement

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

---

<sup>2</sup> As noted in Google's May 2022 Progress Report, Origin-Bound Cookies were removed from the Privacy Sandbox timeline in February 2022.



COMPETITION AND MARKETS AUTHORITY  
Case 50972 - Privacy Sandbox  
Compliance Statement

I, Renée M. DuPree, Director, Competition and Compliance of Google LLC confirm that for the three months to 30 September 2022, 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 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