Privacy Sandbox Progress Report

Prepared for the CMA, 16 May 2022

Overview

As part of its Commitments to the CMA, Google has agreed to provide quarterly reports to the CMA on the progress of the Privacy Sandbox proposals; updated timing expectations; substantive explanations of how Google has taken into account observations made by the third parties; and a summary of the interactions between the CMA and Google, including in particular a record of any concerns raised or comments made by the CMA and the approach retained for addressing such concerns or comments. Accordingly, Google has prepared the present report under paragraphs 12, 17(c)(ii) and 32(a) of the Commitments.

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. This timeline has been updated up to 11 May 2022 as set out below.[1] For convenience, the summary below includes all Q1 2022 updates, covering the period from January to March 2022 even before the acceptance of the Commitments on 11 February 2022 and also, for the purposes of this report, updates up to 11 May 2022. Going forward, the content of subsequent reports will more closely align to calendar quarters.

[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 Q1 2022 Timeline Updates up to 11.05.2022	
January Timeline Updates	• Adding a "Topics API" section to the homepage • Adding a "Topics API" section to the timeline • Updating the FLoC section of the timeline with the fact that Chrome has stopped development on FLoC and are now addressing this use case with Topics API
February Timeline Updates	• Removing “Origin-Bound Cookies" • Extending Purple Testing Bar for "Strengthen Cross-Site Privacy Boundaries" through Q3 2022 • Extending Purple Testing Bar for "Fight Spam and Fraud on the Web" through Q3 2022 • Removing “Ready for adoption” option

March Timeline Updates	• Combine technologies under Measure Digital Ads to just show only "Attribution Reporting API" under “Measure Digital Ads”
	• Add “OT CLOSED” to "Attribution Reporting" under "Measure Digital Ads"
	  ○ The Origin Trial ended on January 25, 2022. See here.
	• Add “OT STARTED” for CHIPS in Q1 2022.
	  ○ CHIPS: The origin trial has been open since Q1 of 2022. Register now.
	• Add “FEATURE FLAG” for First Party Sets in Q1 2021.
	  ○ First Party Sets: The feature flag is available from Chrome 89. Read more
	• Anti-Covert Tracking (ACT) timeline redesign: Implement new bottom timeline, replacing “Earliest Date of Scaled Availability” language
	  ○ Remove Storage Partitioning and Network State Partitioning from the top timeline as it will be incorporated into the redesign on the bottom timeline

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.

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, 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 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

Common themes from all feedback sources

A common theme across our discussions and feedback channels is questions about the timing, traffic levels and availability of testing. In particular, testers have consistently wanted confirmation of when APIs will be available for testing and whether testing will be available globally.

To address this feedback, Chrome has communicated broadly, and Chrome will post an FAQ confirming the same, that testing will be available globally. Furthermore, Chrome will continue to update public timelines in consultation with the CMA regularly.

Show relevant content and ads — Top Feedback Themes

API / Technology	Feedback Theme (Ranked by Prevalence)	Questions and Concerns Summary	Chrome Response
Topics	Usefulness of coarse-grained topics	Concerns have been raised that the coarse-grained topics taxonomy may not be useful enough for interest-based advertising.	The usefulness of the API will be explored through testing. Chrome expects the taxonomy to evolve based on testing results.
Topics	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.

Topics	Usefulness for different types of sites	Concerns have been raised about the usefulness 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.
Topics	Site-classification methodology	Request that sites be able to decide or influence their Topics classification.	Chrome is exploring this request, but have heard concerns (from the web browser community and from DSPs) about the potential risk of sites being able to "game the system" to target users in a privacy-invasive way or reduce relevance of ads. Chrome is seeking feedback and weighing potential changes.
Topics	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.
Topics	Site-controlled third-party permissioning	Request that sites be able to choose which ad techs can call the Topics API from their site.	This requested capability is already supported via the 'browsing-topics' permissions policy as mentioned in the explainer.
Topics	Topics API effect on page performance	Concerns around time delays to first ad as a result of depending on Topics API.	Chrome is discussing possible support for Topics in HTTP Request Headers to improve performance. We're relying on testing to see if such changes are necessary.
Topics	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.
Topics	Documentation	Interest in documentation that covers the details of the classifier model and taxonomy used by Chrome as you did for FLoC, such as how often the classifier and taxonomy will change,	Chrome already provides the taxonomy being used as part of the Origin Trials, and the classifier model that categorizes websites into Topics is made available within Chrome's code base as part of the open-source code. As part of the Origin Trials, Chrome reserves the right to make changes to either as feedback is received and learnings are gathered about how well it works.
FLEDGE	Frequency capping	Desire to be able to control the per-user frequency within a campaign or within an ad group.	FLEDGE will support frequency capping for on-device auctions. There is an open issue where this is covered for FLEDGE to support contextual/branding campaigns as well. Shared storage, another in-development API, and site-specific caps can also be used for additional frequency capping controls.
FLEDGE	FLEDGE impact on performance	Concerns have been raised about the potential impact of 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.
FLEDGE	Testing FLEDGE with other features	When and how will testing with other features (k-anonymity server, key-value servers, etc) take place.	Chrome is intentionally rolling out features in phases for our initial origin trials to make testing easier. Chrome recognizes that providing clarity on timeline for other features is important and will clarify when possible.

FLEDGE	Testing coordination	How to coordinate testing across multiple ad techs.	Chrome is investigating providing additional support to help coordinate experiments so that different ad-techs experiment on the same users. This is also a key focus of Chrome partnerships outreach; industry trade bodies have also expressed interest in playing a role.
FLEDGE	Interest groups limits	Will there be limits on the number of interest groups a user can be added to or that can be included in the auction?	Chrome is open to refining these limits for web page performance or user experience reasons during the testing period based on feedback and measured latency impact. There is an ongoing discussion amongst testers of additional ways to let buyers and sellers tune resource usage.
FLEDGE	Cross-API Capabilities	How will attribution reporting work with FLEDGE?	Full details are still TBD, and Chrome expects to have an update on this in Q2. Chrome expects to continue providing event-level reporting for auction outcomes (wins and losses) during the origin trial.

Measuring digital ads — Top Feedback Themes

API / Technology	**Feedback Theme (Ranked by Prevalence)**	**Questions and Concerns Summary**	**Chrome Response**
Attribution Reporting (and other APIs)	Testing traffic	Concerns if there will be enough traffic for testing	Chrome is starting the origin trial at very low traffic to ensure that there aren't any serious bugs or issues with user controls. Early testers play an important part in confirming that the APIs are working as intended from a technical standpoint, which helps to ramp up to a larger traffic faster. Once there is

			confidence that the APIs are functioning as expected, Chrome will increase the origin trial to support utility testing.
Attribution Reporting	Ergonomics for registering events	Questions about supported forms of registration for events.	Chrome has published a response on github to clarify what forms of registration are supported today. Chrome is collecting feedback from the ecosystem on the current design to see whether the proposed changes sufficiently address these concerns or further updates are needed.
Attribution Reporting	Noise generation	Want more detail on how noise is generated for aggregate reports.	Chrome has published a response on GitHub to provide more detail on the systematic way noise is generated. Chrome plans to provide a library to simulate noise and test with a range of parameters during OT. Chrome also plans to provide additional developer documentation and guides for the aggregate reporting mode.
Attribution Reporting	Less accurate data for small sites	Concern that smaller sites or campaigns will 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.
Attribution Reporting	Conversion delays impact on utility	Concern that conversion delays will interfere with campaign setup and verification or campaign optimization.	Chrome has heard some conflicting feedback on the impact of conversion reporting delays. However, given that the Attribution Reporting API does introduce randomized delays in reporting to protect users' privacy, Chrome expects that specific use-cases or concerns will become clearer during the testing period, and may be addressed by additional debugging support or developer guidance.
Attribution Reporting	Longer attribution window	Request to extend the 30-day attribution window	Chrome has published a response seeking more feedback on the length of the attribution window, taking to account both data minimization and utility.
Attribution Reporting	Non-viewable impressions	Questions about whether non-viewable impressions are counted for view-through conversion reports.	Chrome has published a response on GitHub to provide more clarity on viewable impressions.

Limit covert tracking — Top Feedback Themes

API / Technology	Feedback Theme (Ranked by Prevalence)	Questions and Concerns Summary	Chrome Response
User Agent Reduction	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.
User-Agent Reduction / User-Agent Client Hints	Anti-Fraud / Anti-Abuse concerns	Having as much information as possible is important when debugging certain types of attacks, including Denial of Service. Losing some info from the UA string may pose challenges.	Chrome is in discussions and evaluating ways to maintain privacy while providing sufficient information that will be useful for debugging.
User Agent Reduction	Confusion around OT setup	Multiple Origin Trial participants recommended improving documentation with examples of how to enroll in the Origin Trial.	The Reduced UA Origin Trial is ending, but Chrome intends to improve the instructions for the Deprecation Trial (including making the example demo more prominent).
User Agent Reduction	Concern about values of specific hint	Questions around if the Sec-CH-UA-Model is the same as <deviceModel> in the User-Agent string.	Sec-CH-UA-Model is the same as <deviceModel> in the User-Agent string. Chrome will try to make this more clear in future documentation.
User-Agent Reduction	Concern about enrolling in Deprecation Trial	Questions around how to enroll a large number of domains into the Deprecation Trial.	Chrome has considered centralized approaches when designing the Deprecation Trial, but Chrome believes the existing Origin Trial is the best option as it gives all control to developers (since they can choose to send the header or not).

User-Agent Client Hints	Concerns around prescriptive nature of UA-CH	There is a concern that 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). However the issue remains open in case others also share this concern and would like to provide feedback.
User-Agent Client Hints	Concerns that the API is being used to block certain browsers	Concern that a site is using the API to look for “Google Chrome” or “Microsoft Edge” and blocking all other browsers.	The concept of a brand list was designed to handle this case - a browser can send “Google Chrome” in addition to their own brands.
User-Agent Client Hints	Request for a method to enumerate all supported hints	Interest in having a programmatic way to know all supported hints for a browser.	Chrome is evaluating the feature request.
User-Agent Reduction / User-Agent Client Hints	Anti-Fraud / Anti-Abuse concerns	Client hints are not available on first load for HTTP1	One of the Client Hints Reliability APIs (ACCEPT_CH) is only available over HTTP2 and HTTP3. For servers who are still served over HTTP1, they will need to rely solely on Critical-CH.
User-Agent Reduction	Impact on Chrome for Android	Questions on how this impacts Chrome on Android in particular.	UA Reduction as well as UA-CH will ship on Chrome on Android, in addition to Desktop. For Chrome on Android, the changes will only take place in “Phase 6”, currently scheduled for Chrome 110.

Gnatcatcher (WIPB)	Non-conforming uses and methods	Clarity around what non-conforming uses and non-conforming methods would be.	Chrome will be updating the explainer with more details.
Gnatcatcher + User-Agent Reduction	Reducing signals for anti-fraud	Anti-fraud impact of *concurrently* reducing IP *and* UA access.	Expecting Willful IP Blindness anti-fraud policy stipulations (to allow use of IP for anti-fraud use cases) will resolve defensibility concerns around IP proxying.
Navigational Tracking	Concern about future breakages	Advertisers are concerned about potential breakages; identity providers have also expressed interest in Chrome's plans.	Chrome is not making imminent breaking changes, and is still exploring use cases.
SameSite Cookies	Interoperability with other browsers	Questions around Chrome's plans for fixing crbug.com/1221316, as it's an area where Chrome's implementations diverge from other browsers.	Chrome discovered a bug in the metrics, and landed new metrics as a result. Chrome is gathering data to better understand the impact of fixing the bug.
Storage Partitioning	Concern about partitioning message channels	Questions around whether messaging channels (i.e., SharedWorker & BroadcastChannel) should be partitioned.	Chrome is evaluating the feedback, however Chrome believes partitioning messaging channels along with storage is necessary to prevent covert tracking.

Strengthen cross-site privacy boundaries — Top Feedback Themes

API / Technology	Feedback Theme (Ranked by Prevalence)	Questions and Concerns Summary	Chrome Response
First Party Sets	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.
First Party Sets	The Independent Enforcement Entity (IEE) is likely to receive a large number of challenges of FPS validity	Summary of foreseeable challenges to determining FPS validity: text or privacy policy does not match across set members, clarity on how to define user-obvious set membership, bandwidth and timing challenges, and specialized expertise around corporate structure.	Chrome is still defining our policy requirements; and will keep this feedback in mind.
First Party Sets	Process for maintaining the FPS list of browsers	Concerns about barriers to entry for websites in non-western countries, inconsistent versions of the FPS list across browsers due to differences in update cadence, and ability of smaller/newer browsers to use the list.	Chrome is still defining our policy requirements, acceptance process, and usage rights for the list; and will keep this feedback in mind. Chrome will also look to learnings from other static lists used on the web platform, such as the Public Suffix List
First Party Sets	Dynamic per-site assertion design	A dynamic design (as opposed to a static list) might be more prone to false assertions of common ownership, and page load latency/failures.	Chrome is currently pursuing the static list approach; and will keep this feedback in mind if the signed assertions approach is re-evaluated in the future.
First Party Sets	Potential use cases for First Party Sets (if trustworthy and	Single sign-on, customizable data prompts, possibilities for enhanced	Chrome will consider this feedback as it considers next steps

	equitable version of FPS list can be created)	transparency reporting to users.	for First Party Sets.
CHIPS	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.
CHIPS	Design requirement	Concern that it may not be feasible to include the __Host- name prefix.	Chrome has removed the naming requirement for the Origin Trial; and will consider whether to make it permanent at the end of the testing period.
CHIPS	Usage of CHIPS for ads use cases	Questions about whether it is possible to use CHIPS for ads use cases.	CHIPS allows for a third-party to create client-side cookies that are partitioned to the top-level site (or its First-Party Set). If the use-case needs partitioned state, and not cross-site state; then CHIPS can be used for that use case.
CHIPS	Integration of CHIPS with FPS	Concern that testing with CHIPS may not be possible alongside other Privacy Sandbox proposals, like First Party Sets.	Chrome is actively exploring how to facilitate testing environments that would allow for such tests to occur. Chrome has also published instructions for local testing for FPS, and CHIPS; which can be used in the interim.

FedCM	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 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. Some ideas Chrome is exploring include branding customizations (e.g. logos, colors) and string customization (e.g. “access this article” as opposed to “login with").
FedCM	Browser involvement	Concern that the browser is more involved in the identity federation flow than previously, so it is more explicitly aware of which websites the user is logged into (also with which IDP).	Chrome recognizes that the browser now plays a more active role, but this extra level of involvement is necessary for the browser to distinguish and prevent cross-site tracking while still supporting federation.
FedCM	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.
FedCM	Various API challenges	Concern that FedCM is still early / immature and will take a long time to offer all the features that the ecosystem needs.	Chrome will explore this further as part of ecosystem testing.
FedCM	Enterprises Policies & User Controls	Concern whether there is going to be a control (e.g. enterprise policies and/or user settings) that would allow enterprises to keep their deployment of federated identity without any changes. There are a lot	Chrome is exploring controls for enterprise admins and users that it believes will address these concerns. Chrome welcomes feedback from enterprises on specific

		of on-premise deployments of federated identity that are exceptionally hard to re-deploy / change, so there is a lot of resistance towards new browser API that require IDPs to redeploy.	use cases that they would like to see accounted for.

Fight spam and fraud — Top Feedback Themes

API / Technology	Feedback Theme (Ranked by Prevalence per API)	Questions and Concerns Summary	Chrome Response
Trust Token API	Redemption limits	Concerns around 2 per page being too restrictive, especially for scenarios where one may be embedded on the same page multiple times or have a second issuer domain within their organization. One would likely hit the limit themselves without considering other market participants.	Chrome is open to expanding the redemption limit per page slightly if it would increase adoption, but need to keep it relatively low in order to introduce excessive entropy. Further, caching a redemption record may reduce the need for one issuer to redeem multiple tokens for a single user in a short period of time.
Trust Token API	Latency	Typically need to respond to bid requests within 10 ms or less, so redeeming a token on first page load makes it near impossible to include in pre-bid Invalid Traffic decisioning.	Chrome is trying to understand how latency impacts pre-bid use cases via testing.
Trust Token API	OpenRTB adoption	For prebid use cases, it is critical to pass the redeemed token information to SSPs and DSPs for use in ad decisioning.	Chrome is open to collaboration with the IAB to help ensure any useful anti-fraud/anti-abuse signals can be propagated through

			openRTB, though they own the standard for adding any new default fields.
Trust Token API	Privacy	Questions about long-term viability of any form of cross site data propagation, albeit a low amount of entropy (~2.5 bits).	Given the robust user protections to avoid unique user identifiability Chrome believes there is a good case for ecosystem acceptance. Chrome is working closely with key stakeholders to ensure long term viability.
Platform Attestation Signals	Gauging Interest in new idea/proposal	Strong support for various feasible (and infeasible) signals, such as conveying device integrity signals that platform can provide.	Chrome plans to take this idea to the W3C anti-fraud community group as a new idea for feedback.
Trusted Servers for Anti-fraud	Gauging Interest in new idea/proposal	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.

Announcements. The CMA explained that some stakeholders have expressed a view that Google's announcements may cause uncertainty in the market, and that there should be greater transparency around the role of the Commitments in the development of Privacy Sandbox for the web.

- Google continues to work closely with the CMA in line with the Commitments, and it recognises the importance of communicating that commitment to the wider ecosystem, highlighting the CMA's oversight and signposting its involvement to interested parties.
- At the suggestion of the CMA, Google has changed the wording of the introductory paragraph of the timeline page on privacysandbox.com to remind market participants that the proposals are being developed with the CMA in line with the Commitments. Google is in the process of adding similar references to the Commitments in its FAQs on privacysandbox.com, as well as prominently in various places on its developer microsite.

User Agent Reduction. The CMA has pointed out suggestions by certain stakeholders that the reduction of the User Agent string may have negative impacts on third parties that currently make use of User Agent string information. Specifically, it has been said that certain functionalities which currently rely on User Agent string information may 'break' once the change is made. The CMA wants to understand how Google intends to monitor the impact of the changes, particularly on latency.

- Google has made great efforts to explain the proposal to reduce the User Agent string, with the information affected remaining available through User Agent Client Hints. In particular, this has been done through explainers on the proposal and the corresponding origin trial, with various updates on the Chromium blog and Chrome Platform Status.
- Going forward, Google plans to monitor several metrics, including: *Net.HttpResponseCode* (material changes in the number of requests that failed to deliver content), *ClientHints.StoreLatency* (captures the time it takes, in milliseconds, to store the client hints for an origin in the PrefsService), *ClientHints.FetchLatency* (captures the time it takes, in milliseconds, to retrieve the client hints for an origin from the PrefsService, that will be added to the outgoing HTTP request headers), *ClientHints.CriticalCHRestart* (measures the number of times a navigation had to be restarted in order to include the requested client hints on the initial navigation) and *PageLoad.PaintTiming.NavigationToFirstContentfulPaint*

(measures the latency, in milliseconds, from the time the navigation starts to the time the response first starts getting painted to the screen). Google will also work with partner teams, both internal and external, to receive feedback and metrics on client hints latency from the server's perspective and will monitor community reports through Chromium and issues reported on the Github repository. Results of tests will be shared with the CMA in accordance with paragraph 17(c)(ii) of the Commitments.

Functional and effectiveness testing. The CMA has commented that some stakeholders may not understand the difference between functional testing of APIs and effectiveness testing from the perspective of the Commitments. This arises from comments made to the CMA by certain stakeholders that the design of Google's Origin Trials does not adequately assess the impacts on ads relevance and measurement from the point of view of competition or privacy.

- Such comments do indeed suggest a misunderstanding of Origin Trials, which provide a platform for the testing that website developers and ad tech providers may wish to carry out.

- Google continues to work with the CMA to thoroughly examine both the functional characteristics of its proposals and their effectiveness from the perspective of the Development and Implementation Criteria established under the Commitments. To provide more detail on this approach to testing, Google is in the process of publishing a blog post on this issue, and will add an FAQ on privacysandbox.com which links to the post.

Testing by Google Ads. The CMA has informed Google that certain stakeholders have suggested that the Google Ads business may benefit from internal testing on the impact of the Privacy Sandbox tools before these are announced to the market. The CMA suggests that it would be useful for Google to clarify what internal modelling and assessment it typically carries out in advance of significant product launches, and whether more of this could be opened up to public discussion.

- Like other active participants in the ads ecosystem, Google Ads routinely conducts simulations on different ideas that could provide value to publishers and advertisers, as illustrated by Google's paper discussing the privacy/utility trade-offs of the FLoC API. Google Ads has likewise conducted research on alternatives to the FLEDGE API (like PARAKEET) for the remarketing use-case, to try to understand whether there are better utility/privacy trade-offs which do not affect Chrome's API design.

- These evaluations are not based on prior knowledge of the final Privacy Sandbox API designs developed by Google Chrome. Indeed, other ad tech providers have conducted comparable simulations, the most notable example being Criteo, which conducted a competition for predicting clicks using mostly aggregated data to simulate the effectiveness of the Conversion Measurement API.

- Chrome welcomes all these evaluations - and especially simulation results - for the valuable directional insights they provide into whether a proposal has potential to succeed. An example of how industry feedback has helped in the design of an API is an issue raised by Meta which inspired multiple design elements for the Topics API.

- Chrome's role in testing is to provide a public development process including Origin Trials as well as a well-established system of moving potential new features through

a series of release channels, that enables publishers and ad tech providers to test proposed new features and, where appropriate, provide feedback to Chrome.

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).

Status Meetings

Google and the CMA began regular meetings in January 2022, in advance of acceptance of the Commitments, with a view to ensuring that dialogue foreseen at paragraph 17 would be in place and fully effective immediately, in the event the Commitments were accepted by the CMA. These meetings are reported below, together with the meetings held subsequently.

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. During the initial period, Google and the CMA have in fact held meetings much more frequently, generally on separate topics with respect to testing, targeting, measurement and boundaries, to assist the CMA with carrying out the regulatory scrutiny and oversight foreseen in the Commitments. There has also been discussion on user controls. As the APIs reach a more advanced state, it is anticipated that the dialogue on this issue will expand. In addition, Google and the CMA have recently instituted monthly meetings to discuss procedural and legal aspects of the Commitments as they arise.

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 April 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 Signature redacted

Full name Renée M. DuPree

Date 5. May. 2022

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