Privacy Sandbox Progress Report

Q2 Reporting Period – April to June 2022

Prepared for the CMA, 25 July 2022

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, details are provided in the blog posts entitled "Progress in the Privacy Sandbox" 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.[1] The summary below includes all Q2 2022 updates, covering the period from April 1 to June 30, 2022.

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

Privacy Sandbox Q2 2022 Timeline Updates	
April Timeline Updates	**Change "Testing" Tooltip to say:** All technologies for the use case are available for early testing and origin trials to gather feedback. To start testing, APIs may be available to a limited amount of Chrome traffic. This may happen at any point during the quarter. **Change "Transition Period: Stage 1" tooltip to say:** All technologies for each use case are launched in Chrome for general availability and are ready for adoption. This is the period for scaled business use case testing across multiple APIs, deeper integrations and ongoing refinement. Chrome will monitor adoption and feedback carefully before moving to the next stage. **Add "OT STARTED" for Federated Credential Management in Q2 2022** Tooltip Text: The origin trial has been open since Q2 of 2022. Register Now. **Topics: Change "OT Announced" to "OT Started"** Tooltip Text: **Topics API:** The origin trial for Topics API was announced in Q1 2022 and started in April 2022. Register Now. **FLEDGE: Change "OT Announced" to "OT Started"** Tooltip Text: **FLEDGE API:** The origin trial for FLEDGE API was announced in Q1 2022 and started in April 2022. Register Now. **Attribution Reporting: Change "OT Announced" to "OT Started"** Tooltip Text: **Attribution Reporting API:** The second origin trial for Attribution Reporting API, which includes support for aggregate measurement and view-through conversions, was announced in Q1 2022 and started in April 2022. Register Now.
May Timeline Updates	**Add FAQ:** Outside of Google, who does Chrome collaborate with to build the Privacy Sandbox technologies? Chrome works with a broad group of stakeholders throughout the web ecosystem – including web browsers, online publishers, ad tech companies, advertisers, developers, and users – to build and test Privacy Sandbox technologies. Additionally, Chrome continues to work with regulators, including the UK's Competition and Markets Authority in line with the commitments offered for Privacy Sandbox for the Web. • **Add FAQ:** What is the difference between functional testing and effectiveness testing?

	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 i ts intended use cases at scale. Both the functional and effectiveness testing will be done in compliance with our commitments to the CMA. Read more about how we collaborate with stakeholders to discuss, test, and adopt privacy-preserving technologies. • **Add "OT CLOSED"** label to Trust Tokens API, Q2 2022 ○ Trust Tokens API: The origin trial for Trust Tokens API ran from Chrome 84 - 101.
June Timeline Updates	**Add "OT Started" for Fenced Frames** Tooltip: **Fenced Frames:** The Origin Trial has been open since Q2 of 2022. Register Now. **Add "OT Started" for Shared Storage API** Tooltip: **Shared Storage API:** The Origin Trial has been open since Q2 of 2022. Register Now.

Taking into account observations made by third parties

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

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

More specifically, meeting minutes for web 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 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.

Feedback received after the end of the current reporting period 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

General feedback, no specific API/Technology

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Clearer timelines	Clearer, more detailed release schedules for the Privacy Sandbox technologies.	We set out our current plans for the deployment schedule on privacysandbox.com, and update it monthly. These take into consideration development time for both Chrome and web developers, as well as feedback we've received from the broader ecosystem on time needed to test and adopt the new technologies. Each technology goes through multiple steps from testing to release (launch) and the timing of

		each step is informed by what we learn and uncover in the prior step. While we don't have committed releases at this time, as we do, we'll be sure to update our public timeline on privacysandbox.com.
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.	We understand that some developers have concerns about the impact of the Privacy Sandbox technologies. Google has committed to the CMA not to design or implement the Privacy Sandbox proposals in a way that distorts competition by self-preferencing Google's own business, and to take into account impact on competition in digital advertising and on publishers and advertisers, as well as impacts on privacy outcomes and user experience. We continue to work closely with the CMA to ensure that our work complies with these commitments. 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. Feedback is critical in this respect, especially specific and actionable feedback that can help us further improve the technical designs.
Third-party cookie deprecation timelines	Requests to avoid further delay for third-party cookie deprecation	We have heard from some stakeholders who want Chrome to proceed with third-party cookie deprecation with no delay, and we have heard from others who believe more time is needed to test and adopt the Privacy Sandbox technologies. We are committed to proceeding responsibly given the complexity of the technologies and the importance to the ecosystem of getting things right. Feedback from the industry and from regulators has been critical to this process.
Third-party cookie deprecation timelines	Requests to delay third-party cookie deprecation, and to provide more time to test the APIs.	We have heard from some stakeholders who want Chrome to proceed with third-party cookie deprecation with no delay, and we have heard from others who believe more time is needed to test and adopt the Privacy Sandbox technologies. We are committed to proceeding responsibly given the complexity of the technologies and the importance to the ecosystem of getting things right. Feedback

		from the industry and from regulators has been critical to this process.
Documentation requests	Requests for more resources detailing how to manage testing, analysis and implementation.	We appreciate that developers have found our current material helpful, and we are committed to providing more material including developer office hours and technical documentation over the coming weeks and months so developers can continue to understand how the new technologies can work for them. We've also held public external developer Office Hours sessions to share best practices and demos along with Q&A sessions with Product and Engineering leads to allow for live discussion/questions.
Industry expertise	The Chrome team engaging with standards bodies lack expertise in the ads ecosystem necessary to properly balance privacy and utility.	We recognize we have a big responsibility, and we're depending on specific feedback to get this right. We also consider both privacy and effectiveness to be critical and necessary design criteria. Across the team working on Privacy Sandbox for the Web, the sum total number of years worked in the ads ecosystem is well in the hundreds.

Show Relevant Content & Ads

Topics

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Usefulness for different types of stakeholders	Concerns have been raised about the value created and distribution of that value for sites depending on their level of traffic or how specialized their content is.	The usefulness of the API will be explored through testing. 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.
Taxonomy	Industry stakeholders wish to have a voice in influencing the taxonomy.	Chrome remains open to input on the taxonomy. Chrome is very interested in feedback on the governance model for modifying the taxonomy, and discussion of how other industry bodies can play a more active

		role in developing and maintaining the taxonomy in the long term.
Not enough browsing history	Proposal to surface topics the caller has seen in previous weeks if the user doesn't have enough browsing history to create 5 topics for the most recent week	For our current design, they are chosen at random. We will investigate the correlation with past topics and consider whether there is a possibility to incorporate this, however, correlations may have adverse privacy considerations that need to be factored in.
Calling Topics on behalf of a publisher	Can a third-party service provider share Topics with a publisher?	Yes, that is a way in which we expect Topics to be used.
Potential attack vectors	Identifying the noisy topics	Based on feedback from many in the ecosystem, Chrome chose to filter topics and introduce noise. These decisions were made with privacy in mind - to limit access to information to those that otherwise wouldn't have had access to such information and introduce plausible deniability for users, respectively. We recognize that those decisions have drawbacks, such as the attack vector outlined here. However, our assessment is that the privacy benefits outweigh the potential risks. We welcome public discussion on this decision.
Origin Trial eligibility	Is there a way to detect if a user is eligible for an Origin Trial?	An origin trial feature might not be available to a user, because of browser settings or other factors, even if they're visiting a web page that provides a valid trial token and their browser is included in the group for which the trial is enabled. For that reason, feature detection should always be used to check if an origin trial feature is available, before attempting to use it.
Performance impacts	Overhead and latency concerns with Topics	We are soliciting feedback for approaches to avoid expensive and slow x-origin iframes and for the proposal to disentangle the Topics API such that getting topics does not change browsing state.
Split Topics API functionality	Providing more control over the three different aspects of the API	We understand the use case and have proposed a possible way to solve this within GitHub. We are currently awaiting further feedback from the ecosystem on whether to build the functionality. See ongoing discussion here.

Classifier timeline and documentation	Developers have requested more information about the classifier.	We have provided publicly more information about the classifier here. As well as here And here.
User controls and safety	Certain topics may be proxies for sensitive groups and users need more controls to prevent negative outcomes.	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 impact their Topics by deleting their browsing history. We welcome continued discussion regarding more advanced user controls, such as those suggested by developers; however we need to make sure that for the concerns raised in this bug, it actually removes the risks (for example, removing just the Topic 'foreign language study' but not the websites that generated the Topic from Browsing History does not fully protect the user).
Use of topics on sites with prebid.js	Can Topics API be used on websites with prebid.js?	Short answer is yes. More information has been published in our FAQ.
Use of Topics API in a recommendation widget	Can we use Topics API in Recommended widget (e.g. Outbrain)	We don't limit the use case of retrieved Topics after the API is called (that will depend on each developer's data policy).
Privacy / Policy	Questions around the purpose of filtering responses by caller if some third parties will share their topics with anyone that calls.	Based on feedback from many in the ecosystem, Chrome chose this design to limit access to information to those that otherwise wouldn't have had access to such information. Of course, publishers and third parties that receive Topics could decide for themselves what information they will share with parties on their site. If they do this type of sharing, Chrome strongly encourages them to be transparent to their users about such sharing, and offer them controls.
Noisy signals	Delivering a random topic 5% of the time might create too much noise / false signal.	Noise is an important method for protecting user privacy, and the noise levels versus usefulness of topics will be explored through testing.

FLEDGE

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Testing coordination	Testing for performance and revenue impact	FLEDGE performance, and how we can best support ecosystem testing during Origin Trials as well as General Availability, are being actively discussed in the public WICG meetings.
Trusted Server for FLEDGE	When will the Trusted Server be available for testing?	We appreciate this feedback and are actively working on a more detailed plan that we can share for use of trusted servers in FLEDGE.
Protocol standardization	Will there be a common protocol for passing data between SSPs and DSPs, such as common labels for interest groups?	We welcome feedback from DSPs, SSPs and the broader ads ecosystem on potential standardization of the spec. For the purposes of initial testing at this time, we recommend working directly with your testing partners since they are in the process of experimenting with different approaches. We also encourage, and plan to continue working with, ads trade organizations to also weigh in to create standardization in case it is useful for their member companies.
Frequency capping	Per-user frequency controls within a campaign & ad group.	FLEDGE will support frequency capping for on-device auctions and contextual / branding campaigns as well. Shared storage and site-specific caps can also be used for additional frequency capping controls.
FLEDGE impact on performance	Computationally-intensive bidders in the FLEDGE auction	Chrome is in active discussions with developers about the potential impact on site performance. Chrome welcomes the opportunity to learn more during testing.
Testing FLEDGE with other features	How will the event-level reports from the Attribution Reporting API and FLEDGE fit together?	This was discussed in a recent WICG/conversion-measurement-api call, with detailed minutes here. A summary of the meeting is that the current design for Fenced Frames Ad Reporting makes it possible to associate an id generated inside the Fenced Frame with contextual information. Event-level reports generated inside the Fenced Frame will therefore be joinable to the same contextual information on the server (using 2 server-side joins instead of 1).
Impression counting	Which Impression counting methodology should or	The FLEDGE API already supports alignment on methodology between the seller and buyer

	could be used between buyers and sellers	during the auction. We've received suggestions on alternate implementations without feedback on why our current design can't work for the ecosystem.
Displaying Multiple Ads	Whether one can display multiple ads in one auction in a given Fenced Frame	This is currently possible via component ads (not to be confused with component auctions). To do this, all ads must be in the same interest group.
"Seller Defined Audiences (SDA)" specification and FLEDGE	Could FLEDGE become a mechanism to keep buyers from building profiles from SDA on ad requests?	FLEDGE is designed to avoid information leakage that isn't relevant when the publisher already knows what SDAs its visitors are in and targeting is same-site. If it is important to support buying on SDAs within all of the protections built into FLEDGE, then one solution may be for a seller to pass SDA labels into the on-device auction, and a buy-side ad tech to create their own Interest Group whose bidding logic says "I want to buy Audience X."
Support for currencies besides USD	Support for testing FLEDGE with currencies beyond USD	We appreciate this callout and have added building in support for other currencies within our backlog of feature requests. We hope this is made available very soon.
Support for negative Interest Group targeting	An API to support negative IG targeting: showing ads only if a user does not belong to an IG.	Ongoing discussion, including some proposed options to support, in the github issue.
Multiple SSPs in FLEDGE	Risk of favoring Google when implementing multi-level auctions in FLEDGE	Support for multiple SSPs in FLEDGE was added in order to provide for a fair and equitable playing field. Google has promised under the Commitments not to design, develop or implement the Privacy Sandbox proposals in ways that will distort competition by self-preferencing its advertising products and services. Google takes this seriously, and is very open to discuss any concerns that stakeholders may have about specific aspects of the technology. For information, Chrome has publicly documented the component auction mechanism here.

Measuring Digital Ads

Attribution Reporting (and other APIs)

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Multi-touch attribution	Publishers requesting support for multi-touch attribution	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. In some cases, approximation of credit assignment (e.g., by using weighted, randomized priorities) is possible without tracking individual users.
Noise generation	Questions regarding the levels of noise within the reports	Our initial experiment allows for developers to set their own epsilon value so that they can experience how the reports change based on the level of noise. As of now, developers can choose an epsilon value up to epsilon=64. We have done this specifically to make it easier for developers to test the APIs and provide us feedback on appropriate epsilon values. We've also made a public request for such feedback.
Testing coordination	Can the local testing tool be used for the OT?	Yes, the local testing tool can be used for the duration of the OT. The local testing tool can be used with debug reports as long as third-party cookies are available.
Query Ergonomics	Enable querying aggregate of keys	We agree that this seems to improve API ergonomics with little to no apparent privacy cost. We will make a proposal and see whether there's broad consensus that it is worth supporting.
Less accurate data for small sites	Smaller sites or campaigns may receive less accurate data.	Chrome recognizes that noise based privacy protections have greater impact on smaller data slices. However, it's possible that methods like aggregating over longer periods of time would solve this problem; it's also unclear if the conclusions based on very small data slices (like one or two purchases) are meaningful to advertisers. During the origin trial, Chrome encourages testers to take advantage of the ability to experiment with a wide range of privacy and noise parameters so they can provide more specific feedback on this issue.

Limit Covert Tracking

User Agent Reduction

Feedback Theme (Ranked by Prevalence)	Questions and Concerns Summary	Chrome Response
Bot protection	UA-R impact to bot protection	We appreciate this feedback and are in the process of gathering information on bot protection approaches to inform our future designs.
Deployment Dependencies	Addressing Structured User Agent (SUA) deployment dependencies	We have rolled out "Phase 4", aka minor version version reduction to 100% of Chrome users in versions 101 and above. See update here.

User Agent Client Hints

Feedback Theme (Ranked by Prevalence)	Questions and Concerns Summary	Chrome Response
Enumerating all supported hints	Interest in having a programmatic way to know all supported hints for a browser.	We appreciate this feedback and are in the process of evaluating the feature request. We are interested in understanding if this is a common use case.
Flexibility of UA-CH vs. User-Agent header	UA-CH is overly prescriptive when compared to the flexibility the User-Agent header offers, as defined by rfc7231.	Chrome sees the prescriptive nature of UA-CH headers as an important improvement over the flexibility of the UA string, both from the point of view of eventual cross-browser interoperability and user privacy protection (by preventing arbitrary additions of high-entropy identifiers). The issue remains open in case others also share this concern and would like to provide feedback.
UA-CH: Anti-Fraud / Anti-Abuse concerns	Certain features that might be lost via UA-CH: Click redirect tracker, and fraudulent clicks.	The team is investigating these potential issues with anti-fraud and measurement stakeholders.
Performance	There are concerns about the latency of getting hints via Critical-CH (on the first page load).	Chrome is investigating ways to improve performance.

Gnatcatcher (WIP)

Feedback Theme (Ranked by Prevalence)	Questions and Concerns Summary	Chrome Response
Latency concerns	Adding extra hop(s) could impact latency	We are considering a two hop proxy and exploring ways to find the right balance between user privacy and latency. We are open to feedback and would love further discussion in W3C forums.
Fraud and bot protection	Impacts to fraud and bot protection, including in less developed countries	Safety is a core requirement as we look for ways to improve user privacy in meaningful ways, such as proxying IP addresses. A two hop proxy partnering with reputable companies provides verifiable user privacy. We are also incubating ideas for new signals to help convey user trust.
Compliance with local privacy laws	Country-level geo data reporting makes compliance with more granular local regimes difficult	We have posted our proposed principles publicly, which includes potential approaches to that would allow for websites to remain in compliance with local requirements.

Strengthen cross-site privacy boundaries

First-Party Sets

Feedback Theme (Ranked by Prevalence)	Questions and Concerns Summary	Chrome Response
Usefulness for different types of stakeholders	Impact of FPS for small vs. large publishers	The primary goal of the Privacy Sandbox is to improve user privacy by replacing current practices with solutions that do not rely on cross-site tracking mechanisms. We want these solutions to be as broadly useful as possible for different types and sizes of stakeholders. We welcome specific, actionable input on how these solutions can be improved, and we expect they will continue to evolve with community discussion and testing.
Improving privacy	Too many sites in the same set could result in similar outcomes to third-party cookies	We appreciate this feedback and are evaluating whether or what the right limits could be, while also trying to provide both users and developers with treatment or signals such that they could understand when such a limit is hit. We don't have a specific proposal yet to share but hope to very soon.

Ecosystem support of FPS	Collection of support and concerns for continuing to develop FPS outside of Privacy CG	While we would have preferred that the First-Party Sets proposal remain in the PrivacyCG, we look forward to continuing to pursue the proposal in the WICG. We were also encouraged by the numerous statements of support for continued discussion of First-Party Sets and the use cases it is intended to address. Google remains committed to finding solutions that allows the web to continue to grow and thrive in a way that protects and respects user privacy.
Browser interoperability	Implementation by other browsers	We recognize the importance of browser interoperability for developers and will continue to collaborate with other browsers to pursue standardization of FPS.
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.	Chrome is still defining our policy requirements; and will keep this feedback in mind.

Fenced Frames API

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Documentation request	Differences with sandboxed iframes	We appreciate the feedback and suggestion. There's current discussion on this on GitHub, where we're hoping to get final clarity on the request to then be able to evaluate it completely. The public discussion is available here.
Cross-API Capabilities	Default support for Attribution Reporting in Fenced Frames	We are soliciting feedback on a proposal to allow the Attribution Reporting API in "opaque-ads mode" of fenced frames by default. We encourage developers who would find this valuable to weigh in on the discussion.

Shared Storage API

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Data limits	Will there be a restriction on how much data can be stored per partition?	Yes, there will be limits. See github issue for more details. We will need storage quotas. Our current proposal is to have a per-entry size cap of 4 KB, both keys and values will be limited to 1024 char16_t

		characters apiece, and a per-origin entry cap of 10,000 entries with a mechanism that prevents additional entries from being committed when an origins' capacity is full. We are actively seeking feedback on the specific limits proposed here.
User transparency	User transparency for data sources versus data usage	We appreciate this feedback, and we think this is a promising approach worth exploring. In particular, we are evaluating whether it would be possible to do this in a way that offers sufficient transparency to users.

CHIPS

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Adoption impediments	Should CHIPS be hostname-bound? (the no-Domain requirement)	We are removing this requirement from the OT based on feedback from OT participants that this requirement added additional complexity and serves as an impediment to the adoption of CHIPS. We will discuss this requirement in the Privacy Community Group as part of standards incubation here.
Ads use cases for CHIPS	Can CHIPS be used for Ads use cases on a single site?	User tracking within one site is an allowed use case. We have updated our developer article to highlight this use case.
Authenticated embeds	Is sign-on state preserved with CHIPS?	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.
Testing coordination	Are there any additional user actions needed to test partitioning?	As long as the OT token is valid and present in the headers of the pages visited, the feature should be available for users, without requiring any additional user actions
Browser compatibility	Interest in understanding how other browsers have handled partitioned cookie attributes.	Chrome continues to work within public standards groups such as the W3C to identify designs and implementations that can work across browsers.

Web Identity API, fka FedCM

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Potential attack vectors	Potential attack vectors via link decoration and timing attacks	We are actively gathering public input and investigating potential ways to address this issue.
UX to allow for multiple IDPs	Only one IDP can be presented at a time	We believe in supporting multiple IDPs, and are actively working on approaches to support.
Expressivity	Concern that because the browser renders part of the federated identity flow, it is hard to capture all of the nuances that IDPs would like to present to their users.	Chrome is exploring including branding customizations (e.g. logos, colors) and string customization (e.g. “access this article” as opposed to “login with"). Chrome recognizes the trade-off and will continue to work with the ecosystem to both cover as much ground as possible and to make it as expressive as possible.
Applicability and Interoperability	Concern that other browsers will not adopt or implement FedCM.	Chrome has also been working with other browser vendors to find common solutions for federation at the FedID Community Group.
Suggestion to remove personal data requirements in sign-up flow	(1) a UX that indicates to the user which IdP they are choosing, without signaling that their email, picture, and name will be shared would be more privacy friendly (2) Use-cases-sign-up is sparse in its user experience and selection of claims from the IdP	We are in agreement and are exploring how to implement the feedback in a more user, and privacy friendly way.
User interaction with IdP	Need for direct interaction between user and IdP if a risk threshold is exceeded	We are actively investigating this feedback.

Network State Partitioning

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Performance	Partitioning network state could lead to increase in resource intensive	We are still investigating the performance characteristics of Network State Partitioning,

	connections to CDNs	including measuring different possible keying schemes. We have not yet made a decision between the trade-offs of performance, security, and privacy and need to gather more data.

Fight spam and fraud

Trust Tokens API

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Regulatory feedback	Concerns about investing time and resources in Trust Tokens without clear signal from regulators about long-term viability	Our goal is to build technology that works for the ecosystem, making feedback from the industry and regulators critical to the process. We will continue to consult with regulators around the world as we develop the Privacy Sandbox and make the proposals available to developers, including Trust Tokens. As with all new technologies, companies should make decisions based on their own assessment of regulatory requirements.
Launch timing	When will Trust Tokens be launched to GA?	We provide our current estimates for delivery in our public timeline on privacysandbox.com. As soon as we make a final decision on its delivery date to GA, we'll post it publicly via Chrome's release processes and update the timeline on the website.
Trust Tokens vs others	What role do Trust Tokens play given the other tokens undergoing standardization, such as Private Access Tokens	We are engaged in standardization discussions and our goal is to align with other efforts as much as possible, while enabling the different use cases each technology affords. For example, Trust Tokens and Private Access Tokens both rely on the Privacy Pass protocol.
Data limits	Max 2 Issuers for token redemption per page potentially limiting	We are looking for long term options where we can safely allow companies to redeem tokens without risking more user entropy, perhaps by partitioning access to token redemptions.
Access restrictions	Only approved (and verified/not spoofed referrer) origins should be able to verify presence of a token and redeem	We are exploring approaches for who can see and redeem tokens.
Device support	Javascript runtime dependencies limit use on certain devices. Can TT support be extended to work across other types of devices?	This is something we could consider for future development and a topic we would love to hear more feedback from developers in W3C forums. We also have an open issue for discussing an HTTP

		Header triggered token redemption that we invite feedback on.
Use cases	Unclear what the right use cases for Trust Tokens are. Lack of clarity about intended uses.	Our goal is to facilitate innovation within the anti-fraud space, and understand each company may employ proprietary techniques with trust tokens, which is why we have not been prescriptive regarding intended use(s). However, we will likely expand our documentation to include more examples as starting points for partners who are considering experimentation or adoption.
Trust Token Coverage	Removing this 'trust-token-redemption' feature policy should significantly increase the trust token coverage.	This is in consideration as we collect feedback from the OT and make decisions about next steps.
Issuer trust	Why should we trust websites that issued trust tokens?	There are no guidelines on becoming an issuer - anyone can do it. It is expected that the publishers would only work with issuers they trust. Additionally, other legitimate actors in the ads ecosystem would eventually discount (or stop buying) traffic associated with suspicious or unknown issuers.
3P embedded services	Can 3P embedded services redeem and/or request trust tokens?	Yes, a 3P embedded service can issue and redeem Trust Tokens.
Ecosystem of issuers	Greater utility can be achieved if trust signals can be shared with other companies	Trust Tokens is designed to be a low-level primitive, and can be used by cooperating issuers/redeemers to share trust/reputation signals.
Maintenance overhead	The cryptographic implementation underlying Trust Token operations is in BoringSSL; which Google is the sole maintainer of. How will maintenance of the library be managed?	Trust Tokens relies on standardized cryptographic operations (see Privacy Pass protocol) that may also be implemented in other libraries. We recommend that developers request/develop/maintain support for these operations in the libraries of their choice.
Maintenance overhead	Not clear how long protocol versions will be supported	We are looking into developing and documenting more specifics on the expected support timeframes for protocol versions.
Issuer Limits	If you are further down the chain, your opportunity to execute Trust Tokens might not arise	As more organizations begin to use trust tokens, we could increasingly see these types of timing dynamics at play, and are investigating potential solutions. As described previously, we are looking for long term options where we can safely allow companies to redeem tokens without risking more user entropy, which would minimize the importance of location on page or loading order.

New Anti-Fraud Solutions in Incubation

Feedback Theme (Ranked by Prevalence)	**Questions and Concerns Summary**	**Chrome Response**
Device Integrity Attestation Signals	Generally strong support for pursuing device integrity signals attested by platforms and made available to the web	We will continue to gather feedback and pursue the proposal through public design and iteration.
Device Integrity Attestation Signals	Questions over how much user entropy could be conveyed through new signals, and whether certain use cases (such as a user logging into their bank) could justify higher entropy signals.	We lean towards providing high value signals with as little user entropy as possible to preserve user privacy.
Device Integrity Attestation Signals	Would this signal limit access for older devices or open-source / modified platforms?	Any new signals should consider universal access as a key principle in development, and these are important questions to address upfront as we continue incubation.
Device Integrity Attestation Signals	There was some concern if new signals cause security and anti-fraud companies to overly rely on the browser and platforms	Any new signal should be viewed as supplemental data and not an indication of “trust” from the browser. We fully expect security companies to continue to rely on their own proprietary data, models and decision engines with device attestation as an additional input. Hopefully any new signal will improve detection efforts across the ecosystem and make fraud more difficult to execute.
Cookie Age Signal	Interesting concept but likely requires more investigation into applicable use cases.	Depending on levels of interest, Chrome may conduct further ideation on this concept, and craft it into an explainer for future ecosystem feedback.
Trusted Servers for Anti-fraud	Interesting concept but likely requires more investigation into applicable use cases.	Depending on levels of interest, Chrome may conduct further ideation on this concept, and craft it into an explainer for future ecosystem feedback.

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 has responded to a continuous sequence of detailed questions in this respect.

The CMA maintains close supervision over Google's announcements to the market regarding the Privacy Sandbox. In order to facilitate this, the parties have jointly implemented a process by which the CMA can review announcements before they are published by Google. Specifically, for documents containing new substantive information like Github explainers or Keyword blog posts, Google shares the draft text with the CMA at least 3 working days before publication to allow for pre-review and comments. For more routine process documentation, like Blink Intents, Google informs the CMA at least 3 working days before the announcement but the CMA does not generally review the text in advance. Google also updates the CMA on a monthly basis on minor technical exchanges to explainers, and on forthcoming routine process documents.

CMA concerns

The CMA has expressed its own concerns, as well as those received from market participants, regarding Google's First-Party Sets proposal in which, using SameParty Cookies, a party can set and retrieve cookies when it has an embed across the sites in its First-Party Set, and thus track users across those sites in which it is embedded. These concerns have centered around the use of corporate ownership to determine the boundaries of a First-Party Set. In the context of Google's commitment to have regard to the impact on publishers as part of the Development and Implementation Criteria under paragraph 8 of the Commitments, it has been suggested that a corporate ownership-focussed definition would in principle give Google, and other larger publishers, a greater ability to pool data across a wide range of domains and user-facing services. The CMA has questioned whether such an arrangement might change the relative competitiveness of larger publishers compared with smaller publishers after the removal of third-party cookies. In the context of Development and Implementation Criterion relating to privacy outcomes, the CMA has also raised the question of whether, in a First-Party Set defined by common ownership, the majority of consumers would be aware that they can be tracked across the different domains of the First-Party Set. There are also concerns around how a corporate ownership-focussed First-Party Sets would be governed, and

particularly what the funding and structure of any 'Independent Enforcement Entity' would look like.

Google has worked closely with the CMA to explore these concerns in detail, including how they might be addressed without undermining the various use cases that depend on First-Party Sets. This work is ongoing. As at the date of this Progress Report, Google is in the process of revising its proposal in response to the issues raised by the CMA as well as to enhance the prospects of multi-implementer support.

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

In addition to the concerns raised above on First-Party Sets, the CMA has informed Google about certain concerns expressed by stakeholders:

Announcements - The CMA has explained that some stakeholders have expressed a desire for greater transparency in the development of the Privacy Sandbox proposals. Google recognises the importance of transparency, and it continues to work with the CMA to provide a transparent process in line with Section D of its Commitments. Google publishes a variety of literature which can be examined to determine the direction and shape of its proposals, both in public fora like Github and in W3C discussions, and also on i ts privacysandbox.com website and dedicated microsite for developers.

Overall timetable - The CMA has pointed out that some stakeholders have 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. Google shares wider market concerns about delays to the introduction of privacy-enhancing changes and the consequent negative impacts on users' privacy this would have. It is this concern in particular that underlies Google's extensive efforts to achieve the key goals of optimizing the functionality and the success of the Privacy Sandbox technologies, along with ongoing ecosystem engagement. Google fully understands the desire for clarity around timing and hopes to provide a detailed update on its plans in the near future.

Advertising impacts - The CMA has commented that some stakeholders have raised the importance of taking into account advertising impacts in the development of Privacy Sandbox proposals. Google fully endorses this sentiment and, in line with points (b) and (c) of the Development and Implementation Criteria in its Commitments, is taking into account impact on competition in digital advertising in all design decisions relating to the proposals as well as, in particular, the ability of publishers to generate revenue from advertising inventory and of advertisers to obtain cost-effective advertising. While other factors, such as impact on privacy outcomes and the user experience, are also taken into account, and an assessment is made in the round, impact on competition remains a key consideration for Google, as required by the Commitments.

Incentives to take up Privacy Sandbox tools - The CMA has explained that some stakeholders are concerned about the possible prevalence of the Privacy Sandbox proposals in the market and whether they would become a 'de facto' standard. Google's focus is on designing the Privacy Sandbox proposals in line with the Development and Implementation Criteria set out in the Commitments, so that market participants see them as an attractive way of conducting effective, privacy-preserving advertising. While Google is optimistic that these proposals will provide the required functionality, like other ad tech providers it is also exploring multiple different ways to assist publishers by helping them leverage their existing resources. Google expects that publishers of all descriptions, large and small, will want to make greater use of their own first party data, and that this will make an important contribution to the future of digital advertising.

In addition, Google welcomes the development of alternative privacy-preserving solutions that aim to support ads targeting and measurement. While encouraging the development of such technologies, Google must always keep in mind the privacy, safety, and security of its users. Google supports a rigorous public debate of the privacy merits of all technologies affecting users, and it will not implement or support technologies that run contrary to its values. Google has nonetheless made a specific commitment at paragraph 31 of its Commitments not to change its policies for customers of Google Ad Manager, Campaign Manager 360, Display & Video 360 or Search Ads 360 to introduce new provisions restricting a customer's use of non-Google technologies before the removal of third-party cookies, unless in exceptional circumstances or required by law.

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, together with the ICO as foreseen under the Commitments, 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. Google and the CMA typically also hold one legal status meeting focusing on legal, procedural, and competition considerations. Google and the CMA collaborate on the agendas for each meeting to ensure that adequate attention is given to each topic. Additional meetings are held to discuss specific issues when the need arises.

In addition to synchronous meetings, Google and the CMA typically engage with each other on a regular basis. These engagements range from emails to formal written responses, and consist of questions and answers, the sharing of information, and the like.

Standstill

Paragraph 21 of the Commitments on notification of concerns during the Standstill is not yet applicable, as Google has not entered the Standstill Period.

Compliance statement

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

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 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 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 Renée M. DuPree

Date 14. July. 2022

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