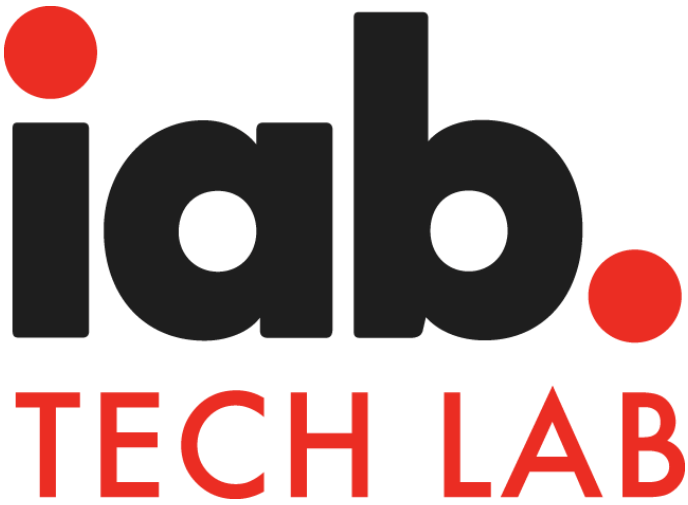


Privacy Sandbox

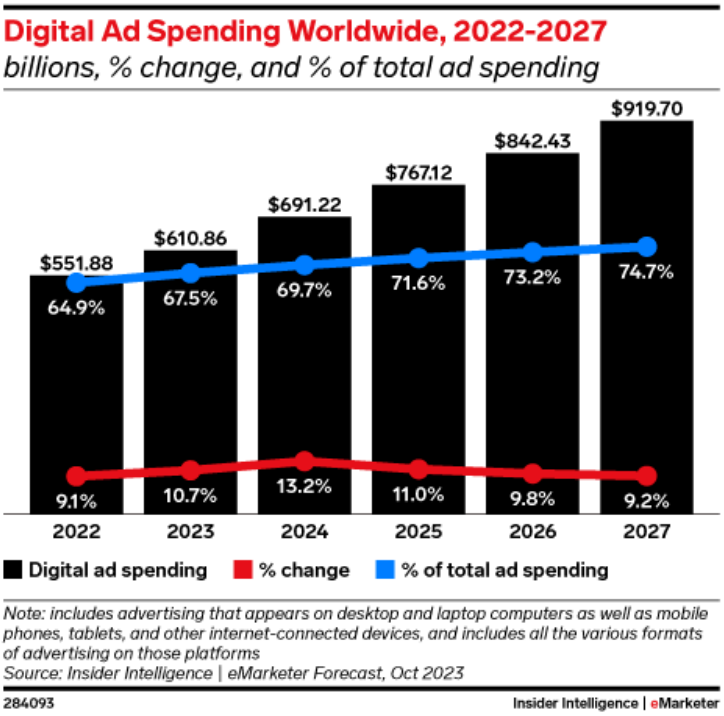
Fit Gap Analysis for Digital Advertising

Please email support@iabtechlab.com for questions and feedback.

This document is available online at *https://iabtechlab.com/privacysandbox*

About this document

Privacy Sandbox APIs rebuild the digital advertising transactions and processing into the Chrome browser as well as Android mobile platform at a later time. Current systems and processes support an estimated $690+ billion in ad spend worldwide in 2024. (Source: Insider Intelligence | eMarketer, October 2023).



Privacy Sandbox is a huge shift and everyone who runs programmatic advertising on websites in Chrome browser needs to have an understanding of how Google's changes will impact them. The focus of this document is primarily the assessment of fundamental and common everyday use cases and the implied business impact. Specifically the document focuses on analysis of Protected Audience API (PAAPI) and Attribution Reporting API (ARA) and other Privacy Sandbox features that are used for performing the following functions:

- Audience management to serve personalized advertising
- Auction management
- Measurement of key metrics- impressions, clicks and attribution
- Creative management and ad rendering showing ads on page
- Interoperability for collaboration among supply chain partners

The document is intended to inform the industry about the changes and how digital advertising will function in the Privacy Sandbox, create a call to action for industry to start testing and engage with Google Chrome team and provide Google Chrome team with industry feedback.

This document is developed by the IAB Tech Lab Privacy Sandbox Task Force.

License

IAB Tech Lab Lead

Hillary Slattery, Director Programmatic, IAB Tech Lab
Miguel Morales, Director Addressability & Privacy Enhancing Technologies (PETs)

About IAB Tech Lab

The IAB Technology Laboratory is a nonprofit research and development consortium charged with producing and helping companies implement global industry technical standards and solutions. The goal of the Tech Lab is to reduce friction associated with the digital advertising and marketing supply chain while contributing to the safe growth of an industry.

The IAB Tech Lab spearheads the development of technical standards, creates and maintains a code library to assist in rapid, cost-effective implementation of IAB standards, and establishes a test platform for companies to evaluate the compatibility of their technology solutions with IAB standards, which for 18 years have been the foundation for interoperability and profitable growth in the digital advertising supply chain. Further details about the IAB Technology Lab can be found at https://iabtechlab.com.

Disclaimer

THE STANDARDS, THE SPECIFICATIONS, THE MEASUREMENT GUIDELINES, AND ANY OTHER MATERIALS OR SERVICES PROVIDED TO OR USED BY YOU HEREUNDER (THE "PRODUCTS AND SERVICES") ARE PROVIDED "AS IS" AND "AS AVAILABLE," AND IAB TECHNOLOGY LABORATORY, INC. ("TECH LAB") MAKES NO WARRANTY WITH RESPECT TO THE SAME AND HEREBY DISCLAIMS ANY AND ALL EXPRESS, IMPLIED, OR STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AVAILABILITY, ERROR-FREE OR UNINTERRUPTED OPERATION, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. TO THE EXTENT THAT TECH LAB MAY NOT AS A MATTER OF APPLICABLE LAW DISCLAIM ANY IMPLIED WARRANTY, THE SCOPE AND DURATION OF SUCH WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. THE PRODUCTS AND SERVICES DO NOT CONSTITUTE BUSINESS OR LEGAL ADVICE. TECH LAB DOES NOT WARRANT THAT THE PRODUCTS AND SERVICES PROVIDED TO OR USED BY YOU HEREUNDER SHALL CAUSE YOU AND/OR YOUR PRODUCTS OR SERVICES TO BE IN COMPLIANCE WITH ANY APPLICABLE LAWS, REGULATIONS, OR SELF-REGULATORY FRAMEWORKS, AND YOU ARE SOLELY RESPONSIBLE FOR COMPLIANCE WITH THE SAME, INCLUDING, BUT NOT LIMITED TO, DATA PROTECTION LAWS, SUCH AS THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (CANADA), THE DATA PROTECTION DIRECTIVE (EU), THE E-PRIVACY DIRECTIVE (EU), THE GENERAL DATA PROTECTION REGULATION (EU), AND THE E-PRIVACY REGULATION (EU) AS AND WHEN THEY BECOME EFFECTIVE.

Glossary

Attribution Reporting API	This API enables advertisers and ad tech providers to measure conversions in the following cases: ● Ad clicks and views. ● Ads in a third-party iframe, such as ads on a publisher site that uses a third-party ad tech provider. ● Ads in a first-party context, such as ads on a social network or a search engine results page, or a publisher serving their own ads.
Demand Side Platform (DSP)	Entity servicing advertisers which bids on advertising opportunities presented by an SSP or (sometimes) a header bidding solution.
Fenced Frame (FF)	A fenced frame (<fencedframe>) is an HTML element for embedded content, similar to an iframe. Unlike iframes, a fenced frame restricts communication with its embedding context to allow the frame access to cross-site data without sharing it with the embedding context. Some Privacy Sandbox APIs may require select documents to render within a fenced frame. Similarly, any first-party data in the embedding context cannot be shared with the fenced frame
Header Bidding System(s)	A client-side or server-side system servicing publishers by sending bids to SSP auctions and then running an auction itself, before sending the chosen ad request payload to a publishers primary ad server. Popular header bidding systems include Prebid.js and Prebid Server, Amazon Transparent Ad Marketplace (TAM) and Google Open Bidding (OB)

Interest Groups	A Protected Audience API interest group represents a group of people with a common interest. Every Protected Audience API interest group has an owner. Interest group owners act as the buyer in the Protected Audience API ad auction. Interest group membership is stored by the browser, on the user's device, and is not shared with the browser vendor or anyone else. Interest Groups are not the same as audiences. Interest Groups are required to meet all of the following criteria simultaneously before they can start adding users: ● A creative URL (a campaign ad) must be registered and associated with the Interest Group. ● The owner of the Interest Group must agree to Sandbox terms and have an attestation placed in a well known location. ● The owner of the Interest Group must have code directly on a page before any user can be added to an Interest Group. If site visitation is a criteria to be added to an Interest Group, only behavior observed on a single site may be used to determine the signals or user interest stored on the Interest Group. Theoretically multiple sites may be used, but there is no mechanism for conflict resolution making this functionally not possible. Sandbox does support 1st party sets for publishers who own multiple websites, with a maximum of 5 related sites (as defined in the Sandbox) but the requirement that a creative is associated with an Interest Group implies that Interest Group owners will be demand partners, not website owners (unless the Publisher has created their own Interest Group to sell their own inventory). It should also be noted that ● Interest Groups may only be updated once in a 24 hour period ● Interest Groups are available on a single browser only ● Activation strategy must be pre-determined at audience building time
Open Real-Time	Most widely used protocol for managing ad requests and auction bidding between SSPs and DSPs and Header Bidding Systems.

Bidding (OpenRTB or RTB)	
Privacy Sandbox (PS)	Google Privacy initiative to phase out third party cookies and replace with privacy enhancing technologies and limit the information websites and other code on page can collect from the browser. It also includes APIs for enabling digital advertising and measurement of digital ads with privacy constraints.
Private Aggregation API	An API to generate aggregate data reports using data from Protected Audience and cross-site data from Shared Storage. While the Attribution Reporting API gathers data from an impression and a conversion that happen at different times, Private Aggregation API gathers data from a single cross site event like impression
Private Marketplace (PMP)	Curated or exclusive access, or preferred pricing for buyers on subsets of inventory from one or more publishers. Also referred to as “deals” or “programmatic deals,” agreements for PMPs can be organized between publishers or SSPs and DSPs, agencies or advertisers.
Protected Audience Application Programming Interface (PAAPI)	A set of APIs to support on device auctions for remarketing and custom audience via interest groups in Google Chrome browser (and potentially Android platform later)
Real Time	Real-time simply refers to the actual time during which something happens. In the context of computers and technology, real-time

	often refers to systems that process and respond to information or events with minimal delay. This typically means within milliseconds or microseconds, which is fast enough to seem instantaneous to humans. Some processes require even faster responses measured in nanoseconds or picoseconds.
Supply Side Platform (SSP)	Entity servicing publishers, responsible for receiving ad requests from publishers or publisher header bidding systems, requesting bids from DSPs and running an auction to determine the ad to show, or respond with a bid to the header bidding system.
Trusted Execution Environment (TEE)	A Trusted Execution Environment is a secure environment where code is executed and data is processed in an isolated private server that is inaccessible to external parties. The technology protects data by ensuring no other application can access it, and both insider and outsider threats can't compromise it

Change Log

Update as of May 2024 - Additional information about the change(s) made to the use case can be found below the associated Use Case in the “Update Comments’ section.

Epic	Use Case	Update
Audience Management	Exclusion Targeting	Supported Designation
Audience Management	Create and Modify an Audience Across Domains	Text Update
Auction Dynamics	Target a Single Campaign to My Online Audience	Text Update
Auction Dynamics	Bid Using a Deal ID	No update, but additional conversation was deemed necessary
Auction Dynamics	Receive a No Bid Response from a DSP	No update, but additional conversation was deemed necessary
Auction Dynamics	Second Price Auction	Removed from Analysis
Creative & Rendering	Invalid Traffic	Text Update
Reporting	Second Price Auction Reporting	Removed from Analysis
Reporting	Bid Loss Reporting	Text Update
Reporting	Publisher Revenue and Accrual Validation	Supported Designation
Reporting	Multi-Touch Attribution	Fully Reassessed
Technology and Interoperability	Managing Infrastructure Costs	Text Update

Table of Contents

Executive Summary

The Privacy Sandbox initiative, while aimed at bolstering user privacy, introduces significant hurdles for the digital ad economy. It is more expansive than only a technical or ad operations change, as it necessitates widespread adjustments across technical, procedural, and strategic dimensions for media companies, advertisers, and their supporting infrastructure. It requires deep collaboration among a broad spectrum of internal stakeholders, including legal, finance, compliance, ad operations, product development, and engineering organizations. The need for substantial investments in infrastructure and procedural overhauls demands resources that publishers, ad technology providers, and agencies may especially find challenging to muster, potentially diverting their limited resources away from innovation and core business functions.

In its current form, the Privacy Sandbox may limit the industry's ability to deliver relevant, effective advertising, placing smaller media companies and brands at a significant competitive disadvantage. The stringent requirements could throttle their ability to compete, ultimately impacting the industry's growth.

The purpose of the Tech Lab Privacy Sandbox Task Force and this assessment is to accomplish the following:

1. Inform the digital advertising industry on how the Privacy Sandbox impacts their businesses. The changes to how digital advertising will function in the Chrome browser are material. In our discussions with the industry, the Tech Lab has found that while the industry is aware that the Privacy Sandbox is here, they need to be made aware of the practical business implications Privacy Sandbox will have on their business, whether they are a publisher, advertiser, or agency.
2. Create a call to action for companies to start testing the Privacy Sandbox and engage with the Chrome team to learn more and provide feedback. Reading this assessment, we hope to encourage companies who have not started testing to engage with the Chrome team and the IAB Tech Lab to share their input on how the Privacy Sandbox can be improved now and in the future from a technical, operational, legal, and governance perspective as well as start developing standard methods to use the Privacy Sandbox APIs more efficiently.
3. Share Privacy Sandbox product feedback with the Google Chrome team on the critical gaps the industry sees in the Privacy Sandbox APIs. While the digital advertising industry recognizes that there needs to be some compromise to balance advertising utility and publisher monetization against enhancing consumer privacy, the gaps the Task Force has analyzed present material challenges for the digital ad economy. Some of the use cases reflect open questions to the Chrome team where the Task Force had to make assumptions based on the lack of clarity in Privacy Sandbox technical documentation.

Beyond the forty-five use cases we have assessed below, the Privacy Sandbox Task Force maintains additional concerns and questions for the Chrome team in several key areas. They are:

Fragmented Documentation
As the Task Force analyzed each Privacy Sandbox use case, it was difficult to understand the totality of some aspects of the various APIs supporting it. This was the core reason we shared our initial assessment with the Chrome team on January 25 – to ensure our functional assessments were accurate based on the public documentation available. Robust centralized technical documentation is the backbone for understanding and efficiently integrating systems. When documentation is poorly organized, incomplete, or scattered across various sources without a coherent structure, it significantly impedes the ability of users to effectively implement, troubleshoot, and leverage a system to its full potential. This leads to increased support costs and hampers an organization's ability to adapt the Privacy Sandbox to industry needs. Quality documentation should be comprehensive, easily accessible, and well-organized, serving novice users and seasoned professionals.

We understand Chrome is working on improving and centralizing Privacy Sandbox documentation soon. Clarifications on aspects of the Privacy Sandbox as "feature complete" in this newly centralized documentation are welcomed.

Lack of Consideration for Commercial Requirements
At its core, the Task Force views Privacy Sandbox as an ad exchange and ad server built into the browser. A contract with clear party-to-counterparty relations historically governs business relationships with these entities; e.g., a DSP maintains a business relationship with an ad exchange governed by a contract creating legal parameters around latency, discrepancy thresholds, data protection, privacy compliance, and limitations of liability. With Chrome acting as an active participant in a financial transaction (the ad auction) and delivery of goods (serving the ad), if Privacy Sandbox neglects legal and business requirements, that poses a grave concern. Failure to incorporate these considerations can result in legal penalties and loss of trust from customers and partners.

How does Chrome address the need to maintain contractual relationships with media buyers, publishers, and technology partners?

Absence of Third-Party Audits
Third-party audits are crucial for verifying digital advertising transactions' security, performance, and accuracy today. They objectively assess that an advertising transaction is fraud-free, properly targeted, and meets vital measurement standards. The absence of such audits leaves users in the dark about the advertising transaction's robustness against threats and its adherence to best practices.

How does Chrome propose the digital advertising industry support third-party audits in the areas of fraud, ad delivery, and measurement, to name a few critical areas subject to audits today?

Lack of Standard Industry Accreditation
Standard industry accreditation, such as MRC accreditation, is a benchmark for data quality, accuracy, and trust. Since Privacy Sandbox is rendering the ad impression, if Privacy Sandbox lacks these accreditations, it's challenging to gauge its adherence to industry data quality standards. This can deter potential buyers, as MRC accreditation is a prerequisite for many agencies and brands. Moreover, the absence of a clear path to achieving accreditation suggests a lack of commitment to data quality assurance.

Scalability & Performance of Privacy Sandbox in Chrome
The digital advertising supply chain was built on a server-to-server architecture for a good reason. Collectively, the programmatic ecosystem processes billions of daily transactions in the form of millions of auction queries per second. Web browsers are inherently limited in processing power and memory compared to server environments. As the Privacy Sandbox scales up, these limitations could significantly impact performance, especially for applications requiring intensive computations or handling large datasets. Server architectures are designed to handle multiple requests concurrently, leveraging multi-threading and distributed computing. Browsers, however, have a more limited scope for parallel processing, which could hinder the Privacy Sandbox's ability to scale as volumes increase. By shifting more auctions to the browser, the Privacy Sandbox also increases its dependency on the user's network connection. This could lead to inconsistent performance, especially in areas with poor connectivity. The shift to browser-based operations must not compromise the user experience. Performance bottlenecks and the need for frequent updates could deter business users, impacting Privacy Sandbox adoption and success.

How does Chrome plan to address this potentially explosive growth of auctions on the browser without degrading the user experience and ensure that auctions are completed in a timely fashion without causing undue harm to media companies and advertisers?

Chrome Transparency
There is general agreement that Privacy Sandbox will be challenged with resource constraints imposed by the browser run-time environment. There will be a range of storage, network, and processor constraints due to differences in hardware platforms and operating conditions that the browser will need to manage. As a consequence, the browser will have to make decisions about how to allocate resources that directly impact the ability of users of the Privacy Sandbox to execute campaigns successfully. While it is clear that the browser will have to make these decisions, it is unclear on what basis they will be made. Without transparency regarding how the browser will make these decisions and adequate monitoring to ensure they are applied accurately and consistently, participants will be entirely dependent on the Chrome browser to make decisions that adequately and fairly support them.

For example, suppose Chrome doesn't have space for another interest group, can only make three of five network calls, or can only successfully process the code of half the Interest Groups that qualify for a Privacy Sandbox auction. How does Chrome decide who gets included? This is incredibly important when it comes to making sure companies are not wasting resources. Participants in the Privacy Sandbox require contractual assurances; for example, if a buyer pays for an impression, the succeeding dependencies on attribution interactions will be properly prioritized so systems are not buying ads they will rarely or never be able to measure the value of.

Given the resource constraints imposed by the browser, how does Chrome plan to ensure that auction participants are treated fairly? Does Chrome have plans to make the decision criteria public and the setting of those criteria something that is owned by an industry body to ensure fair treatment?

Future Governance

Without clear governance structures, it's challenging for industry stakeholders to understand who decides about the Privacy Sandbox development, feature prioritization, and data handling policies. This uncertainty can lead to hesitancy in adoption and investment. Proprietary control without transparent governance mechanisms increases the risk of arbitrary changes that may not align with the broader needs of the digital advertising ecosystem. Such changes could impact advertiser campaign strategies, media company revenues, and overall marketing budgets without warning.

A lack of communicated governance structures often means limited opportunities for stakeholders to provide input or feedback on the development roadmap. This can lead to a misalignment between the Privacy Sandbox's capabilities and the industry's evolving needs. The digital advertising industry is subject to complex regulations, including data protection laws like GDPR and CCPA. A Privacy Sandbox with unclear governance in partnership with the digital advertising industry could complicate compliance efforts, potentially exposing stakeholders to legal and financial risks.

Relying on a proprietary system for critical industry functions creates a risk of vendor lock-in, where switching costs are high and alternatives are limited. This dependency can reduce bargaining power for advertisers, publishers, and the advertising technology ecosystem, ultimately impacting their bottom lines.

Without clear communication about future governance and development plans, there's a risk that the Privacy Sandbox will not prioritize interoperability with other systems. This lack of interoperability can lead to siloed data and systems, reducing efficiency and effectiveness across the digital advertising ecosystem.

How does Chrome consider future governance of the Privacy Sandbox in collaboration with the digital advertising ecosystem to ensure that consumer privacy is balanced with advertising utility and continues to power a robust ad-subsidized open web?

The Tech Lab welcomes the Chrome team's feedback on our assessment, clarifying our understanding of the Privacy Sandbox APIs, and maintaining the ongoing dialogue the IAB Tech Lab and the Chrome team have had leading up to this assessment.

Introduction

The IAB Tech Lab Privacy Sandbox Task Force, composed of senior ad tech leadership across over 65 companies, evaluated the Privacy Sandbox APIs to determine how, or if, foundational digital advertising use cases are supported. Where a use case is supported, implementation notes are provided. Where a use case relies on functionally which is explicitly not supported, or is so degraded that production support is impractical, this is indicated.

Privacy Sandbox APIs were evaluated based solely on technical version controlled specification documentation, focusing only on functionality that is intended to be supported in the publicly released version and exclusive of temporary, transitional capabilities. Where functionality includes temporary capabilities which are only intended to be supported short-term, it was evaluated based only on what is intended to be available in the long term, while identifying temporary features that may be employed during a transitional period.

Use cases have been grouped into five programmatic advertising ‘pillars’:

1. **Audience Management**: Use cases related to creating and managing audiences across sites.
2. **Auction Dynamics**: Use cases related to offering inventory to buyers, receiving bids, and selecting a winning bid.
3. **Creative delivery and rendering:** Use cases related to Invalid traffic, malware, acquiring assets for display, and ad rendering.
4. **Reporting:** Use cases related to measuring advertising from request to conversion to lifetime value
5. **Interoperability:** Use cases related to partnerships and collaborations.

The business impact of each use case is outlined in the Business Impact section after the Technical Assessment. Links to each use case’s Technical Assessment have been provided for readers who would like more information as to how the group arrived at their determination.

Approach

Each use case was deemed to be foundational to programmatic advertising and evaluated using technical specification documentation available during November 2023. Ongoing conversations and unresolved issues in the GitHub repositories, or otherwise not clearly enumerated in version controlled technical specifications are considered to be in the ideation or design phase and therefore were not evaluated by the Task Force.

Evaluations focus on Protected Audience APIs and reporting and attribution APIs along with other features that impact serving and rendering of the ad , for e.g. fenced frames. It is noted in the Business Impact session of each use case where traditional OpenRTB auctions can be used instead of Protected Audience Auctions.

Use cases that are not supported, but where the adoption of Privacy Sandbox would not represent loss of existing capabilities are not included in the assessment.

Each use case was assigned one of the following classifications:

- **Supported:** Parity with existing capabilities, even after full removal of temporary features.
- **Temporarily Supported:** Planned removal of current functionality or temporary work-arounds. Implementers should proceed with the expectation that the use case may not be supported or be degraded once the mechanism is removed and achieving the use case may not be possible in the long term.
- **Degraded:** Some support exists, but missing a significant amount of current functionality such as timeliness, integrity of data, or unrestricted access.
- **Impractical:** Technically possible, but so difficult to implement that only the most well resourced companies are expected to be able to accomplish.
- **Not Supported:**
    - Use cases that can not be accomplished in Privacy Sandbox, either by design or technical inability.
    - Use cases that rely on the ‘forDebuggingOnly’ features.
    - Use cases considered to be simultaneously Impractical and Temporarily Supported.
    - Use cases that could only theoretically be fulfilled via undocumented features, or hacks that are not compatible with the design goals of Privacy Sandbox (for example; passing data out of APIs via iFrame post messages).

Where documentation is unclear, the Remarks section of the use case will note a likely update or provide suggestions for changes.

Evaluations were done by members of the Privacy Sandbox Task Force and approved by at least 4 additional members outside of the original assessors company. To ensure the most candid possible conversation, Google employees were not included in the Task Force but were given a copy of the assessment 13 days prior to release for public comments.

Use cases that attracted differences of opinion concerning the interpretation of source technical specifications were subject to multiple reviews many weeks apart in an effort to improve assessment accuracy. At the point of initial public comment all differences have been resolved.

The Taskforce has not considered the impact on current OpenRTB data flows beyond the degradation in quality and reliability of the input data available once Privacy Sandbox is fully deployed. The transmission and interoperability of the OpenRTB data schema is not impacted by Privacy Sandbox. Current workflows will continue to be supported using traditional OpenRTB, just without 3rd party cookies (once deprecated).

Technical Assessment

Audience Management

Use cases related to creating, managing and addressing audiences in partnerships

Summary
Media owner audience creation and management is possible albeit quite different to mechanisms used today; however, the ability of brands and their media agencies to create, manage and activate audiences is severely degraded.

Exclusion Targeting

Supported
Degraded

Description
Exclusion (or negative or anti) targeting, in which a decision is made not to bid on the avail or show an ad creative, is a core component of many digital marketing strategies. Consider a brand executing a new user acquisition campaign, in this case, users who have previously engaged with the brand by visiting its Owned and Operated (O&O) properties, purchasing its products, etc., should be excluded from the campaign.

Assessment
As stated in PAAPI 5.2: “Additional bids are commonly triggered using contextual signals” meaning that either:

1. A buyer must submit all additional bids to all Protected Audience auctions as there is no way to pre-filter potential additional bids based on Interest Groups that are included in the auction.

2. A buyer must attempt to know the Interest Groups that will be available in the upcoming Protected Audience auction at the time of the ORTB auction, which is specifically prevented by the implementation of Protected Audience.

Moreover, the term additional bids does not have a normative description.

The sections 5.2, 5.3, and 5.3.1 of PAAPI confirm that the only ability to leverage negative interest groups is by leveraging the non-normative additional bids feature.

Remarks

There are three possible ways in which exclusion targeting could be achieved by a buyer, on behalf of a brand, within the Protected Audience framework, however all are blocked by current API restrictions.

1. Consider an exclusion targeting interest group at bid time

Exclusion targeting could be achieved by allowing the buyer to check if the current browser is a member of an exclusion targeting interest group (such as “HAS VISITED BRAND X”) in addition to the interest group that is the subject of the current auction. This workflow is prevented by the restriction: “the generateBid() function is called once for each interest group that the browser is a member of” with no exposure to other interest groups supported.

http://web.archive.org/web/20231127020721/https://developer.chrome.com/docs/privacy-sandbox/protected-audience-api/interest-groups/#generatebid

2. Conditionally manage a browser’s inclusion within the target interest group by considering it’s membership of an exclusion targeting interest group

Exclusion targeting within the Protected Audience framework could be achieved by conditionally managing the inclusion and removal of a browser from the target interest group based on their inclusion within an exclusion targeting interest group. For example, when a browser visits BRAND X the buyer adds this browser to the exclusion interest group “HAS VISITED BRAND X”. Elsewhere within the buyer’s publisher network, inclusion within the “HAS VISITED BRAND X” interest group is checked when considering if a browser should be included in the target interest group “BRAND X AUDIENCE ACQUISITION”. This workflow is prevented by the absence of a “listInterestGroups()” function within the API.

http://web.archive.org/web/20231127020721/https://developer.chrome.com/docs/privacy-sandbox/protected-audience-api/interest-groups/#joinadinterestgroup

3. Leverage userBiddingSignals to maintain an exclusion targeting subset of a target interest group

Exclusion targeting within the Protected Audience framework could be achieved by leveraging the userBiddingSignals within a target interest group to record when a browser has met the exclusion targeting criteria. Consider: across a buyer’s publisher network, browsers that visit any publisher and meet the targeting criteria are added to the “BRAND X AUDIENCE ACQUISITION” interest group, any browser that then visits BRAND X has the userBiddingSignal within this interest group (for example “NEGATIVE”) set to true. At bid time, the buyer could check this userBiddingSignal to exclude the negative targeting set. This workflow is prevented by the absence of a UPDATE operation associated with the joinAdInterestGroup() function. Consider: A qualifying browser that visits BRAND X would be added to the interest group “BRAND X AUDIENCE ACQUISITION” with the userBiddingSignal “EXCLUDED” set to true, the

next time this browser visits any other publisher within the buyer's publisher network, the buyer would add the browser to the "BRAND X AUDIENCE ACQUISITION" interest group without setting the userBiddingSignal "EXCLUDED", however as all joinAdInterestGroup() function calls are SET not UPDATE, the original value of the "EXCLUDED" userBiggingSignal is lost and can no longer be considered at bid time.

https://web.archive.org/web/20231121101019/https://wicg.github.io/turtledove#joining-interest-groups

Update Comments
Per Public Comment Analysis - Working Group majority vote to update supported designation to Impractical 3/18/2024

Create and Modify an Audience Across Domains

Supported
Not Supported

Description
A buyer wants to create a custom audience across multiple domains, not necessarily owned by the same publisher. The buyer wants to further segment that audience in real time based on their behavior across those domains.

Assessment
The PAAPI section 2.1 describes how buyers can register the interest group in the browser using the joinAdInterestGroup() function. PAAPI section 2.1 subsection "check-interest-group-permissions" describes the requirements of registering the interest groups from the site with a different origin. Once the interest group is registered it will take a part in the Protected Audience auction conducted later on any other site (including the sites of the multibrand publishers). According to the section 4.1 subsection "validate and convert auction ad config" browser will add all interest groups of all buyers listed in the interestGroupBuyers property of the auction config.

If the interest group is registered in the browser and the buyer is present in the auction config on any other site the group will participate in the auction.

Remarks
See Interest Group section in Introduction and the Target a Single Campaign use case for more information

Further the following must be noted:

- It is only possible to change the composition of an Interest Group from the point in time the update was made and moving forward
- Updates to Interest Groups can only be done once per 24 hours
- It is functionally impossible to manage conflicts if site visitation of more than one site is considered in the composition of an Interest Group.

Update Comments
Per Public Comment, creatives do not need to be associated with an Interest Group Prior to adding users, so some text was removed.
It should be noted that it is possible to join Interest Groups across sites, but it is not possible to append an existing user's membership details based on backwards-facing attributes within an Interest Group.

There are mechanisms to send and receive user attributes at bid time, but they are limited only to actions taken on a single publisher or site. A mechanism for buyers to segment a user within an Interest Group

Look-alike Modeling

Supported
Not Supported

Description
Look-alike modeling is a common digital advertising strategy used by brands wishing to run campaigns designed to market a product or service to users who are considered likely to want to engage with this product or service.

Consider for example a "new customer acquisition" campaign. In principle, the brand provides a "seed audience" of users who are already customers of the brand and an ad tech platform (typically a DSP or Data Company) provides a means for the brand to reach more users "like" the users in the seed audience.

Technically, the instrumentation of how the ad tech platform is able to support the delivery of the advertising to users "like" those in the seed set varies but common approaches include:

1. Bid stream modeling: When the bid stream data of users in the seed audience (including context such as page url, device characteristics such as user agent, location data such as IP address and temporal data such as date and time) is used as the training data for machine learning based predictive models that are then deployed to predict the similarity of a new bid request to those observed during the training process. The acceptable level of similarity is set to deliver the desired balance of scale and specificity required by the advertiser.

2. Audience Data Modeling: Where an ad tech platform provides a facility to extrapolate likely marketing-relevant categorization for a given seed audience (including categories such as age, gender, household income, in-market-status and product affinity), this categorization is then used to identity users whose own categorization overlaps that of the seed audience to a degree that provides the desired balance of scale and specificity required by the advertiser.

Assessment
PAAPI contains no references to features that would support this use case. TOPICS similarly does not support this use case.

Remarks
While it may be technically possible to replicate part of the processes and workflows that currently support Look-alike Modeling within the Protected Audience ecosystem, it is impractical that this use case can be supported without significant behavioral and commercial changes by existing ad tech companies.

By design, a Protected Audience auction is conducted in such a way that any analog of OpenRTB bid stream data is no longer available outside opaque worklets to any ad tech platform involved in the delivery of an advertisers campaign. In the case of Look-alike Modeling, this paradigm shift removes the facility for any bid stream modeling meaning that, if an Interest Group were to be created to represent the browsers that should fall into a Look-alike audience based on the observation of seed audience, this decision can not be made at bid time and must be made and applied at the time of Interest Group joining.

While it is noted that 1. Temporary Event Level reporting is available and 2. It is possible for a seller to pass additional signals to a buyer in the generateBid call, the stated intention [FLEDGE 5] is that no Event Level data from a Protected Audience action will be available to the buyer. Given this, it is impossible for a DSP to observe the Bid Stream characteristics of a seed audience and thus derive a Look-alike model to meet an Advertiser's request.

While it remains possible that an ad tech provider with a sufficiently large code-on-page publisher network would be able to observe the characteristics of a seed audience and create and populate a Look-alike Interest Group which could be brought by the provider (or delegated to another buyer [FLEDGE 1.3]), it is non-normative for a DSP to maintain such a network. Given this, for a DSP to offer Look-alike modeling capabilities to an Advertiser, the DSP would be forced to work in partnerships with another entity that maintains such a network, this involves significant behavioral change and with it, significant new contracting agreements and commercial arrangements.

Add a User to an Audience Even if They Have Not Visited My Site

Supported

Impractical

Description
As a brand, I want to create an Interest Group composed of my customers, even if they haven't visited my website in their current browser.

Assessment
Privacy Sandbox offers two ways to address a given audience: Interest Groups as part of PAAPI and Topics. An Interest Group allows an advertiser to register a function for use in future auctions on that browser. Chrome determines Topics from a coarse taxonomy and makes up to 3 available at any one time.

Interest Groups
PAAPI doesn't state restrictions on the context of the joinAdInterestGroup() method. According to section 2, the algorithm allows the joining of an interest group if it passes the validation described in the "check interest group permissions" subsection.

- If the owner of the interest group is the same as the context origin (same site), the validation is passed.
- If the owner of the interest group differs from the context origin - additional validation steps will be required.

Following the validation requirements, agencies are able to use third parties such as DSPs to register interest groups in browsers that haven't visited the agency's site or their advertiser client before. There can be a special interest group indicating that the browser has been registered from a third-party context.

However the reliance on a third party and the complexity of the permission delegation when operated at scale means we consider the use case is impractical; the agency is not able to perform this function directly without access to the web browser.

Topics
As Topics are both a) prescribed by the browser, not the inventory owner which removes a publishers ability to describe their own inventory and b) based on a coarse taxonomy, they cannot be used for customer identification on the open web.

Remarks
In order to create and address an audience, data brokers will be required to run an out of band user matching process that can only be accomplished with a user's email address or other form of user authentication. Once the mapping process has been completed *and* the user subsequently visits a website where the data broker has a direct integration, the data broker can

then drop the delegated Interest Group on behalf of the brand (i.e. where the Interest Group owner domain=brands_dsp.com) and address the user's browser.

The Protected Audience API explainer describes how the interest groups can be joined in the third-party context:

> *1.3 Permission Delegation*
>
> *When a frame navigated to one domain calls joinAdInterestGroup(), leaveAdInterestGroup(), or clearOriginJoinedAdInterestGroups() for an interest group with a different owner, the browser will fetch the URL https://owner.domain/.well-known/interest-group/permissions/?origin=frame.origin, where owner.domain is domain that owns the interest group and frame.origin is the origin of the frame.*
> *…*
>
> *The fetched response should have a JSON MIME type and be of the format:*

```
{
  "joinAdInterestGroup": true/false,
  "leaveAdInterestGroup": true/false
}
```

> *Indicating whether the origin in the path has permissions to join and/or leave interest groups owned by the domain the request is sent to.*
> *….*

Further GitHub issue 418 describes possible changes to PAAPI which are yet to appear in the PAAPI document. Specifically the concept of “delegate”. If PAAPI is updated to reflect the direction of thought in issue 418 then this assessment should be revised.

Auction Dynamics

Use cases dealing with offering inventory to buyers, sending material instructions, receiving bids, and selecting a winning bid.

Summary
Traditional ways of running the request/response protocol are entirely different when running Protected Audience Auctions. Programmatic Supply Chain constituents will need to carefully weigh the constrained addressability capabilities provided by the Privacy Sandbox against the ability to do many foundational things in cookieless environments (once deprecated) using traditional OpenRTB.

Target a Single Campaign to My Online Audience

Supported
Supported

Description
As a brand, I want to run a campaign targeted to users who have previously visited my website.

Assessment
The PAAPI provides the one-directional registration of the interest groups without the ability to check and reuse the already registered ones. Advertisers can't see the existing Interest Groups. They can only use the following methods to manage interest groups:

- joinAdInterestGroup() to add the interest group to the browser (section 2 of PAAPI)
- leaveAdInterestGroup() to remove the interest group from the browser (section 3 of PAAPI).
- In addition, at the end of each auction (section 4.1 of PAAPI), the interest groups can be updated (section 8).

These methods can only manipulate the data stored in the browser and don't provide any information to the advertiser. As a result advertisers can't read interest groups. However this does not impact this narrow use case.

Remarks
Brands may message users who have visited their owned and operated website on that device across the web but it should be noted that it may only be used for a single Interest Group.

See Create and Modify an Audience, and all other use cases in this section for additional information.

Update Comments
Text removed pertaining to Interest Groups being limited to a single campaign. Per Public Comment, Interest Groups may be associated to multiple campaigns.

Avoid Bidding Against Myself

Supported
Not Supported

Description
As a buyer, I want to avoid submitting multiple bids that will be competing with each other.

Assessment

The PAAPI specification allows buyers to register the interest groups in the browser using the joinAdInterestGroup() function (section 2.1). Then, in the scope of the runAdAuction() function, the browser generates bids, calling generateBid() function, for each interest group eligible for entering the particular auction. The group's owner should be present in the interestGroupBuyers property of the auction config (section 4.1 subsection "validate and convert auction ad config").

Adding the interest groups to the browser buyers add auction entries.

The parameters that are passed to the generateBid() function for each eligible interest group are described in section 4.1. subsection "generate a bid". None of the available parameters contains information about other interest groups of the same owner which also takes part in the auction. Therefore, the specification keeps silent about the opportunity to prevent participating multiple interest groups from the same buyer in the same on-device auction.

Because the buyer does not know if generateBid() is being called more than once for the same impression opportunity, it can submit one each per interest group, resulting in multiple bids for the same impression. Therefore, the buyer is bidding against themselves.

Competitive Separation

Supported
Not Supported

Description
Competitive Separation ensures that a brand's advertising does not appear alongside messaging from their competitors.

Assessment
Section 4.1 of PAAPI describes the auction configuration. There is no option or mention of the configuration of multi-placement (impression) auctions. Hence, publishers can only determine a single ad slot per call to runAdAuction(), and can call runAdAuction() N times on a page for N slots.

However, the API intentionally does not provide a way for understanding other advertising content on the page, and therefore calls runAdAuction(), to coordinate based on the renderUrl of the winning bid. Since there can be no coordination between slots, there is no ability to ensure competitive exclusion is respected.

Remarks
The current system relies on the ability to know what advertisements are being shown on a page. Because Interest Groups are siloed and may only see a single ad unit at bid time, there is

no mechanism to understand what other ads are on a page which in practice removes the ability for any party to accomplish competitive separation.

Frequency/Recency Capping

Supported
Degraded

Description
As a buyer I want to control how often I will pay for an ad shown to the same user for any combination of ad creative, campaign, or to see messages from my brand.

Assessment
Section 4.1 of PAAPI subsection “generate a bid” describes the collecting values of prevWins array which is passed as a part of the browserSignals parameter to the generateBid() function. The prevWins array contains data about the time period elapsed from the last win of the current interest group and the winning ad info. Only the items occurred in the last 30 days will be added to the prevWins. Using this data, it is possible to do frequency capping but only within a single Interest Group.

Interest Groups do work across sites, but do not span across devices.

The prevWins array only relates to the current Interest Group and therefore we conclude that it is not possible to frequency cap across different Interest Groups resulting in a creative in multiple Interest Groups not being properly capped.

Remarks
Today, a buyer can limit the number of times an ad, campaign, or brand shows to a user in a given time period. This is done by keeping track of the number of times a user has seen an ad, and aggregating that at different levels in real time to use as a restriction on future auctions. Buyers are able to verify this is working properly using log level or aggregated data.

Privacy Sandbox proposes to replace this functionality browser side, with a list of a creative's previous wins within an interest group, which can be evaluated.

Should the technical specification be modified such that the prevWins array no longer relates to the current interest group but all interest groups then this assessment will likely change.

Budget and Pacing

Supported
Temporarily Supported

Description
As an advertiser, I want to be able to budget and pace my campaigns such that budgets are respected and spent according to my expectations throughout a given time period.

My campaign does not relate to a specific single interest group.

Assessment
The PAAPI section 4.1 subsection “generate and score bids” states that the generateBid() function will get the allTrustedBiddingSignals as a parameter that should be considered on generating the bid for a given interest group.

The allTrustedBiddingSignals is a result of fetching the real time data from the buyer platform described in the subsection “build trusted bidding signals url”. The trusted bidding signals function is built based on the interested group properties like trustedBiddingSignalsURL and trustedBiddingSignalsKeys (section 2.1 of PAAPI).

So the buyer may temporarily use the KV store to retrieve the spend in conjunction with event level notifications to get real time signals from the on-device auction to allocate the budget. However, there is no explicit commitment that support for values necessary to determine budget in real time will be supported.

At time of publication, the official mechanism to do pacing in the long term rely on the Private Aggregation API which creates limited, delayed, aggregated, and noised reporting.

Remarks
While it is noted that within a single interest group, an advertiser may use trustedBiddingSignalKeys to retrieve a campaign’s current spend within the PAAPI generateBid() function, the technical requirements associated with changing budget and pacing algorithms and integration within DSP platforms to accommodate effective campaign management within Privacy Sandbox are extensive and non-normative.

Bid Using a Deal ID

Supported
Degraded

Description
As a buyer or publisher, I want to create specific deals with another party and be able to submit and receive bids for those deals.

Assessment
Privacy Sandbox provides primitive key value pairs with which to pass through any data pertaining to deals in auctionSignals and perBuyerSignals.

Section 12.4 of PAAPI describes the auction config structure, that includes such fields as “auction signals” and “per buyer signals”. They are custom JSON objects that will be passed to the generateBid() function (section 4.1, subsection “generate a bid”) and later to the reportWin() function (section 4.1, subsection “report win”). A publisher can use the “auctionSignals” or “perBuyerSignals” to pass in a deal id value. This value is then available within the generateBid() function so that a buyer knows if a given bid opportunity matches a given deal id.

Here is a sample of how a deal could be constructed (this is not a recommendation; just an example):

```
const auctionConfig = {
  seller: 'https://ssp.example',
  decisionLogicUrl: ...,
  trustedScoringSignalsUrl: ...,
  interestGroupBuyers: ['https://dsp.example', 'https://buyer2.example',
...],
  auctionSignals: {..DEAL ID here},
  sellerSignals: {...}
}
```

It is expected that some level of standardization will be needed on how to structure and format deals but it is possible.

DealIDs may be passed to be used in real time decisioning but their use for frequency capping and campaign pacing is severely degraded.

Remarks
It should be noted that these primitives lack details concerning the validation, time delay, availability, and filtering of data they contain. For example; there is no explicit text which prevents the implementer from removing key value pairs that appear to be identifiers.
There is no explicit mechanism that describes deal ids specifically within the Privacy Sandbox. Additionally, documentation does not guarantee that the current functionality in auctionSignals or perBuyerSignals that deals are dependent on will not be modified in future.

See also: Budget and Pacing and Reporting by Deal ID use cases for additional information.

Update Comments
No updates were made, but the Working Group deemed it necessary to have more in depth conversations around specific mechanisms as Feature Requests.

Receive a “No Bid” Response from a DSP

Supported
Not Supported

Description
As a publisher, I want to keep track and get reports on how many times my bid requests received no bids from a given buyer.

Additionally, as a publisher, I would like to know the reason as to why a bidder didn’t return a bid response.

Assessment
Auction reporting within Protected Audience via the reportResult() function (PAAPI section 4.1 subsection “report result”, also non-normative FLEDGE 5.1] does not provide sufficient documented facility for a Publisher to track common “no-bid” data points.

Remarks
Before an auction starts, the publisher will specify the buyers it’s interested in receiving bids from. Therefore it can know which buyers potentially received a bid request, though this is assuming those buyers have added the user to an interest group.

scoreAd() is only called whenever generateBid() submits a bid -- in other words, in order for a seller to be able to see the 'bid landscape', the following must be true:

- top-level seller must execute the on-device auction
- user must have interest groups on device for the requested buyer origins
- buyer bidding logic needs to choose to submit a bid to the component auction seller
- the bids need to be submitted and scored before the timeout

At the moment, there is no way for the seller -- and hence the publisher, who relies today on seller reporting for the DSP bid landscape -- to be able to distinguish between these cases.

For comparison, in OpenRTB, sellers know which DSPs get a bid request, and are always able to see which DSPs respond (either with a bid or a pass), and even which ones timeout. In PAAPI, sellers can only see the bids, which are a subset of these workflows.

Update Comments
This use case was not updated, but will move to a workstream dedicated to feature requests for further analysis.

Creative & Rendering

Use cases related to Invalid traffic, malware, acquiring assets for display, and ad rendering.

Summary: The rendering of static display ads are not impacted. Ad supported video is severely degraded, but there is an alternate path through traditional OpenRTB.

Use a VAST Tag

Supported
Not Supported

Description
A VAST (Video Ad Serving Template) Tag is a widely used, industry standard technology designed to facilitate the communication between ad server and video player for the purposes of delivering digital advertising.

Assessment
It is technically possible to render a VAST tag into a video player. However, this process requires passing information back and forth between an iframe and the parent frame which can be unreliable, would add latency (particularly as the message length increases), and require extensive changes to the ad server and video player.

Remarks
It is possible to render a VAST tag into a video player using an iframe (fenced frames would not be supported.)

Here are the steps that implementers would need to go through to get a VAST tag to work:

1. Buyer specifies a creativeURL which includes a specialized script and initial VAST XML template
2. Seller calls runAdAuction() and uses an iframe to serve the creative
3. The creative's script requests the additional information from the SSP (e.g. beacon urls) to generate the final VAST XML
4. The creative's script then passes the final VAST XML within the iframe to the seller's parent frame via window.postMessage()
5. The seller then passes the VAST XML to the video player for final rendering

Other items to note:

- It's not clear how concepts such as video fallback (or VAST error handling) would be supported, which is very important for Publisher advertising operations
    - There are significant issues with error scenarios that would typically result in fall back creatives being broken.

- Any mechanisms that rely on precise sequencing of postMessage() are rife with potential errors
- Every player stack would be required to overhaul integrations with their ad servers
- Once Fenced Frames are introduced, all support is removed

Due to the level of complexity, requirement to update every video player's integration with their ad server, and the risk vectors for errors introduced by reliance on postMessage(), this has been deemed as unsupported.

PAAPI contains no reference to features that would support this use case in the long term.

Render a Video Ad Alongside Video Content

Supported
Not Supported

Description
As an advertiser or publisher, I want to be able to serve pre-, mid-, or post- roll video advertisements alongside video content.

Assessment
In order for a video ad creative to be rendered alongside content it must ultimately be delivered to the video player in a raw format such as MP4.

Similarly to "Use a VAST Tag", it is technically possible to pass raw asset(s) to a video player by "breaking it out" of the sandbox iframe via window.postMessage().

However, due to the impracticality and temporary nature of the described "break out" mechanism this use case is deemed not supported.

Remarks
A publisher can't practically inject a video ad inside a running content video.

In addition, the "break out" mechanism described in the assessment is only temporarily supported and all functionality will be removed once fenced frames are required.

There is ongoing work by the Sandbox team and an update is expected prior to the Fenced Frame requirement being enforced.

Render Video Ads Without Content

Supported
Temporarily Supported

Description
As an advertiser, be able to serve standalone video ads in players without editorial video content. These types of creatives typically auto-close once the ad's video has finished playing. This means that the frame playing the video must be able to tell the outer frame that the video ad has finished playing.

Assessment
Rendering a video ad without content is temporarily supported by using an iframe. It is unclear if support will continue once Fenced Frames are required.

Remarks
A publisher can serve a Privacy Sandbox generated ad with a traditional iframe. This allows an auto-playing, muted, audience targeted video ad within HTML code may be served. Using an iframe allows traditional communication with the publisher's outer frame which would allow the ad to auto-close when done playing.

However, Privacy Sandbox will require fenced frames to be used to render winning ads (section 4.1 subsection "The runAdAuction(config) method steps"). Fenced Frames are much more restrictive and do not allow communication with the outer frame which may result in complete removal of this functionality

Video ads may be rendered, but reporting is degraded. Currently video reporting is done by tracking when the video starts playing, quartiles, video ends, etc. It is not possible for the publisher to independently receive notifications of these events when using Sandbox. This is due to the limitation of not being able to inject content into the ad as in the case of traditional video advertising using VAST.

Render Native Ad on Web

Supported
Not Supported

Description
Facilitate the serving of non-HTML ads, including formats such as JSON or raw assets like MP4 or JPGs, as well as support for 'seller-rendered native,' a scenario where a seller provides the final ad markup upon receiving native components from a buyer.

Assessment
Sandbox APIs do not cater to 'seller-rendered native' scenarios, where sellers contribute native components for buyers to integrate. While graphical assets and color information can be passed through to make ads appear more native to the website, the absence of support for non-HTML

content and 'seller-rendered native' poses limitations on the API's versatility and compatibility with various ad formats and structures.

As noted in the "Use a VAST Tag" use case, it is technically possible to natively render non-HTML content. However, due to the impracticality of that method this use case is deemed as not supported.

Remarks
Common "high impact" display products such as desktop skins, "interscroller" type products, and many other variations of ad products that integrate seamlessly with the publisher content are incompatible with the Privacy Sandbox API.

Render Responsive Display Ad on Web

Supported
Supported

Description
The term "Responsive" in the context of displaying content on a web page relates to an approach to web design that aims to make web pages and their content render well on a variety of devices and window or screen sizes.

In the context of digital advertising, this concept relates to the delivery and display of ads that adjust their size and layout based on the browser viewport.

Assessment
Section 1.2 of Google Documentation states:

> "When an ad with a particular size wins the auction (including in the current implementation), the size will be substituted into any macros in the URL (through {%AD_WIDTH%} and {%AD_HEIGHT%}, or ${AD_WIDTH} and ${AD_HEIGHT}), and once loaded into a fenced frame, the size will be used by the browser to freeze the fenced frame's inner dimensions. We therefore recommend using ad size declarations, but they are not required at this time."

Remarks
Advertisements that adjust their size and layout based on the dimensions of the browser viewport are not supported in Privacy Sandbox. All ad components submitted as part of a Protected Audience auction are required to specify a fixed width and height, which subsequently restricts the containing iframe (or fenced frame) to these dimensions for the duration of the ad's lifecycle.

Note that the initial display of the creative is supported at render time but dynamic resizing is not supported.

Render Ads that Interact with a Website

Supported
Temporarily Supported

Description
As an advertiser, I want to be able to render audience targeted ads to continuously communicate with the publisher's content to create interactive experiences.

Assessment
Fenced Frames prevent interaction between the Fenced Frame advertiser content and the publisher's website. It will not be possible for the Fenced Frame to respond to events on the publisher page or vice-versa. See 3.4 of Fenced Frames.

iFrames could provide support for this in the short term via the Post Message feature. We understand that iFrames will no longer support this ability once Privacy Sandbox is fully deployed.

As such we conclude that the use case is temporarily supported.

Creative Quality Assurance and Malware in Creatives

Supported
Not Supported

Description
As a publisher, I want to view and analyze advertisements to ensure that creatives served on my properties meet my quality standards.

Assessment
The section 4.1 of PAAPI states that the promise returned by the runAdAuction() function can be resolved to Fenced Frame Config or iframe's urn, or null in the case of error or no ads. The function makes a decision between fenced frame and iframe due to the value of auction configuration property resolveToConfig (section 12.3 of PAAPI).

Publishers won't have direct access to the ad markup as a result of the on-device auction.

Remarks
Creatives that are associated with an Interest Group and meant to serve if the ad wins the PAAPI auction, creative pre-registration and quality enforcement processes may only be orchestrated by SSPs or other ad tech partners.

Publishers will be reliant on their partners to go through the quality assurance process and will not be able to independently validate anything about the creatives.

Invalid Traffic

Supported
Impractical

Description
As an advertiser, I wish to ensure that traffic where my ads are shown originates from humans.

A publisher with low fraud and fast performance is more valuable to advertisers and more trustworthy to partners.

Assessment
Privacy Sandbox is designed to make users and/or devices unidentifiable. Advertisers and Publishers might be able to distinguish traffic from humans using the Private State Token (PST) with a suitable issuing party.

Private State Token issuers can place “Tokens” into the browser. The issuer is responsible for establishing that the browser is being used by a human, and will likely achieve this using a User Interface for sign in, or Captcha. Private State Tokens is silent concerning the issuer authentication method.

API Access
Section 11 of PST describes two APIs available to publishers to inspect Tokens.

- “hasPrivateTokens” is passed the domain name of an issuer and returns true if the browser has a Token for the issuer, or false if not. Section 11.1 states there is a limit of two issuers per publisher domain.
- “hasRedemptionRecord” is passed the domain name of an issuer and returns true if the issuer has provided a valid redemption record to the browser, or false for any other condition.

PST can be used to determine for up to two issuers if a Token is present using the hasPrivateTokens API. If not then the publisher might redirect the primary navigation of the web browser to an issuer so that the issuer can place the Token on the browser, coordinating with the issuer to return to the publisher once the Token has been set up. When navigation returns to the publisher the initial request to hasPrivateTokens API will return true avoiding further redirects.

The publisher will now know at least one issuer has a Token present in the browser. Validity of the token can be established via the hasRedemptionRecord API which will return true if the Token is valid, or false for any other status.

Fetch

Subject to permissions policy the Fetch method can be used to provide the publisher's server up to two Redemption Records (RRs) from the browser via the `Sec-Private-State-Token` HTTP request headers. The publisher's server will be responsible for validating the RR data.

PRIVACY-PASS, an IETF document referenced from PST describing the underlying protocol, explains that DLEQ proof needs to be verified. There is little additional information available concerning how this can practically be achieved and would likely require a sophisticated understanding of the underlying cryptographic concepts involved.

It would be trivial for a bot network with compromised browser code to fake the results from the two APIs, returning true in all situations, and thus tricking the caller into believing an issuer had provided a valid Token. Absent other signals any publisher reliant on PST APIs would be signaling they were open to fraud and become a target for fraud.

Should the publisher wish to use the Fetch method to obtain the RR it is not clear how the publisher will know that the RR data originated from the same browser. It would be trivial for a bot network to hijack RR records from legitimate browsers.

Further considerations.

1. The number of issuers per publisher is limited to two which limits choice for publishers using the API or Fetch methods. See PST 11.1 and 5 where the limit is clearly set to two.
2. PST is silent concerning the performance of these APIs. However the implementation of hasRedemptionRecord is complex involving network activity and cryptographic operations. Without performance guarantees publishers could be unwilling to incur such an unknown delay before any advertising requests commence.
3. The absence of the token doesn't mean that the traffic didn't come from a human. As the existing techniques used to combat fraud are being degraded via non Privacy Sandbox APIs it seems likely that the effectiveness of alternative approaches will diminish.

Remarks
The limit of two issuers is likely to drive publishers towards a small number of highly scaled issuers with high probability of already having issued a Token for the browser. At least one such scaled issuer will be the browser vendor. Such a technical specification thus has foreseeable dependency problems.

The PRIVACY-PASS documentation advises the following.

> *Is Privacy Pass completely finished? No, we regard Privacy Pass and the protocol we use as being beta releases currently and still under active development. There are still features that have not been completely implemented in the extension such as DLEQ proof verification.*

The underlying IETF specifications appear close to becoming a standard however.

PRIVACY-PASS contains the following performance guidance for a browser extension implementing the underlying cryptographic features of PST.

> *In preliminary tests on consumer hardware, our extension takes ~1.1 seconds to generate blinded tokens to be signed by the server and ~1.9 seconds to parse the signed tokens and verify the DLEQ proof.*

The assessment was performed using Private Stake Tokens and PRIVACY-PASS. The APIs as described take a single parameter for the issuer. See section 11 of the specification. However other uncontrolled documents which describe Private State Tokens suggest that multiple additional parameters can be provided. It is not clear if these predate the specification and were rejected, or if the specification will be modified to incorporate them in the future. This assessment should be revised once Google has clarified the specification is current and provided details concerning the implementation.

Update Comments
Updated the first sentence of the assessment to clarify that Privacy Sandbox was designed to make users and/or their devices, not traffic, unidentifiable.

Loss of Runtime Data for Brand Safety

Supported
Not Supported

Description
AdTech companies that provide Advertisers with Brand safety services depend on top level page URLs to decide if they should display the Advertiser's creative on a webpage, or block the ad from displaying.

Assessment
The main signal used is the top level page url (full path) which is not available via PAAPI or Fenced Frames in a manner that can be relied upon by the buyer.

Remarks
In direct and friendly frame placements, this signal came from a top window prop like window.top.location.href, which is no longer accessible in FencedFrames. This behavior comes from FencedFrames behaving as a top-level browsing context

In cross domain iframes where access to the top level page url is not available, this signal was made available via the use of creative macro replacement on the creative or ad tag url (DV360's

${SOURCE_URL_ENC} for example). In PAAPI, there is currently no supported technique to replace creative macros on the renderUrl to pass signals like top level page url to vendors who's scripts execute inside of the FenceFrame.

Noting: We are aware of GitHub Issues like the below that aim to help solve limitations due to lack of creative macro replacement in PAAPI, but neither approach helps to provide long term solutions to this issue.

- Macro Support for FLEDGE creatives #286
  - Is being deprecated in 2026 and does not provide a long term solution.
- Supporting creative macros in FLEDGE #477
  - Helps with sending creative macro data post render for reporting purposes, which is really helpful, but again doesn't help solve the current issue at hand.

Remarks

Short term solution:

Macro Support for FLEDGE creatives #286

Short term, the only DSP we know running on inventory with PAAPI enabled is DV360. They will be working with their SSPs to ensure their SSPs use the `deprecateReplaceInURN` method in their script that runs the auction to replace creative macros in the `renderUrl` before they add it to, and append the iframe/Fenced Frame to the page. This gives the DSP the ability to have access to, and replace the creative macros on our tag (given these macros are available on the `renderUrl` request to said DSP).

Using the page url as an example, this gives the SSP a path forward (for now) to pass this value to the DSP (via creative macro replacement on the `renderUrl`) and then to us via the normal DSP (DV360) creative macro replacement on our tag.

This short term solution puts all of the responsibility of creative macro replacement onto the SSP, making it imperative that some standard is put into place, and that all SSPs and DSPs adhere to this new standard, making creative macros available to the DSP via the `renderUrl`. This will require significant industry wide coordination to support something that is being deprecated in 2026.

There is no current standard to support the above, and would still need to be worked out in order to support this "short term" solution.

Long term solution:

Given the `deprecateReplaceInURN` will be officially deprecated in 2026, there is no long term solution to support passing values like top level url into the FencedFrame to support brand safety in real time.

Auction Latency

Supported
Not Supported

Description
We know from market research that auctions are highly sensitive to latency. Publishers and advertisers set performance criteria depending on their commercial objectives. Latency is a non-price factor of competition. All participants are sensitive to even small increases in latency.

The longer the perceived delay in a user requesting a page, and a complete page including advertising being rendered is inversely proportional to customer satisfaction with the page, and also willingness of a customer to click on an advertisement. Therefore the latency of a PAAPI auction must be roughly similar to the current performance of Prebid.js and pre-existing ad-tech solutions in place which typically completes in less than half a second.

Assessment
PAAPI contains no information concerning the performance and latency associated with the implementation. Absent such information in PAAPI we conclude that any specific performance requirements can not be met.

Publishers and advertisers will be unable to make informed decisions concerning the performance of their websites. Further they do not have the choice to conduct the auction in a computing environment they control such as a server.

Should PAAPI be modified to include requirements for implementations to achieve specific performance requirements then this assessment can be reassessed.

Remarks
The proposed architecture for PAAPI auctions assumes running a prebid auction (called a “contextual auction” in google documentation) prior to running a PAAPI auction. This serves two purposes:

a) To supply a floor bid that will “win” the auction in case of less desirable or lack of any bid from the PAAPI auction.
b) To express buyer information (per buyer signals) into the auction to guide the auction. In particular, Google has stated that this can be a preferred way to provide signaling such as rate limit or quota information, additional desirability information, budget information, etc. While there are other ways to express this information (the K/V store) the update frequency restrictions on K/V as envisioned by Google mean that this is the most effective way to express any real-time information to the PAAPI auctions.

Both of these restrictions make it infeasible to not run a prebid or contextual auction prior to running a PAAPI auction. This introduces significant latency by serializing the prebid or contextual auction and then the PAAPI auction.

There are also additional problems. For example, the K/V network calls do not have any easily expressed form of timeouts, which means that a component seller auction may result in unacceptable delays in the overall auction timeline. Bidding logic also must be fetched dynamically, which may also introduce performance issues. Auctions can only be run for a single slot, significantly adding to latency and resource costs. No framework exists for tuning the overall duration of an auction.

There is a document added to GitHub which contemplates further enhancements to PAAPI to handle latency however this is yet to be included in the technical specifications at the cut off point of assessment.

Reporting

Use cases related to measuring advertising from request to conversion to lifetime value

Summary: All aspects of reporting are severely degraded, especially as it pertains to independent validation, troubleshooting potential issues and billable amounts.

Bid Price Reporting for Winners

Supported
Degraded

Description
Winner is notified of the highest losing price versus the winner to understand the degree of overpayment.

Assessment
Section 12 of PAAPI describes the ReportingBrowserSignals structure that is passed to the reportWin() function (section 4.1 subsection “report win”). The ReportingBrowserSignals contains two fields that describe the second highest bid - highestScoringOtherBid and highestScoringOtherBidCurrency. These values come from browserSignals and represent the value of a bid with the second highest score in the auction.

With event-level notifications, it is possible to temporarily accurately report the highest losing bid price - given that the second highest bid’s score was due to price. However, in the future the Private Aggregation API would need to be used which introduces noise and delay.

Remarks

Note that this value may be higher than the winning bid because the seller's scoring function may have scored the bid lower, resulting in this bid not winning the auction.

Bid Loss Reporting

Supported
Not Supported

Description
As either a DSP or an advertiser, I want to understand why my bid did not win to inform and optimize my future bidding strategy.

Assessment
PAAPI contains no reference to functionality that could be considered useful for reporting lost auctions to all auction participants. As the use case does not relate only to the winner of the auction, but all auction participants including those that lose, we do not consider the use case supported.

Remarks
From the point of view of an existing server-side bid request and associated auction, a DSP (and therefore the advertisers it represents) has no way of knowing exactly which Interest Groups are eligible to participate prior to the execution of the client-side auction within the Protected Audience worklet. Through the Event-Level Reporting API (supported at least until 2026), a DSP will be informed of each winning bid along with the name of the Interest Group that won the auction.

Understanding the precise auction behavior (bids submitted, bid price, bid losses and reason for loss) is critical for bidder development and improvement, debugging, customer support and machine learning for automatic optimization.

Currently, Protected Audience API exposes this data through a temporary event level API and a long-term reporting API based on Private Aggregation.

(1) The Temporary Auction Reporting API allows bidders to log arbitrary data relating to a single Interest Group auction (including the internal state of the bidding function). This API is only intended for technical support and debugging of DSP integration to Privacy Sandbox, and not as a mechanism for ongoing monitoring or automatic optimization. For privacy reasons, the amount of data is highly rate limited; it is not recommended (and may be impossible) to record an accurate representation of the bid landscape across all Chrome browsers
(2) The Private Aggregation API also enables exposure of internal auction state (including non-winning bids), but delivers reports through a private aggregation service with

> dimension limits, metric representation, noise, and delay. Although subject to privacy restrictions through aggregation, this API is intended to capture the overall state of all auctions across all Chrome browsers.

Because both APIs record data at the individual IG level, there is no simple way for a DSP to understand behavior at the overall auction level (for instance: understanding how multiple IGs owned by the same DSP interact when bidding against each other).

Update Comments
Removed reference to 'Second Price Auction' because it was removed from the assessment. The mechanism is the same for both, so copied from the removed use case into this use case.

Publisher Revenue Accrual and Impression Validation

Supported
Not Supported

Description
As a publisher, I want to be able to fire a pixel that directly logs an event into my own database, that tells me that an ad rendered, who the advertiser was, and what Supply Path the advertisement took so I can generate reports related to advertising activity on my website.

Assessment
Google documentation on rendering ad events states:

> "Ad rendering in a temporarily relaxed version of Fenced Frames that prevents interaction with the surrounding page — but that does allow *normal network access for rendering the ad, and for logging and reporting some event-level outcomes*, as a temporary model until both a trusted-server reporting framework and ad delivery via Web Bundles are settled and in place."

The reportEvent documentation does allow an event to fire if it's registered to the i-frame or Fenced Frame where the event takes place, but publishers are still required to rely on their ad tech partners who render ads to add their beacon to the report event which functionally negates the ability for publishers to independently validate. Moreover, once the rendering in the Fenced Frame is obligatory, the third-party measurement pixels will become nonfunctional, so only the single measurement approach will work without alternatives and validations.

Remarks
Today, publishers are able to listen to and log page events and generate reports from their ad servers with counts of impressions and associated revenue for each permutation of SSP and DSP partners bidding on their inventory. When the counts for the same events are pulled by the publishers' ad tech partners, the independent reporting pulled by distinct systems gives both parties a high degree of confidence that the numbers are correct.

This ensures that there are no technical issues and allows publishers to accrue expected revenue by partner, and easily validate that the amount that they were paid is within an acceptable discrepancy range.

As the PAAPI worklets do not fire any javascript events, a publisher can not listen to events exposing that a PAAPI ad rendered, and that a particular component seller won or the best available non-PAAPI ad was rendered, publishers can no longer reconcile their own counts of ads with the ad server nor can they reconcile their own count of successful ad renders with each component seller to do billing. Also, publisher ad server technology is not able to count these events for each component seller.

Update Comments
Per Public Comment, changed from Temporarily Supported to Not Supported. Anything that makes publishers reliant on their ad tech partners is considered not supported.

Measure Viewability of an Advertisement

Supported
Temporarily Supported

Description
As an advertiser, measure the percent that an ad was shown on screen.

Assessment
The PAAPI defines the on device auction property resolveToConfig (section 4.1) that is described as (section 12.3):

“resolve to config
> *A boolean or a Promise, initially false. Whether the ad should be returned as a FencedFrameConfig, or otherwise as a urn uuid.”*

The value can be set in the config directly or resolved via promise according to the “fill in a pending fenced frame config” algorithm described in section 4.1.

As an advertiser, or third party vendor, it depends on what kind of frame the winning ad is served to. If the ad is served within a fenced frame, it is not possible to measure viewability because fenced frames cannot access dimension/position information about the outer frame. If the ad is served with a traditional iframe, dimension/position of the outer frame will be available.

Therefore, the ability to measure viewability as an advertiser/third party will not be supported once fenced frames are required by Privacy Sandbox.

Reporting by Deal ID

Supported
Temporarily Supported

Description
When implementing DealID support the ability to report impressions, wins, etc by deal id as a reporting dimension.

Assessment
The auctionSignals, in which a deal id may be passed by the seller to the buyer, object is available for the seller's reportWin() (section 4.1 subsection "report win" of PAAPI) and reportResult() (section 4.1 subsection "report result" of PAAPI) functions. This means that the deal id value contained within auctionSignals may be passed through an event-level notification via sendReportTo(). However, event-level notifications are only temporarily supported (section 13.1 of PAAPI Privacy Considerations).

No-normative documents (see the Remarks section) state that there should be a way to use the Deal ID to create report buckets. So for now it is not clear whether it will be available or not, the official specs keep silent about utilization of such ID. See the use case about the concerns related to the Deal ID data.

Considering the uncertainty concerning support in Private Aggregation API we conclude this use case is Temporarily Supported and request further clarification concerning future data interoperability between APIs and participants.

Remarks
The explainer for Protected Audience API contains a good description of all parameters for reportWin() and reportResult() functions.

The deal id can be used to construct a bucket id, which can then be used as a parameter for the contributeToHistogram() function within the Private Aggregation API. However, this is a degradation from the current Deal ID reports due to the noise injected by the private aggregation API.

Billable Metrics - CPA

Supported
Not Supported

Description
Be able to charge and pay for user actions such as view-through conversions, click-through conversions.

Assessment
The ARA specification in sections 2 and 3 states the API for registering attribution events for view-through and and click-through conversions.

However, the same specification in sections 12.9. “Triggering event-level attribution” and 18.2.2. “Aggregatable reports” states that the noise will be added to the attribution reports.

For the event-level reports the specification states that some reports will be marked with “noised” triggering status. The 6.27. “Triggering result”:
“NOTE: "noised" only applies for triggering event-level attribution when it is attributed successfully but dropped as the noise was applied to the source.”

For the aggregatable reports, the specification (section 18.2.2. Aggregatable reports) states:
“Aggregatable reports protect against cross-site information disclosure in two primary ways:

1. *For a given attribution trigger, whether it is attributed to a source is subject to one-way noise via generating null reports with some probability.*

…..
”

Adding the noise to the attribution reports makes view-through conversions and click-through conversions unsupported.

For more implementation details and limitations of Attribution Reporting API see the assessment and remarks for the Multi-touch Attribution case in this report.

Remarks
From Chrome’s own documentation:

> *The Attribution Reporting API may not be suited for cost-per-conversion billing needs, because of the noise added to event-level and summary reports.*

This use case is not supported based on the Privacy Sandbox documentation. This is due mainly to the noise injected by the Privacy Sandbox Attribution Reporting API.

Billable Metrics - CPC

Supported
Temporarily Supported

Description
Be able to charge and pay for clicks, traditionally known as cost-per-click.

Assessment

It is temporarily possible for a buyer's creative to define a click url that can be filled in with data passed to the buyer by the seller (e.g. publisher id, exchange id.)

The PAAPI in section 7.3.3 describes the methods registerAdBeacon() and registerAdMacro() that can be used to track click events.

These beacons are available for event-level reporting. A non-normative document (see the remarks section) also states that beacon events will be available in aggregation reports. However, neither the specification nor the other sources don't describe whether the macro substitution functionality will be supported in the current scope (see the remarks section). In addition, the noise added to the reports will break billing.

Given that there is no comprehensive specification and future actions for the ad beacons and the noise added in the reports, this functionality looks degraded.

Remarks
The Ads Reporting explainer states that events generated from the ad becones, like click, are available in the event level reports, but further, most probably will be available only in aggregated reports:

"In the long-term, these events could only be exfiltrated using an aggregate report."

In the future, it is unclear if advertisers will be able to add information (e.g. publisher id, exchange id) to the click urls for attributing clicks to specific sources. The Private Aggregation API will also be able to be used to measure clicks. However, the Private Aggregation API will inject noise and delays which would not provide the level of fidelity to make aggregated reports suitable for billing.

Privacy Sandbox is committed to removing link decoration, which may affect CPC and other use cases in the future.

For both href or javascript style beacons it is important to pass auction-time information to the creative, particularly exchange and publisher ID to be able to attribute the click to the correct seller and publisher. Passing this information is covered in more detail under the "Report on Information Gleaned from Macros" use case.

Billable Metrics - CPM

Supported
Degraded

Description

Be able to count and report the number of impressions, their cost, and attribute them to a specific source (e.g. publisher, exchange, etc.)

Assessment
The DSP may implement an event-level impression notification that executes if the DSPs bid wins the PAAPI Top Level Auction. This is achieved via the reportWin() and sendReportTo() functions. The section 12 of ARA describes the ReportWinBrowserSignals structure that contains additional attributes that can be sent in the notification.

While event-level notifications are only temporarily supported, in the future it will be possible to count impressions via the Private Aggregation API, but with some (as yet unknown and intentional) loss of fidelity.

This use case was deemed Degraded because only the buyer and seller are able to receive notification that includes the price.

Remarks
The description of notification's additional attributes can be found here.

MRC standards and methods don't define a way for accreditation of noised and aggregated reporting. There is no industry consensus on noise levels and acceptable aggregation or differential privacy methods. It will be problematic to use the new data sets for billing purposes without clear industry consensus and accreditation path.

Refer to the following for additional information:
Publisher Revenue Accrual and Impression Validation
Billable Metrics - CPM Business impact

Attribution Reports

Supported
Degraded

Description
Know that a user saw/clicked my ad and then took an action, purchase or otherwise

Assessment
The ARA describes attribution properties and algorithms. In particular:

- Section 2.1 introduces a new HTML attribute, "attributionsrce" to register an element <a>, <img> or <script> for attribution
- Section 2.2 described changes to the window.open to register the action for the attribution

- Section 3 describes changes in the Network to send the attribution event
- Section 9 describes report delays as “Randomized aggregatable report delay is a positive duration that controls the random delay to deliver an aggregatable report.”
- Section 10.12 describes the HTTP headers that should be used for sending the attribution event data.

ARA states that it supports the attribution reporting utilizing these objects.

However, the data that can be passed in the proposed headers is limited. In addition, aggregation (section 12.15 of ARA), noise (section 10.11 of ARA), report windows (section 6.7 of ARA), and time delays (12.12 of ARA) don’t allow building full-featured reports.

See more details in the Remarks section and in the assessment of the “Multi-touch Attribution" case.

Remarks

Current State

Today, conversion attribution is accomplished using 3rd party cookies. When an ad is rendered in a given browser, the iframe or .js that renders the ad sets a cookie. Since the cookie is set by a 3rd party (usually a DSP) the cookie is considered a 3rd party cookie. This cookie notes the time the ad was shown and if the ad is clicked the cookie will store that information as well.

As the user moves down the conversion funnel, each ad impression (or click) updates the DSPs cookie. When the user finally converts the DSP who delivered the impression must also have a “conversion pixel” on the brands “thank you” page. This conversion event is recorded server side, where a link between the cookie set at impression time and converting event is made. This flow constitutes the basics of conversion attribution today.

Protected Audience API supports two new types of conversion reporting:

1. Event level Reports
2. Summary level reports

Event Level reports

Include the publisher page the impression or click occurred on and the brand the conversion occurred on, value of the conversion and time are not included. Some percent of event level conversions are random noise added by the browser. Event level reports are not sent in real time, they are delayed at random intervals.

Sample Usage is described here:
https://github.com/WICG/attribution-reporting-api/blob/3582e3f9d166e290a07680c73d46f8312ff9196b/EVENT.md

Major Changes

- DSP may no longer set an impression cookie when their ad is rendered or when a converting event occurs.
- Will **not** contain the exact price or the value of the conversion.
- Report could include a “2” for price/value, 2 could equate to “all purchases between $0.01-$50.00”
- Will contain the site the ad rendered on and the site the conversion was attributed to.
- Will have noise added, meaning that the records in a given “event report” will be fake (Section 6.18 of ARA includes “randomized trigger rate” which is not defined but suggests some random behavior. Future versions of the specification should contain more detail so that a future assessment can be better informed on this feature.)
- Will not be supported in Safari, Firefox, Edge (or other browsers)
- Cross-device attribution reporting is unsupported

Summary Level reports

Include aggregate conversions grouped by campaign, site, and or region. These reports include, price (or value) of the conversion. For example campaign *X* on news site *Y* lead to 100 conversions worth $500.

Sample usage described here:
http://web.archive.org/web/20231208180950/https://developers.google.com/privacy-sandbox/relevance/attribution-reporting#summary_reports

Major Changes

- Conversions will not appear as individual rows but as aggregates.
- Noise will be added depending on the absolute value measured.
- Reporting data is encrypted by the browser then sent to the DSP. DSP must send the aggregate report to an “aggregation service” where noise is added.
- As the level of detail increases so does the relative noise added, slices of data that aggregate many events and users are more accurate.
- Will not be supported in Safari, Firefox, Edge (or other browsers)
- Cross-device attribution reporting is unsupported

Multi-touch Attribution

Supported
Impractical

Description

As a Brand I want to know the relative contribution of prior ad exposures across publishers' ad inventory in driving marketing outcomes (e.g., binary action such as a purchase or continuous value such as dollars spent relative to media spend) for the following purposes:

1) Timeliness requirements. Rapidly informing and optimizing how to purchase future ad inventory after winning a prior exposure opportunity (i.e. "next-click" or less than 3 seconds) via the use of unaggregated data;
2) Accuracy requirements. Accurately informing the optimization of next-click media budget allocation decisions across different OS, browser, media properties, ad creatives by geographic region, day of week and time of day via the use of unaggregated data.
3) Scale requirements. To ensure the improvement in effectiveness is maximized, I want a solution that covers the majority of my Display ad spend across publishers' properties.

Assessment

It is possible for an advertiser to utilize the Shared Storage API in combination with the Private Aggregation API to achieve this use case. Google provides an example on how to do this here.

However, as with other use cases that use the Private Aggregation API there are a few limitations and degradations that are introduced. Private Aggregation API does not support event-level notifications, introduces delay, introduces noise, requires an aggregation service, and sets the limit of an aggregation key of 128 bits.

Due to the removal of IPs the ability to measure a user's journey across devices is severely degraded.

The Shared Storage API does not support Web to App conversions.

The Attribution Reporting API does not currently support multiple touch points, and only allows prioritization of a single event during a user's journey.

Remarks

It is possible for an advertiser to utilize the Shared Storage API to track touch points for a given user across sites, with the caveat of being constricted to the same user agent.

The Shared Storage API can be accessed both by the top level frame and a fenced frame/iframe in which an ad is rendered in. An advertiser can use the Shared Storage API's "append" method to record a user's history of where a certain ad/campaign/etc was viewed.

When a conversion occurs, the advertiser can then use the Shared Storage API's "run" method to retrieve the user's touch points and then report it via the Private Aggregation API.

Note that due to the nature of the Shared Storage API's security feature, it is possible to track a conversion without using the Attribution Reporting API.

As per Google's documentation on the Private Aggregation API, reports are sent with a "random delay up to one hour."

Update Comments
Use case was re-evaluated because the Working Group did not take into consideration the Shared Storage API in the original assessment. Omni-channel is Not Supported, this use case pertains only to Multi-Touch Attribution within a single browser.

After further review, the Supported designation was updated to Impractical. Additional functionality contained in an update to HTTP Response Headers was released after the cut-off date for the analysis but had it been live, the designation would have been Degraded. Future versions of this report will have an updated designation.

Note that we consider the removal of IP addresses for this assessment, not just the removal of 3rd party cookies.

Measure Bot Impressions

Supported
Not Supported

Description
As an advertiser, I want to know if a certain impression was activated from a data center, headless browser, bot, etc.

I don't want to pay for an advertisement that wasn't displayed to a human.

Assessment
See the Invalid Traffic assessment before reading this assessment.

The assessment considers a) an impression that results from PAAPI; and b) an impression via an iFrame.

Protected Audience API
The advertiser would have the same invalid traffic options available to them as the publisher before they decide to join the browser to an interest group and an associated ad via section 2.1 of the PAAPI. If the advertiser considers the browser is not a human then they simply will not trigger the PAAPI features.

The reportWin() logic of the PAAPI described in section 4 is used by the browser to inform the advertiser that they won the auction. It would be trivial for a bot network with compromised browser code to fake the reportWin() call fooling the advertiser into believing that an advertisement had been displayed to a human when it hadn't.

iFrame
If Private State Tokens were used and the advertiser's preferred issuer has not already placed a Token in the browser there is no practical action that the advertisers could take. As such the Privacy Sandbox API is of no use to the advertiser when PAAPI is not used.

Multiple Attribution Report Recipients

Supported
Degraded

Description
As a publisher, I want to be able to register multiple recipients to get the reports for the same impression.

Assessment
The ARA specification states attribution as the consequence of actions:

- Register attribution source (section 11)
- Register attribution trigger (section 12)
- Schedule and send the attribution report (section 12)

Registering the attribution events (both source and trigger) is performed by adding the *attributionsrc* attribute to the respective ad tag (<a>, <img>, <source>). According to section 2.1, the *attributionsrc* is:

> *A string containing zero or more URLs to which a background attributionsrc request will be made.*

The spec is silent about the limit of tokens in *attributionsrc* string, but eventually, it can be limited:

> *ISSUE10 Consider allowing the user agent to limit the size of tokens.*

For each token in the *attributionsrc* the browser will make a respective attribution request and process the respective attribution event (source or trigger) received in the response. (section 12 of ATTR, subsection "*make background attributionsrc requests"*)

If the reporting origin (the origin of *attributionsrc*) for the attribution trigger matches the *destination* property of the previously registered attribution source event, the browser will schedule an attribution report.

It means that by adding multiple *attributionsrc* tokens to the reporting source tag (publisher site) and reporting trigger tag (advertiser site) - multiple entities can register to get reports for the same impression.

Limitations: The section 9 of ARA describes the vendor limits for attribution reports origins:

> *Max source reporting origins per rate-limit window is a positive integer that controls the maximum number of distinct reporting origins for a (source site, attribution destination) that can create attribution sources per attribution rate-limit window.*
>
> *Max source reporting origins per source reporting site is a positive integer that controls the maximum number of distinct reporting origins for a (source site, reporting origin site) that can create attribution sources per origin rate-limit window.*

The specification doesn't provide any particular numbers, but the explainer for Attribution Reporting does. See the details in the remarks section.

In any case, we see that the specification doesn't limit report recipients to 1 instance.

Remarks
The Attribution Reporting with event-level reports states in the section Reporting origin limits the following report limits:

> *If the advertiser is allowed to cycle through many possible reporting origins, then the publisher and advertiser don't necessarily have to agree a priori on what origin to use, and which origin actually ends up getting used reveals some extra information.*
>
> *To prevent this kind of abuse, the browser should limit the number of reporting origins per <source site, destination site> pair, counted per source registration. This should be limited to 100 origins per 30 days.*
>
> *Additionally, there should be a limit of 10 reporting origins per <source site, destination site, 30 days>, counted for every attribution that is generated and a limit of 1 reporting origin per <source site, reporting site, 1 day> counted per source registration.*

Reporting Impressions by Host Domain

Supported
Temporarily Supported

Description
As an advertiser I want to know in which domain my ad was served on.

Assessment

Protected Audience API

The PAAPI section 12 describes the BiddingBrowserSignals data structure.

```
dictionary BiddingBrowserSignals {
  required DOMString topWindowHostname;
  required USVString seller;
  required long joinCount;
  required long bidCount;
  required long recency;

  USVString topLevelSeller;
  sequence<PreviousWin> prevWinsMs;
  object wasmHelper;
  unsigned long dataVersion;
};
```

This structure includes an explicit field for the topWindowHostname which is described in a non-normative reference in PAAPI section 12 as.

```
topWindowHostname // Top-level origin's host
```

Section 4.1 of the PAAPI describes the runAdAuction() method. BiddingBrowserSignals data is referenced in the following text.

> *To generate a bid given an ordered map allTrustedBiddingSignals, a string auctionSignals, a BiddingBrowserSignals browserSignals…*
>
> *...Return the result of evaluating a bidding script with biddingScript, ig, expectedCurrency, igGenerateBid, auctionSignals, perBuyerSignals, trustedBiddingSignals, browserSignals, directFromSellerSignalsForBuyer, and perBuyerTimeout.*

The result of PAAPI generating the bid will include the BiddingBrowserSignals data structure and as such will include the topWindowHostname key and value. This will therefore be available to the buyer.

Further section 12 of the PAAPI describes the ReportingBrowserSignals data structure where topWindowHostname is included.

```
dictionary ReportingBrowserSignals {
  required DOMString topWindowHostname;
  required USVString interestGroupOwner;
  required USVString renderURL;
  required double bid;
  required double highestScoringOtherBid;

  DOMString bidCurrency;
  DOMString highestScoringOtherBidCurrency;
  USVString topLevelSeller;
  USVString componentSeller;

  USVString buyerAndSellerReportingId;
};
```

Section 4.1 describing runAdAuction() also describes the reporting operation which includes the ReportingBrowserSignals structure.

> *To report win given a leading bid info leadingBidInfo, a string sellerSignals, a ReportingBrowserSignals browserSignals, and a direct from seller signals-or-null directFromSellerSignals:...*
>
> *...Let reportWinBrowserSignals be a ReportWinBrowserSignals with the members that are declared on ReportingBrowserSignals initialized to their values in browserSignals.*

As such the topWindowHostname, also known as the domain, will be available to the advertiser at the point of bidding and reporting from PAAPI.

This use case is temporarily supported due to the availability of event-level notifications. In the future, when Private Aggregation API is required it is unclear if the constraints of the aggregation key will make reporting by host domain feasible.

Remarks
PAAPI does not require the topWindowHostname field to be populated via the standard inclusion of the MUST directive commonly defined in RFC 2119. PAAPI would benefit from the adoption of such directives.

Reporting by URL

Supported
Temporarily Supported

Description
As an advertiser I want to know the full page URL my ad was served on. This is useful to know what kind of content my ad is being shown in. For example, there may be brand unsuitable content within a site.

Assessment
Ultimately, this use case is temporarily supported but will not be supported in the future.

If a Sandbox ad is rendered in a traditional iframe, the advertiser can still access the parent frame's full location url. It is unclear if in the future Fenced Frames will allow access to the frame's full location url, but it is assumed that they will not. Google documents that the URL passed into Fenced Frames will have k-anonymity enforced.

A buyer gets access to signals passed into the auction for reporting when the reportWin() function is called. The reportWin() function gets access to browserSignals which is a structure of data populated directly by the browser. However, browserSignals does not include the full location url.

It is also possible for the seller to pass the full location url via auction signals into the auction. However, this is distinctly different from the advertiser being able to query the browser for the current location url.

In the case that the buyer is comfortable relying on the location url passed in by the seller through the auction signals it is possible to report it back to the buyer within reportWin() using the temporary event-level notification mechanism. Once event-level win notifications are disabled, the buyer may use the Private Aggregation API by making the location url part of the aggregation key. However, using the raw url cannot be used as the aggregation key because an aggregation key is limited to 128 bits, and needs to be combined with other reporting dimensions (e.g. campaign id, creative id) to be useful. A mapping of urls to small integers could be used, but may not be feasible due to the cardinality in the number of unique location urls a creative is served on and the limit in the range of a small integer. Thus, in the future it will be impractical for the buyer to get reports on full urls their creative served on.

This use case does not relate just to PAAPI but also the Attribution Reporting API which is more relevant in practice to advertisers. The assessment of Reporting by Host Domain includes analysis of Attribution Reporting API reports specifically for the host/source origin and is not repeated in this assessment. There is no option in Attribution Reporting API to pass either arbitrary data as envisaged in PAAPI or the URL that the report relates to. As this use case relates primarily to reporting we conclude that the use is not supported.

Remarks

It would be useful if the browser populates a field similar to the topWindowHostname described in the Resolve Host assessment. Such a field might be called topWindowOriginalUrl and would contain the URL used by the browser. This could not be altered by the seller and would be included in both Attribution Reporting API attribution sources and PAAPI's ReportingBrowserSignals.

Report on Information Gleaned from Macros

Supported
Not Supported

Description
Ability to generate a report using values gleaned from key values appended to the ad markup using Macros (aka Key Value Pairs).

Assessment
The PAAPI assumes using the reportWin() and reportResult() functions to generate reports of the action result for seller and buyer respectively.

The runAdAuction() function passes the following parameters to generate the result report (section 4.1 subsection "report result" of PAAPI): leading bid info (section 12.4), a direct from seller signals-or-null directFromSellerSignals, an auction config-or-null winningComponentConfig,

The runAdAuction() function passes the following parameters to generate the win report (section 4.1 subsection "report win" of PAAPI): leadingBidInfo (section 12.14), sellerSignals, reportResultBrowserSignals (section 12), and directFromSellerSignalsForBuyer (section 12.12).

The specification doesn't state clearly that any of the bidding signals obtained from the auction config (see section 4.1 subsection "build trusted bidding signals url") will be passed to the report functions.

Until the PAAPI provides a clear explanation of how to pass buyers' trusted signals to the report generating functions, this use case is not supported.

Remarks
The Top Level Seller is able to make a decision using the contents of a key value pair via auctionConfig at bid time. However, generating a report based on the macro in question is only available using event level reporting which is expected to be removed. In the long-term, macros may only be used in histograms generated by the Private Aggregation API, and only after it's gone through the noise and encryption process, removing the ability to run fine grain analysis on a given macro.

Reporting by Creative URL

Supported
Not Supported

Description
As a publisher I want to know which creatives are being served to users.

Assessment
Creatives in PAAPI are rendered via FencedFrames using the FencedFrameConfig defined in Fenced Frames section 2.3.4. FencedFrameConfig contains a URN field that, if readable, would likely contain a URL that would enable the publisher to understand the Creative URL used. The field name is FencedFrameConfigURL. FF advises that the field is an “opaque” property meaning that its value can’t be read.

Section 2.3.3 of Fenced Frames also contains the following notice.

“This fenced frame config instance should really exist on browsing context group, however until third-party cookies are deprecated, this specification supports many of the Fenced Frame concepts on the iframe element. This requires that for the short term, a normal content navigable be able to load a fenced frame config, and therefore have access to the navigation’s corresponding fenced frame config instance.”

The implication of “short term” is that the implementation available for testing prior to the deprecation of third party cookies will support the use case, but will not afterwards.

The combined effect of these two sections of Fenced Frames leads us to conclude that the use case will not be supported.

Remarks
The Google Fenced Frame status document advises that access to the Creative URL will be removed when third party cookies are deprecated. The document states “Note: The temporary navigator.deprecatedURNToURL() will be removed by third-party cookie deprecation.”

Further the Fenced Frame explainer advises;

“The FencedFrameConfig object has a read-only url property; however, since the current use-cases require the actual URL of the internal resource to be hidden, this property returns the string opaque when read.”

This supports the assessment based on Fenced Frames that the URL required will be unavailable to the publisher in practice and will only be known to the web browser and advertiser.

Business Impact
Publishers will need to spend significantly more FTE time in ad operations evaluating creative assets. Risk averse publishers will need to move from exclusion to inclusion lists of approved advertisers and manually review each creative in addition to holding a mapping table outside of the bidstream of approved creative ids to be used in their scoreAd function.

Measure Multiple Conversions from Multiple Ads

Supported
Degraded

Description
As an Advertiser I want to measure attribution when I advertise multiple brands that convert on the same domain.

Assessment
Chrome Attribution Reporting API (ARA) attribution happens in the Customer browser by matching the Source and Trigger registrations. The matching of source and trigger registration for attribution happens in the following priority order: (i) Source events having same destination site in trigger events are matched, (ii) Only the most recent source event with matching destination site is matched, and (iii) filter_data between the recent source event should match with trigger event. When there is a successful attribution, all active source events with the same destination site will be deactivated.

Issue: The above Chrome ARA attribution algorithm will under-report on conversions, when customers convert for multiple brands in the same destination site. Chrome ARA attribution algorithm has two issues, namely (i) under-reporting due to last-touch matching, and (ii) under-reporting due to de-activation of source events. Due to this issue, a common use case like the below will have under-reporting of conversions.

Reference from Privacy-Sandbox:
For the last-touch matching, please refer to the trigger attribution algorithm section in the link below. It states that, “When the browser receives an attribution trigger registration on a URL matching a destination eTLD+1, it looks up all sources in storage that match <reporting origin, destination eTLD+1> and picks the one with the greatest priority. If multiple sources have the greatest priority, **the browser picks the one that was stored most recently.**”

https://github.com/WICG/attribution-reporting-api/blob/main/EVENT.md#trigger-attribution-algorithm

Once a source matches with a trigger and a successful attribution happens, all existing active sources will be deactivated. Reference is available in this ticket.
https://github.com/WICG/attribution-reporting-api/issues/842

Example**:** A sneaker major sells multiple brands on their Sneaker_example.com store. A chrome user sees a 'Brand-one' hiking shoe ad on 1st July and 'Brand-two' running shoe ad on 3rd July. Both source event views are registered in the user's browser. After seeing both ads, if the user first purchases 'Brand-one' shoes, then it won't be attributed due to 'last touch' as 'Brand-two' is the most recent ad. If the user first purchases 'Brand-two' and then 'Brand-one' shoe, then only 'Brand-two' will be attributed and 'Brand-one' will not be reported, as the 'Brand-one' ad event would have been deactivated after 'Brand-two' conversion. In both cases, one eligible attribution is lost and under-reported.

Remarks
Google's 'attribution scope' feature they are considering to add in the future, can allow defining which scopes of ads (e.g., campaigns, brands, etc.) a conversion event is eligible for. However it still 'de-activates' all active ad source events under all scopes once there is one successful attributable conversion event. If the user saw ads for 5 different shoe brands sold at sneaker_example.com, as soon as there is a conversion event for any one brand, the rest of the source registrations are deactivated and become unmeasurable, when the user purchases another brand product later.

Technology and Interoperability

Use cases related to partnerships and collaborations.

Managing Infrastructure Costs

Supported
Not Supported

Description
One of the key challenges of the ad-tech ecosystem is the problem of scale. To meet scale requirements, publishers, DSPs, SSPs, and other members of the ecosystem need to provide network, compute and services, as well as manage those services. These services in turn require resources that have real-world implications - rack space with its physical limitations, power (with its implications for the environment and heat constraints), network capacity and manufacturing costs mean that it is critical that companies scale their resources in the most

efficient way possible. Corporations have spent billions of dollars to stand up and maintain this infrastructure. We need to ensure that we can provide advertising services with a similar cost model and similar scaling model to existing auctions by leveraging this infrastructure and processing the new demands of PAAPI with a minimum of new compute and network load on the system.

Assessment
Privacy Sandbox specifications keep silent about what new services and infrastructure will be required to support it.

Remarks
The serial auction model as described by Google (a traditional programmatic auction followed by a PAAPI auction) already puts significant new traffic and network restrictions into play that previously were not present. This is a simple physics problem - if you ask a system to do more work, it will require more compute, network and power. This means that additional costs need to be incurred to support Protect Audience auctions - more servers to handle traffic, more core network capacity, more top of rack capacity for network switching and more power to drive these systems.

Beyond the core auction flow as part of the Private Aggregation API Google requires that specific portions of the PAAPI reporting flow occur in a TEE (Trusted Execution Environment). This in turn requires Publishers and DSPs to collect encrypted records in their own reporting environments, egress these records from their reporting environment, transit the Internet or VPC-endpoints and ingest this traffic into a TEE running at Google, or in the sole Google preferred partner (Amazon Web Services.)

At the TEE, the data is decrypted, processed, then transmitted (again via the Internet or a private VPC endpoint) into a non-TEE environment. This flow results in massive duplication of data. The requirement to require a TEE, while simultaneously restricting TEEs to only Google and Amazon ensures that a duopoly can dictate commercial terms - a setup highly unlikely to result in competitive pricing. This is especially egregious when compared with already paid for and in-use servers, network infrastructure and rack space.

These problems occur because PAAPI assumes that only Google and Amazon can be trusted with advertising data - all others must pay to process privileged information inside of areas that Google or Amazon control.

Update Comments
Removed line referencing the difficulty forecasting costs because a Cost Forecasting Tool did exist at the time of the analysis.

Privileged Signals

Supported
Not Supported

Description
Data that would traditionally not be accessible to competitors, partners and end-users is forced by PAAPI to be publicly available without any way to protect this information. Specifically, pricing rules (commercially sensitive rate cards) and publisher controls, like advertiser blocks, are applied in the browser.

Assessment
As documented in https://github.com/WICG/turtledove/issues/824, PAAPI or any other part of Privacy Sandbox don't provide solutions to this problem without adopting bidding and auction services, which is not available yet, and requires additional financial impact.

Remarks
By definition, the open nature of these signals means that sensitive publisher signals are being exposed to the browser, rather than being applied server-side. For example, the key-value service can be queried by any party, and there's no meaningful way to restrict access. In addition, the nature of the hierarchical top-level auctions and component auction system means that data that previously would have been protected is no longer protected. For example, in server-side auctions, sellers are the only party privy to the second-highest bid, as well as the clearing price for the final auction conducted by the publisher's ad server (if the seller's bid was chosen.) Sellers are also in a position to determine the rules for disclosure of the second-highest bid (aka minimum bid to win.) In contrast, PAAPI provides automatic signaling of these values to parties that participate in the on-device auction – even if those parties submitted a losing bid.

Data Guarantees

Supported
Not Supported

Description
Since the beginning of digital advertising, business relationships are governed by contracts with clauses pertaining to data usage and security.

Today, a contract exists with Google when data is transferred server to server for the purposes of advertising that sets obligations on the parties concerning the use of data.

Assessment
None of the Privacy Sandbox or Chrome APIs support an equivalent contractual and commercial mechanism to enable the web server operator to be certain they are dealing with a legal Google entity that will honor commitments necessary for commercial operation. As such this common use case is not supported.

Remarks
There are other foreseeable fraud and security implications associated with replacing server to server communication and legal contracts with browser based APIs that are not within the scope of this assessment.

Algorithm Integrity Guarantee

Supported
Not Supported

Description
Today, a contract exists with Google when services are used that sets obligations on the parties concerning the use and processing of data.

Conversely, within the Privacy Sandbox, there is no guarantee the PAAPI algorithms making decisions on my behalf or about my business are implemented as per the specifications in public or adhere to requirements laid out in material instructions.

Assessment
The Privacy Sandbox API specifications, when sufficiently clear, set an expectation among those interfacing with Chrome concerning the data processing that will take place when used. However there is no mechanism available in Privacy Sandbox or Chrome APIs to guarantee that the API is implemented as per the specification.

Remarks
There are other foreseeable fraud and security implications associated with replacing server to server communication and legal contracts with browser based APIs that are not within the scope of this assessment. In an ideal scenario, Google Chrome source code executing PAAPI and other associated APIs will be open source and available for verification by any party.

Business Impact

Analysis of expected impact to businesses based on the technical evaluations.

Audience Management

Use cases related to creating, managing and addressing audiences in partnerships

Summary Media owner audience creation and management is possible albeit quite different to mechanisms used today; however, the ability of brands and their media agencies to create, manage and activate audiences is severely degraded.

Exclusion Targeting

Degraded
Without the ability to exclude certain users from seeing a specific advertisement, every advertising campaign, regardless of strategy (i.e. new customer acquisition, A/B testing, competitive separation, etc.) will be less performant and more expensive for brands.

Implications
For Brands And MediaAgencies
The core benefit of exclusion targeting lies in its ability to increase the efficiency of advertising spend by avoiding waste on impressions that are unlikely to drive additional value. The lack of support for exclusion targeting carries substantial business, financial, and operational implications. Exclusion targeting is pivotal for optimizing ad spend by ensuring ads are not shown to users the brand does not want to address with the given campaign. Without this capability, advertisers risk wasting significant portions of their budget and reducing the overall efficiency and effectiveness of their campaigns. This inefficiency can lead to diminished return on investment, as the advertising spend does not contribute to the campaign goal. For small to mid-sized companies, the impact is even more pronounced due to their limited advertising budgets. Financial resources could be strained, diverting funds from other critical growth areas and hampering the brand's ability to achieve its goals efficiently.

For Publishers and Media Companies
Not supporting exclusion targeting can lead to a decrease in ad revenue, as media owners may choose to allocate their budgets to walled gardens. For small to mid-sized publishers, who may already be facing intense competition from larger entities with more advanced ad tech capabilities, the inability for media owners to offer exclusion targeting could further erode a publisher’s market position. They risk losing valuable advertising partners to competitors, impacting their financial stability.

Create and Modify an Audience Across Domains

Not Supported

While it is reasonable for a publisher to generate an audience across multiple domains using the Protected Audience API (PAAPI), targeting of this Interest Group outside PAAPI is notably more complex involving multiple different technologies to achieve the same outcome. This limitation will hinder publisher adoption as first party audiences are more easily generated and passed to buyers through the use of a variety of 3rd party vendor solutions and existing header bidding signal passing capabilities.

In essence, the support of audience segments in this context excludes existing technology solutions and is only leverageable by Privacy Sandbox enabled systems.

Implications

For Brands and MediaAgencies

The capability to create custom audiences across diverse domains and make real-time adjustments gives advertisers the assurance that their messages reach the right audience at the right time. However, without support for fluid audience modification, advertisers, particularly smaller ones, may face significant operational challenges. Managing and updating audience pools is crucial to campaign effectiveness and cost-efficiency. Legal and financial considerations come into play as well as data privacy compliance, especially as it pertains to deletion requirements, meaning potential legal risks need to be carefully managed. Without proper support, advertisers may find it challenging to navigate these complexities.

For Publishers and Media Companies

Enabling publishers to create and modify audiences across multiple domains presents additional revenue opportunities, typically to provide incremental reach of audiences not only across their O&O properties, but also through their “audience extension” offerings. However, without support for fluid audience modification, smaller publishers may encounter operational hurdles. Adapting to changes in audiences, especially based on recency, can be resource-intensive and complex. Legal compliance and data privacy obligations also require careful attention. Publishers, irrespective of size, must consider the implications of not offering this feature, as it can impact their competitiveness, scaling of audiences and operational efficiency.

Look-alike Modeling

Not Supported

Look-alike modeling and targeting, a subset of prospecting, is commonly leveraged by marketers through programmatic buying channels. With the retirement of identifiers and no suitable replacement from Privacy Sandbox work, this method of customer acquisition will no longer be a reasonable marketing solution.

Implications

For Brands and Media Agencies

Look-alike modeling allows brands to extend their reach beyond their existing customer base, targeting new users who share characteristics with their "seed audience." This approach is fundamental for efficiently scaling campaigns while maintaining a high degree of relevance and engagement potential. Without this capability, advertisers would face challenges in reaching potential customers who may be interested in their products or services, leading to less effective advertising efforts. The implications are particularly stark for small to mid-sized companies, which often have limited marketing budgets and need to ensure that every advertising dollar is spent as effectively as possible. Without look-alike modeling, these companies risk higher customer acquisition costs and lower overall campaign effectiveness, which could hinder growth and reduce their competitive edge in the market.

For Publishers and Media Companies

Look-alike modeling plays a pivotal role in attracting and retaining advertisers, particularly those focused on new customer acquisition campaigns. It relies on cutting-edge data analysis and machine learning techniques, including bid stream modeling, to users resembling a campaigns desired audience. Platforms that can't support these methods risk losing appeal to advertisers striving to maximize campaign efficiency. This challenge is more pronounced for small to mid-sized publishers and ad tech providers competing with larger counterparts offering more advanced capabilities. Look-alike modeling greatly contributes to optimizing ad inventory value by helping publishers tailor their offerings to advertisers' preferences. Without access to such modeling, publishers, especially smaller ones, may struggle to meet advertiser demands, potentially leading to decreased ad revenue and a reliance on lower-value ad networks, hindering effective content monetization.

Add a user to an Audience, Even if They Have Not Visited My Site

Impractical

Technical and commercial requirements needed to satisfy this use case under Privacy Sandbox will be out of reach for many existing data providers. However, cookieless audiences will be available via OpenRTB auctions.

Implications

For Brands and Media Agencies

Advertisers will need to allocate significantly more financial and operational resources to compensate for the operational cost imposed by Interest Group creation, increasing their overall marketing costs. Operationally, it might result in less efficient campaigns, as advertisers struggle to reach their desired audience. The impact on small to mid-sized brands can be even more pronounced. These companies often operate with tighter budgets and limited resources, making efficient ad spend crucial. Legally, small to mid-sized brands may face increased compliance risks if they attempt to work around these limitations without the proper tools or expertise.

Operationally, it will require significantly more manual effort and time to manage campaigns effectively, further stretching their resources.

For Publishers and Media Companies
From a publisher's perspective, not supporting the creation of Interest Groups for brands can also have far-reaching implications. Business-wise, publishers may see a reduction in demand for their ad inventory, as media owners seek more efficient ways to reach their desired audiences. Financially, this limitation may lead to decreased ad revenue, affecting their bottom line. Operationally, publishers may struggle to deliver the level of targeting and personalization that advertisers and users increasingly expect. Small to mid sized publishers face a particularly challenging situation. With limited resources and less diverse user bases compared to industry giants, they rely on efficiently leveraging their user base to attract advertisers. Financially, the loss of revenue can hinder their ability to invest in content creation and platform improvement. Operationally, it may necessitate a more manual and less efficient approach to ad management, affecting their overall competitiveness in the market.

Auction Dynamics

Use cases dealing with offering inventory to buyers, receiving bids, and selecting a winning bid.

Summary: Traditional ways of running the request/response protocol are entirely different when running Protected Audience Auctions. Programmatic Supply Chain constituents will need to carefully weigh the constrained addressability capabilities provided by the Privacy Sandbox against the ability to do many foundational things in cookieless environments (once deprecated) using traditional OpenRTB.

Target a Single Campaign to My Online Audience

Supported
Advertisers and media buyers are able to serve targeted ads to Interest Groups, regardless of where the user/browser joined the Interest Group. However, it should be noted that Interest Groups are not specific to a brand, but to the interest group owner.

Implications
For Brands and Media Agencies
Adjustments in advertising strategies are necessary when it comes to "remarketing" to existing audiences. Advertisers are tasked with transitioning from their reliance on third-party cookies to cohort-based targeting, which clusters users with similar interests and behaviors into Interest Groups. This shift demands a heightened focus on comprehending and segmenting their audience to align with these cohorts.

This can pose substantial challenges, particularly for smaller to mid-sized businesses that may lack a sufficiently extensive audience pool to create Interest Groups. From a financial perspective, it is uncertain whether this transition will be as effective and efficient at retargeting pre-existing audiences currently, given the significant changes in targeting methods and the potential challenges smaller to mid sized enterprises might encounter due to operational inefficiencies introduced by Interest Groups. Note: Brands may message users who have visited their owned and operated website on that device across the web but it should be noted that it may only be used for a single Interest Group which is limited to a single campaign.

For Publishers and Media Companies
Publishers will have to adapt their monetization strategies. Publishers who focus on content quality and building strong audience relationships must now also allow Interest Group owners to embed their code directly on the webpage, necessitating direct integration with multiple companies.

Avoid Bidding Against Myself

Not Supported
A DSP's job is to spend the marketers budget as effectively as possible. In cases where a DSP posts two bids for the same auction, they can and often do lose to themselves, paying the higher of the two prices they've submitted. Had they only submitted the lower bid they'd have saved their advertiser's budget to buy additional impressions. In typical RTB auctions DSPs have made significant investments to minimize the number of times they send in two bids for a single auction.

Implications
For Brands and Media Agencies
The inability to prevent submitting multiple bids that compete with each other can lead to several inefficiencies and challenges in digital advertising efforts, particularly for advertisers. This scenario, often referred to as "bid cannibalization," occurs when the same brand unintentionally competes against themselves for ad inventory, driving up the cost of ad placements without any additional benefit. Such internal competition can significantly inflate the CPM (Cost Per Thousand), as multiple bids from the same buyer increase the auction price for an ad slot that they could have potentially won at a lower price. This not only wastes advertising budget but also reduces the overall efficiency and effectiveness of digital advertising campaigns. For small to mid sized businesses, which typically operate with more constrained advertising budgets, the financial impact can be particularly acute, potentially limiting their ability to compete for ad placements and achieve their marketing goals effectively..

For Publishers and Media Companies
The dynamics of multiple bids from the same buyer seemingly increasing competition for ad slots may, on the surface, appear beneficial, but over time, it can lead to a less healthy advertising ecosystem. As this scenario, often referred to as "bid cannibalization," persists,

buyers may adapt their strategies to offset these inefficiencies, potentially resulting in reduced overall bidding activity and a decreased willingness to pay premium prices for ad inventory and lower the number of websites where they spend media investment. Additionally, this practice can obscure the genuine demand for advertising space, posing challenges for publishers in accurately pricing their inventory and grasping market dynamics. Ultimately, this could erode trust in the advertising platform as buyers move media investment to walled gardens seeking more efficient inventory for their ad spend. Consequently, both buyers and publishers stand to benefit from mechanisms preventing multiple bids from the same entity competing with each other, thereby ensuring a more efficient and effective marketplace for digital advertising. Simultaneously, the lack of support for buyers to avoid submitting multiple competing bids can adversely impact publishers on several fronts. From a business standpoint, it disrupts ad auctions and diminishes the overall yield from their ad inventory, undermining the efficiency publishers rely on to maximize revenue, ultimately resulting in lower ad prices. Legally, this situation may raise concerns about the fairness and competitiveness of the ad ecosystem, potentially harming relationships with advertisers and regulatory compliance. Financially, publishers may forfeit revenue opportunities, especially when media investment is driven towards Walled Gardens. Small to mid-sized publishers, who often grapple with resource limitations, can be especially vulnerable in this scenario, lacking the infrastructure to efficiently manage bidding conflicts. This limitation hampers their ability to generate revenue and effectively compete with larger publishers in the market, exacerbating the challenges they face.

Competitive Separation

Not Supported

Competitive separation will still be available using traditional OpenRTB, but audiences will not be addressable using cookies once they have been phased out. Competitive separation will not work in Sandbox auctions. Media buyers will have to weigh the need for competitive separation in an semi-addressable environment using PAAPI against using non-cookie based audiences.

Implications

For Brands and Media Agencies

The absence of support for Competitive Separation can have substantial implications for brands. it can result in the inadvertent placement of a brand's content alongside messaging from their competitors, which can dilute the impact of their advertising efforts and confuse consumers. This scenario can lead to decreased brand recognition and potentially even the loss of customers to competitors. Legally, it may raise concerns regarding trademark and intellectual property rights, especially if the content of the competitor's ads infringes upon the brand's rights. Financially, the inability to ensure Competitive Separation can lead to wasted ad spend, as advertisers may unintentionally contribute to their competitors' visibility. Operational challenges may arise in managing and monitoring ad placements to prevent such occurrences. Small to mid-sized companies, operating with tighter budgets, may be particularly vulnerable, as these inadvertent placements can be costlier and more damaging to their market position.

For Publishers and Media Companies
The lack of support for Competitive Separation can also impact publishers, affecting their business in several ways. It can lead to brands' reluctance to have ads placed on a platform that does not support Competitive Separation. Brands may be hesitant to invest in advertising space if they fear their content will appear alongside that of their competitors, reducing the appeal of the platform. Operational challenges may emerge in managing ad placements to meet advertiser demands. Small to mid-sized publishers, already contending with resource constraints, may be disproportionately affected, as they rely on advertising revenue and may struggle to compete with larger publishers that can offer Competitive Separation assurances to advertisers.

Frequency/Recency Capping

Degraded
The current functionality in PAAPI does not allow for this cross-device, person-based frequency capping. It will result in more waste in budgets and a degraded, annoying end-user experience.

Implications
For Brands and Media Agencies
The degradation of the capability for advertisers to control how often a brand's ads are shown to the same user across various ad creatives, campaigns, or media companies has significant implications. Having control over ad frequency is vital for optimizing advertising effectiveness and efficiency. Without this capability, advertisers face the risk of overexposure, where users are bombarded with the same ad repeatedly, leading to ad fatigue. Ad fatigue not only diminishes the returns on advertising spend by reducing user engagement but can also harm the brand's image, causing users to feel overwhelmed or annoyed. This situation is particularly concerning for small to mid-sized businesses, where budget efficiency is paramount. Overspending on excessive impressions to the same users can quickly deplete limited advertising budgets, diverting resources from reaching new potential customers or reinforcing messages with users at critical decision-making stages.

For Publishers and Media Companies
From a business perspective, it can lead to brand dissatisfaction due to inefficient ad performance and a diminished ability to provide a positive user experience. Without effective frequency control mechanisms, advertisers with larger budgets could inadvertently dominate ad space, leading to a form of ad cannibalization where the same few ads are repeatedly displayed. This dominance can deter other advertisers from investing in the platform, as their ads are less likely to be seen, reducing the diversity of ad content available to users. Over time, this can limit the publisher's ability to accept and serve ads from multiple brands, affecting the platform's attractiveness and potentially diminishing ad revenue. The absence of frequency capping tools can thus have far-reaching implications for publishers, impacting their competitive

edge in the market, the user experience on their sites, and their capability to sustain a healthy mix of advertising clients.

Budget and Pacing

Temporarily Supported
The efficiencies afforded by the ability to run a campaign with a budget allocated across multiple line items is foundational to digital advertising. The operational cost of having to monitor and pace media investment individually will be exponentially more difficult, requiring significantly more FTE time from Ad Operations teams.

Implications
For Brands and Media Agencies
The ability to budget and pace campaigns effectively is essential for ensuring that advertising spend is allocated efficiently over the desired campaign duration. This capability allows advertisers to avoid exhausting their budget too early or underutilizing it, ensuring a steady and consistent presence in front of their target audience. Mastering the art of budget and pacing management is paramount to ensure that advertising spend is judiciously allocated throughout the campaign period. Ineffectively managing these aspects can result in overspending, which may only become apparent during late financial reviews, turning billing and reconciliation into a logistical nightmare, and/or result in make-goods from their ad tech partners. Similarly, underspending reflects missed opportunities for maximizing brand exposure and engagement. Both extremes pose significant issues: overspending unnecessarily drains valuable resources, while underspending fails to fully exploit market potential. These challenges are magnified for campaigns where strategic budget allocation is critical to achieve optimal reach without breaching financial limits. For small to mid-sized businesses, tight budget constraints make these challenges more pronounced, affecting their ability to maintain a competitive stance and market growth. The necessity for real-time adjustments in budget and pacing to avoid these financial pitfalls is crucial, underscoring the need for precise campaign management to ensure financial efficiency and prevent reconciliation complexities.

For Publishers and Media Companies
Providing tools and platforms that enable advertisers to budget and pace their campaigns effectively is crucial for building and maintaining strong advertiser relationships. When publishers have limited visibility into budget and pacing, it directly impacts inventory management and revenue. Advertisers' overspending can swiftly deplete available ad inventory, restricting availability for others and possibly leading to inflated costs due to heightened demand. On the flip side, underspending results in unutilized inventory, directly diminishing revenue prospects. The obscured view into advertisers' budget intentions complicates effective inventory allocation and pricing, potentially fostering inefficiencies within the advertising ecosystem. This highlights the critical need for advanced tools and analytics that assist advertisers and programmatic partners, especially those from small to mid-sized enterprises, in meticulously managing their campaigns. Such support is essential not only for advertisers

aiming to meet their marketing goals but also for ensuring consistent inventory demand, which aids publishers and ad tech vendors in navigating revenue management and strategic planning challenges. This approach also mitigates the risk of financial reconciliation becoming a cumbersome ordeal, thereby maintaining a fluid and efficient marketplace for all parties involved in the programmatic ecosystem.

Second Price Auction

Degraded

While not the only factor when evaluating bids, pricing is a very large piece of the equation. Some sellers rely on second-price information in conjunction with other signals such as campaign pacing or spend commitments, to determine if a bid should ultimately win. Second price auctions can also give buyers confidence that they're not significantly over paying for an impression opportunity.

Implications

For Brands and Media Agencies

In these auctions, the winning bidder pays slightly more than the second-highest bid, rather than their own maximum bid, allowing for potentially lower advertising costs. Should this capability be degraded or limited, advertisers, especially those with smaller financial resources, may face increased costs for ad placements. This change could force these smaller businesses to retool their digital advertising strategies, and/or endure reduced investment returns, adversely affecting their growth and competitive stance in the market. The challenge for advertisers in this shifted scenario is finding ways to remain visible and engaging to their target audiences without the cost benefits previously afforded by second-price auctions, making strategic bidding and budget management more critical than ever.

For Publishers and Media Companies

The traditional second-price auction model has been instrumental in maximizing ad inventory value by fostering a bidding environment where advertisers are encouraged to bid their true value. This approach has been particularly attractive to a broad spectrum of advertisers, including those from small to midsize companies, ensuring access to premium ad spaces at reasonable costs. However, if the efficacy of second-price auctions is compromised, publishers may struggle to balance achieving optimal inventory prices with keeping their ad spaces appealing to advertisers of all sizes. This shift could disproportionately impact small to mid-size publishers, who rely heavily on attracting a diverse advertiser base to sustain revenue streams. Publishers in this altered landscape must navigate the dual objectives of optimizing inventory revenue while adapting to auction models that maintain advertiser engagement and spending, critical for the health and diversity of the digital advertising market.

Bid Using a Deal ID

Supported

Degraded

While Deal IDs may be passed as a standalone value without issue in the bidstream, there is no mechanism to frequency cap or pace a campaign in real time. Buyers will not be able to leverage them as effectively as they can today. In cases where Deal IDs are necessary, they may still be leveraged as they are today in OpenRTB, just without the use of cookies (once deprecated).

Implications

For Brands and Media Agencies

The ability to create specific deals and engage in bid submissions is vital for creating deals between buyers and sellers of ad inventory. These deals enable advertisers to tailor their campaigns to specific inventory and create preferred terms with sellers, enhancing the efficiency of their ad spend. However, if this capability is degraded, advertisers may face challenges in securing favorable deals, leading to potentially higher costs. Smaller businesses, already operating with tight budgets, rely on such deals to maximize the impact of their advertising efforts. The degradation of this capability can hinder their ability to compete effectively and achieve the desired ROI, potentially impacting their financial stability and market position. Advertisers in this altered landscape must seek alternative ways to optimize their campaigns and navigate a more constrained programmatic advertising environment, making strategic deal-making and budget management even more critical.

For Publishers and Media Companies

The ability to create specific deals and engage in bid submissions is crucial for publishers to maximize the value of their ad inventory and maintain a diverse advertiser base. These deals allow publishers to offer tailored advertising opportunities that cater to the needs and preferences of their clients, attracting a wider range of advertisers, including small to mid-sized companies. However, if this capability is degraded, publishers may struggle to negotiate favorable deals and may see a reduction in the diversity of advertisers participating in their programmatic platform. Smaller publishers, heavily reliant on a broad advertiser base to sustain their revenue streams, could face more significant challenges. The degradation of this capability could impact their ability to generate revenue, compete with large publishers effectively, and maintain a healthy programmatic advertising ecosystem. Publishers must adapt to an environment where deal-making and bid submissions may become less flexible, requiring them to find innovative ways to retain advertisers and optimize their inventory value. Small to mid-sized publishers, in particular, may need to explore alternative revenue streams to offset potential losses from degraded programmatic deal-making capabilities.

Receive a “No Bid” Response from a DSP

Not Supported

Bid Response rates are not a viable option for sellers to analyze demand sources directly within PAAPI. Information gleaned from traditional OpenRTB will not be a suitable proxy for sellers to determine which DSPs are bidding on their inventory due to the additional layers of obfuscation outlined above.

Implications

For Brands and Media Agencies

The absence of bid request tracking and bid response insight can disrupt advertising strategies. Without the ability to monitor bid requests from publishers, advertisers risk inefficient allocation of their budgets and diminished ROI. This lack of visibility can be particularly challenging for small to mid-sized advertisers, who may have limited resources to navigate these complexities, potentially leading to wasted ad spend. From a financial perspective, the absence of comprehensive bid request tracking can impact cost-efficiency, potentially leading to media investment being biased towards a small number of publishers. In contrast, publishers' revenue opportunities may be hindered by not receiving bids from interested advertisers. This financial impact can be more pronounced for small to mid-sized advertisers, who operate with tighter budgets.

For Publishers and Media Companies

The inability to track bid requests and bid response reasons can disrupt operational efficiency. Publishers may struggle to optimize their inventory management and identify patterns in bidder behavior. This operational challenge can lead to missed revenue opportunities, particularly if publishers are unaware of why bidders are not responding. Moreover, the lack of distinction between bid response scenarios can hinder campaign optimization for publishers, making it difficult to allocate resources effectively. It's vital to address these issues to ensure transparent and efficient auction processes. Small to mid-sized publishers, in particular, may feel the operational bottlenecks more acutely, as they often rely on streamlined operations and cannot afford inefficiencies. Addressing the need for comprehensive insights into bid response rates is essential to maintaining fairness, transparency, and efficiency in the digital advertising ecosystem, benefiting both advertisers and publishers, regardless of their size.

Creative & Rendering

Use cases related to Invalid traffic, malware, acquiring assets for display, and ad rendering.

Summary: The rendering of static display ads are not impacted. Ad supported video is severely degraded, but there is an alternate path through traditional OpenRTB.

Use a VAST Tag

Not Supported

All traditional VAST implementations will not work in Privacy Sandbox using i-frames without significant development and re-working current ad tech stacks. Once Fenced Frames are required (no sooner than 2026), all ad support will be removed.

Traditional OpenRTB will continue to support VAST and auctions will run as they do today, just without cookies (once deprecated).

Implications

For Brands and Media Agencies

VAST Tags are a standard technology that streamlines the communication between ad servers and video players, ensuring seamless ad delivery. Without this support, advertisers may face challenges in ensuring their ads are displayed correctly across various video platforms and players, potentially leading to inconsistencies in ad appearance and performance. Small to mid-sized advertisers, who often rely on cost-effective and standardized solutions, may find it especially challenging to navigate the complexities of ad delivery without VAST Tags.

For Publishers and Media Companies

The absence of support for VAST Tags poses significant challenges in terms of monetizing video content and maintaining a smooth operational workflow. Publishers rely on VAST Tags to efficiently deliver video ads to their audiences while ensuring a consistent user experience. Without this support, significant disruptions and a subpar viewer experience are expected. This can result in user dissatisfaction, decreased viewer retention, and ultimately, reduced advertising revenue. Smaller publishers, for whom video content plays a substantial role in their revenue streams, may face particular hurdles in attracting advertisers who prefer VAST-compliant ad delivery. Moreover, without VAST support, publishers may struggle to effectively manage ad placements, optimize their inventory, and meet advertiser expectations. In an increasingly competitive digital advertising landscape, the inability to support VAST Tags can impede publishers' ability to remain competitive and financially sustainable.

Render a Video Ad Alongside Video Content

Not Supported

Traditional implementation of VAST will break without significant development, and are only expected to work until Fenced Frames are introduced.

Server Side Ad Insertion (SSAI) will continue to work as it does today because it is server side and existing Sandbox documentation deals only with client-side calls.

Implications

For Brands and Media Agencies

The ability to serve pre-, mid-, or post-roll video advertisements alongside video content is paramount for optimizing advertising campaigns, and it's especially beneficial for small to

mid-sized companies with limited resources. Video ads provide a powerful platform for engaging with target audiences, but if this capability is not supported, advertisers may miss out on a valuable channel for reaching potential customers. Smaller businesses, often operating with tight advertising budgets, rely on cost-effective video placements to maximize their impact. The absence of this feature can limit their ability to compete effectively and achieve their marketing objectives. Advertisers in this scenario must explore alternative ways to reach their audience, potentially diverting resources from other critical aspects of their advertising strategy.

For Publishers and Media Companies
The implications of not supporting the ability to serve pre-, mid-, or post-roll video advertisements alongside video content extend to publishers and media companies, especially concerning the monetization of their video assets. Video advertising represents a significant revenue source, with distinct price points for each placement, and publishers need the ability to control delivery and monetize inventory according to revenue potential or advertiser willingness to pay. Without this flexibility, publishers may face challenges in attracting and retaining advertisers seeking specific video placements. This shortfall can devalue their video inventory, potentially impacting ad revenue. Smaller publishers, often reliant on a diverse advertiser base, may be disproportionately affected, hindering their revenue generation, competitive standing, and advertising ecosystem sustainability. In this evolving landscape, where video ad placements vary in accessibility, publishers must seek alternative strategies to offset potential revenue losses. Small to mid-sized publishers, in particular, may need to diversify their content offerings or explore additional monetization avenues to maintain financial viability and cater to advertisers' pricing preferences.

Render Video Ads Without Content

Temporarily Supported
Standalone video ads that serve without content will be the only supported format in Protected Audience Auctions. Support will be removed after fenced frames are required, which will not be before 2026.

Implications
For Brands and Media Agencies
The capability to serve standalone video ads in players without editorial video content is essential for advertisers, providing an avenue for delivering impactful video campaigns. These standalone video creatives often auto-close after the ad's video has finished playing, ensuring a seamless user experience. However, if this functionality is not supported in the long term meaning, advertisers, especially small to mid-sized companies, may eventually encounter several challenges. Firstly, they might lose a valuable advertising format, limiting their ability to engage audiences through compelling video content. Secondly, without the auto-close feature, advertisers may struggle to control the user experience and message delivery effectively. This limitation can lead to longer ad exposure times or user interactions that are not aligned with the

campaign's goals, impacting the efficiency of their advertising spend. Smaller businesses, with tighter budgets, rely on cost-effective and impactful ad formats, making the absence of this feature particularly detrimental to their advertising efforts. Advertisers in this scenario must seek alternative ways to create engaging video campaigns and may need to allocate additional resources to manage ad placements effectively.

For Publishers and Media Companies
The implications of not supporting the ability to serve standalone video ads in players without editorial video content extend to publishers and media companies, particularly when it comes to monetizing their inventory. Standalone video ads offer a valuable format for advertisers looking to deliver impactful messages, and if this functionality is lacking, publishers may struggle to attract and retain advertisers seeking this format, which is especially critical for those where video comprises a significant portion of their revenue. This shortfall can lead to a decrease in the perceived value of their ad inventory, potentially impacting ad revenue. Smaller publishers, often reliant on a diverse advertiser base, may be disproportionately affected. The absence of this feature could hinder their ability to generate revenue, compete effectively, and maintain a sustainable advertising ecosystem. Publishers must adapt to an environment where standalone video ad placements become less accessible, requiring them to explore alternative strategies to offset potential revenue losses. Small to mid-sized publishers, in particular, may need to diversify their ad formats or explore other monetization avenues to remain financially viable.

Render Native Ad on Web

Not Supported
At publication time, no forms of Native advertising are supported in Protected Audience Auctions, but there are ongoing conversations to determine long-term support.

Implications
For Brands and Media Agencies
The lack of support for serving non-HTML ads, including formats like JSON or raw assets such as MP4 or JPGs, as well as 'seller-rendered native' scenarios, can have multifaceted implications for advertisers, affecting their business and operational strategies. Advertisers often rely on diverse ad formats to reach their target audiences effectively. Without the ability to serve non-HTML ads, they may find it challenging to leverage these formats for creative and engaging campaigns. This limitation can hamper their ability to deliver visually appealing and interactive ads, potentially leading to reduced audience engagement and conversion rates. Additionally, in 'seller-rendered native' scenarios, where sellers provide the final ad markup, the absence of support can disrupt the ad creation process, potentially leading to delays and misalignment between buyers and sellers. Small to mid-sized advertisers, who often seek cost-effective solutions and flexibility in their ad creatives, may find it particularly difficult to navigate these limitations. Furthermore, the inability to support diverse ad formats can hinder their ability to innovate and compete with larger advertisers in the market.

For Publishers and Media Companies

The lack of support for serving non-HTML ads and 'seller-rendered native' scenarios can impact publishers in terms of monetizing their ad inventory and streamlining operational processes. Publishers rely on flexibility in ad formats to attract a diverse range of advertisers and effectively utilize their ad spaces. Without support for non-HTML ads, publishers may struggle to accommodate advertisers seeking these formats, potentially limiting their ability to secure premium ad placements and command higher ad rates. Additionally, in 'seller-rendered native' scenarios, the absence of support can disrupt the collaboration between publishers and buyers, leading to operational inefficiencies and miscommunication. Smaller publishers, who may heavily rely on streamlined processes and quick turnaround times, may face disproportionate challenges in managing these limitations. The inability to support diverse ad formats and seller-rendered native scenarios can impact their competitiveness in the digital advertising landscape and their ability to maximize revenue. As a result, publishers may need to adapt by exploring alternative monetization strategies and finding ways to bridge the gap between advertisers' expectations and available capabilities.

Render Responsive Display Ad on Web

Supported

Ads can render in fixed pixels or aspect ratios, but when employing Protected Audience Auctions, advertisers are required to include their size and shape parameters prior to a campaign running, whereas today advertising technology has the ability to dynamically resize ad creatives based on the device

Implications

For Brands and Media Agencies

Responsive ads can enhance user engagement by delivering a seamless and visually appealing experience across various devices and screen sizes. However, the limits imposed by Protected Audience Auctions around the use of responsive ads may result in poor user experience which creates negative sentiment for the brand or missed opportunities to bid on inventory if the exact size and shape parameters aren’t met. Advertisers may find themselves constrained by fixed ad dimensions, limiting their ability to tailor ad experiences to different user contexts. Small to mid-sized companies, with limited resources, may find it financially burdensome to redesign their ad creatives and adapt to these changes. The absence of responsive advertising could disadvantage them further in a competitive market. Creating ads in different sizes, across devices and screen resolutions, can be a costly and time-consuming endeavor. Such financial constraints could potentially put these businesses at a disadvantage in a fiercely competitive market.

For Publishers and Media Companies

Responsive ad formats can enhance user experience on their websites, potentially increasing user engagement and revenue. Publishers can cater to a broader range of advertisers who seek versatile ad placements. However, the adoption of Privacy Sandbox may necessitate adjustments in their website layout and ad placement strategies. Small to mid-sized publishers may encounter operational bottlenecks during this transition, especially if they lack the resources to swiftly implement these changes. If there is no or limited support for responsive ad formats, user experience on their websites may suffer, potentially leading to decreased user engagement and, consequently, reduced revenue. Publishers may struggle to cater to advertisers seeking versatile ad placements that adapt to different user devices and screen sizes. The absence of responsive ads may necessitate significant adjustments in their website layout and ad placement strategies, resulting in operational challenges. Small to mid-sized publishers, with limited resources, may find these challenges particularly daunting, potentially impacting their competitiveness in the digital landscape and their ability to offer effective ad placements to advertisers.

Render Ads that Interact with a Website

Temporarily Supported
Once Fenced Frames are introduced, ad units with responsive design (i.e. can change dimensions based on the environment into which they are served) that do not have a fixed size will rely solely on OpenRTB auctions that will not be addressable using 3rd party cookies (once phased out).

Any ad design that changes shape after it has loaded on a page or once the user interacts with it will be restricted from Sandbox opportunities.

Implications
For Brands and Media Agencies
It's common practice for advertisers to harness the power of rich media expandable ad units. These dynamic ad formats are designed to captivate and entertain, ultimately amplifying brand awareness. They provide a canvas where advertisers can truly showcase their brand's value and convey their message in an engaging manner. In contrast, standard HTML5 or GIF/JPEG banners often fall short in providing the necessary space to deliver the full impact of a brand's message.

The absence of interactive ad experiences poses the risk of reduced user engagement and the inability to craft dynamic and relevant content tailored to their target audiences. This, in turn, makes it difficult for advertisers to effectively communicate their messages and keep audience interest alive.

For Publishers and Media Companies
The absence of support for rendering ads with interactive capabilities within Privacy Sandbox can have significant repercussions. It's worth noting that these types of placements, such as

homepage takeovers, often come at a premium because they possess the unique ability to break through the clutter on a website. Interactive ads, in particular, play a pivotal role in elevating user engagement, resulting in higher revenues for publishers. When advertisers can deliver interactive and captivating ads, it translates into more engaged users for publishers, which, in turn, can attract more advertising spend. This heightened engagement enhances the earning potential of publishers.

In a scenario where publishers are unable to offer such interactive ad experiences, they may encounter challenges such as reduced ad demand and potentially diminished revenue streams. Advertisers could start exploring more engaging platforms elsewhere, putting additional pressure on publishers. Moreover, publishers would have to rely solely on OpenRTB auctions for these kinds of ad units, potentially limiting their ability to fully monetize their inventory.

Creative Quality Assurance and Malware in Creatives

Not Supported
Publishers should negotiate quality controls with their ad tech partners responsible for the creative registration process *a priori* to running a Protected Audience Auction.

Implications
For Brands and Media Agencies
Advertisers may encounter prolonged delays in getting their ads served on a publisher's site, especially if there is no support for publishers' ability to view and assess advertisements for quality assurance. This situation can pose challenges for advertisers in ensuring that their creative materials meet the exacting quality standards set by publishers. This cautious approach could potentially result in pacing and budgetary challenges, particularly for time-sensitive campaigns, such as product launches, where delays in ad delivery could carry significant consequences.

For Publishers and Media Companies
The inability to directly access and analyze advertisements for quality assurance within Privacy Sandbox can significantly impact publishers. Each publisher has their own set of ad guidelines, and some may have stricter policies concerning the types of images used or the ad copy, as well as other criteria they deem as inappropriate content. Publishers also need to ensure that ads do not introduce user experience issues or increase the load on their web pages.

The absence of pre-approval and previewing capabilities also exposes publishers to risks like malware, which could result in financial disputes involving buyers, sellers, and ad tech partners. These challenges, with legal, financial, and operational implications, can impact user experience and financial stability, especially for small to mid-sized publishers.

Publishers might feel compelled to establish extended processes for lightly serving impressions to ensure ad compliance, which can introduce inefficiencies and delays.

Invalid Traffic

Impractical
It's imperative to acknowledge the constant efforts of "bad actors" seeking to exploit the system. These organizations continually devise new and sophisticated methods to undermine digital advertising to receive media investment meant for legitimate publishers. To stay ahead of these fraudulent activities and maintain trust in the industry, ad tech companies must have the ability to collect data and monitor for anomalies and emerging tactics employed by these bad actors.

The Media Rating Council (MRC) Invalid Traffic Detection and Filtration Guidelines stipulate that measurement provider should furnish Gross (unfiltered) and Net (filtered for General Invalid Traffic - GIVT) as well as Total Net Metrics (filtered for any and all Invalid Traffic, including General and Sophisticated IVT) for both rendered impressions, viewable impressions and clicks. These requirements are essential in ensuring transparency and accuracy in the measurement of digital advertising performance.

Implications
For Brands and Media Agencies
The absence of IVT data disrupts strategic decision-making, potentially leading to misguided advertising strategies and inefficient resource allocation. Legal consequences may arise from inadvertently engaging in fraudulent activities, jeopardizing compliance and reputation. Operationally, logistical challenges emerge as distinguishing genuine engagement from fraudulent interactions becomes problematic, impacting campaign optimization. Financially, inefficient spending on unfiltered invalid traffic depletes budgets and diminishes ROI, hindering business growth. Operational inefficiencies arise as identifying and filtering invalid traffic becomes challenging, reducing campaign effectiveness.

For Publishers and Media Companies
In the absence of Invalid Traffic (IVT) data carries notable implications. Strategically, it disrupts decision-making, hindering Publishers' ability to optimize content placement and ad inventory, potentially leading to missed revenue opportunities. Legally, it exposes them to regulatory risks, as non-compliance due to fraudulent activities can result in fines and industry reputation damage. Operationally, the lack of IVT data creates logistical challenges, making it harder to differentiate genuine interactions from fraudulent ones and impacting ad placement effectiveness. Access to reliable IVT reporting is essential for publishers and media companies to make informed decisions, comply with regulations, and maintain their competitive edge in the digital advertising landscape.

Concerns from both buyers and sellers around potential weaknesses include the reliance on issuer authentication methods which could be exploited, the complexity of the APIs, limited

issuers per publisher, incomplete documentation, and vulnerability to deception by malicious actors.

Loss of Runtime Data for Brand Safety

Not Supported
Removing the primary mechanism used to determine if a piece of inventory is appropriate to receive a brand's message is a linchpin of the digital advertising ecosystem. Brands requiring this information are encouraged to weigh the addressability capabilities provided by PA APIs against the need to employ brand suitability analysis in traditional OpenRTB auctions.

Implications
For Brands and Media Agencies
The absence of reliable top-level page URL data for brand safety decisions has substantial business and operational implications. Without this crucial signal, AdTech companies may struggle to accurately determine whether or not to display an advertiser's creative on a webpage. This can result in increased risks of brand misalignment, potentially damaging the advertiser's reputation and effectiveness. For small to mid-sized companies, this lack of support can be particularly challenging as they may lack the resources to implement alternative solutions or navigate complex workarounds, potentially leading to missed opportunities and revenue losses.

For Publishers and Media Companies
The absence of dependable top-level page URL data poses significant business, legal, financial, and operational challenges. Publishers heavily rely on this information to ensure brand safety and compliance with industry standards. Without it, they may face legal issues if inappropriate content is displayed on their websites, potentially leading to legal liabilities and damage to their reputation. From a financial standpoint, publishers may experience reduced demand for their inventory due to advertisers' hesitancy to display ads without reliable brand safety measures. This could adversely affect their revenue streams. Moreover, operationally, the absence of top-level page URL data complicates the integration process with AdTech partners, requiring extra efforts to implement alternative methods. For small to mid-sized publishers, these challenges can be even more burdensome, as they may lack the resources and bargaining power to negotiate favorable terms with AdTech vendors, potentially putting their businesses at a disadvantage in the digital advertising ecosystem.

Auction Latency

At time of publication, there is no enumerated value for delays in page loading caused by Protected Audience Auctions, other than to note there will likely be some latency introduced. Constituents of the programmatic ecosystem will need to carefully analyze the costs and

benefits of running Protected Audience Auctions alongside the issues caused by the latency they experience.

Implications

For Brands and Media Agencies

The failure to meet the 100ms latency threshold in auctions can directly impact customer satisfaction and engagement. Advertisers may witness a decline in user satisfaction with the web pages where their ads are displayed. This reduced satisfaction can, in turn, lead to a decrease in customers' willingness to click on advertisements. Moreover, small to mid-sized companies in the advertising space may face even more significant challenges. These companies often have limited resources and may struggle to adapt to the increased technical demands imposed by the latency requirements. It could lead to a competitive disadvantage, hindering their ability to effectively compete with larger players who can invest in optimizing their ad-tech solutions. Additionally, the lack of clear performance guidelines within PAAPI may result in uncertainty and potential disputes between advertisers and publishers, further complicating business relationships.

For Publishers and Media Companies

Publishers rely on the efficient delivery of ads to generate revenue, and any latency can disrupt this revenue stream. When auctions take longer than the specified 100ms, publishers risk a decline in customer satisfaction with their websites due to slow loading times, which can lead to decreased user engagement and ad clicks. Small to mid-sized publishers may find it particularly challenging to cope with the latency constraints imposed by PAAPI. They may lack the technical infrastructure and resources needed to optimize their ad delivery systems to meet these requirements. This discrepancy in capabilities can create disparities in the competitive landscape, potentially favoring larger publishers with more substantial investments in technology and operations.

Reporting

Use cases related to measuring advertising from request to conversion to lifetime value

Summary: All aspects of reporting are severely degraded, especially as it pertains to independent validation, troubleshooting potential issues and billable amounts.

Bid Price Reporting for Winners

Degraded

The consequences of a compromised Bid Price Reporting system are made more challenging by the intricate dynamics of seller's scoring functions, where the winning bid may not necessarily match the highest-priced bid due to various factors, including scoring algorithms. This complexity can create additional difficulties, impacting businesses of all sizes within the digital advertising ecosystem and potentially leading to legal disputes and financial losses.

Implications

For Brands and Media Agencies

Understanding the degree of overpayment is crucial for optimizing advertising spend and ensuring a competitive edge. If this functionality is compromised, it can lead to inefficiencies and resource waste, impacting both large corporations and small to mid-sized businesses. It may also raise questions about transparency and fairness in advertising auctions, potentially resulting in legal disputes that could affect companies of all sizes. Financially, overpayment can strain budgets, and operational efficiency can be compromised when trying to analyze campaign performance and make necessary adjustments, particularly affecting smaller companies that rely on cost-effective strategies.

For Publishers and Media Companies

Publishers depend on accurate reporting and fair compensation for their ad inventory. If the reporting of the highest losing bid price is affected, it can lead to disputes with advertisers, impacting revenue streams for all publishers. Legally, it can raise concerns about contract compliance and compensation agreements, potentially leading to legal disputes that affect the entire industry. Financially, inaccurate reporting can result in revenue losses, affecting the sustainability of media companies of all sizes. In terms of operations, publishers rely on transparent and efficient auction mechanisms, and any degradation can disrupt their workflow, especially affecting smaller players who rely on stable revenue streams for growth and survival in the competitive landscape.

Second Price Auction Reporting

Temporarily Supported

Once support has been removed, only the winner of the auction will be able to see the price of the second highest bid. Publishers will not be able to evaluate losing bids in any capacity, second price or otherwise.

Implications

For Brands and Media Agencies

Once support has been removed, the absence of transparency in reporting on the winning and second-highest bid in an auction can have profound repercussions for advertisers. This lack of visibility can severely impede advertisers' ability to make informed decisions regarding their bidding strategies, potentially resulting in suboptimal outcomes. However, the impact is particularly pronounced for small to mid-sized companies, which often operate with limited resources, making it challenging to absorb the negative effects of inefficient bidding.From a legal perspective, this deficiency may give rise to concerns surrounding the fairness and transparency of the auction process, potentially triggering regulatory scrutiny. Addressing regulatory issues can be not only be time-consuming but also financially burdensome. In addition to the legal implications, there are significant financial consequences. Advertisers may miss out on valuable opportunities to optimize their advertising spend efficiently, and

operationally, the absence of comprehensive data on losing bids can impede the analysis of campaign performance, making it arduous for advertisers to fine-tune their advertising strategies. This lack of support doesn't discriminate; it affects both larger industry players and smaller companies, placing them at a disadvantage in the fiercely competitive landscape of digital advertising.

For Publishers and Media Companies
The absence of support can impact publishers' ability to assess the value of their ad inventory accurately, potentially leading to undervaluation. Small to mid-sized publishers, in particular, rely heavily on revenue generated from their ad space, so any discrepancies in bid evaluation can directly impact their bottom line. Legally, it may raise concerns about transparency and fairness in ad auctions, potentially leading to disputes with advertisers or regulatory challenges. Financially, publishers may miss out on potential revenue by not being able to optimize their pricing strategies effectively. Operationally, the lack of insights into losing bids can hinder their ability to refine their inventory management and content strategies, affecting both their revenue and user experience. In this context, ensuring support for transparent bid reporting is vital for the sustainability and competitiveness of all players in the digital advertising ecosystem.

Bid Loss Reporting

Not Supported
Reporting on auction state for all bids (including non-winning bids) will require significant added complexity for SSPs and DSPs. During the transitional period while third-party cookies are still available, the Temporary Auction Reporting API is an option for debugging, but that API is probably unsuitable for generating customer-facing reports or automatic optimization.

Until the industry gains experience attempting to use the Private Aggregation API, it will be difficult to assess whether aggregate reporting can be a suitable replacement for the observability mechanisms inherent to today's server-side auctions under direct control by SSPs and DSPs.

Implications
For Brands and Media Agencies
Without insights into why a bid did not win, advertisers may struggle to optimize their bidding strategies effectively, leading to potential inefficiencies and wasted ad spend. This lack of transparency can also impact customer support, making it challenging to address client inquiries and concerns, especially for small to mid-sized companies that rely on responsive and tailored solutions. The absence of clear bid data may raise compliance issues, potentially exposing companies to legal risks. Financially, inefficient bidding can lead to higher costs per acquisition, negatively affecting the bottom line. Operationally, debugging and machine learning for optimization become more challenging, slowing down progress in the highly competitive digital advertising landscape.

For Publishers and Media Companies
Without transparency, publishers risk losing business opportunities and revenue. Financially, publishers may face difficulties in setting fair pricing strategies, impacting their profitability. Operationally, understanding the dynamics of auctions and optimizing yield becomes an uphill battle, hindering the ability to thrive in a competitive market. In summary, the implications of not supporting detailed bid information have far-reaching consequences for both advertisers and publishers, with small to mid-sized companies particularly vulnerable in these areas.

Publisher Revenue Accrual and Impression Validation

Not Supported
Publishers are reliant on their ad server and each component seller to ensure that the integration is working correctly, and that the top level server trusts each component seller, whereas today integration issues are quickly surfaced by these reconciliations of javascript events with impression pixel counts.

Implications
For Publishers and Media Companies
Publishers rely on the ability to fire a pixel that directly logs ad events into their database for both business and operational reasons. If this capability is not supported, it has far-reaching implications, especially for small to mid-sized companies. Without the ability to independently track and log ad rendering events, publishers would have to rely solely on their ad tech partners for this data. This reliance not only poses operational challenges but also raises legal and financial concerns. Small to mid-sized companies, in particular, may find it challenging to negotiate favorable terms with ad tech partners and could face potential disputes over revenue sharing and data ownership, which could strain their financial resources.

Measure Viewability of an Advertisement

Temporarily Supported
At time of publication, once support for iframes has been removed (not before 2026), there is no mechanism for DSPs and verification vendors to determine the viewability of a given ad.

Advertisers actively exclude sites that fail to meet the viewability standards and necessary thresholds. If advertisers lack confidence in a site's viewability rate, it's highly likely that they will opt to exclude it from their ad buys.

Implications
The Media Rating Council (MRC) Viewable Ad Impression Measurement Guidelines stipulates a served ad impression can be classified as a viewable impression if the ad was contained in the viewable space of the browser window, on an in-focus browser tab, based on pre-established

criteria such as the percent of ad pixels within the viewable space and the length of time the ad is in the viewable space of the browser. It is recognized that an “opportunity to see” the ad exists with a viewable ad impression, which may or may not be the case with a served ad impression.The impression must be rendered and meet the current requirements for a valid served ad impression as specified by the MRC Desktop Impression Measurement Guidelines, with the exception of those ads counted as served utilizing a “Cout on Decision methodology.

For Brands and Media Agencies
When there isn't robust support for measuring the percentage of ad visibility on a screen, it puts advertisers in a precarious position. The accuracy of their ad measurement data, a vital aspect of assessing the effectiveness of their advertising campaigns, becomes compromised. This lack of certainty can have significant ramifications for their strategies. If and/or when this is not supported, the ability to measure the percentage of ad visibility on the screen becomes significantly compromised. This affects the accuracy of the data that is crucial for assessing advertising campaigns.

Moreover, if the winning ad is served within a fenced frame, the inability to access dimension and position information about the outer frame hinders viewability measurement. This, in turn, impacts ad performance evaluation and optimization, affecting businesses of all sizes in the competitive advertising landscape. In such scenarios, the inability to access dimension and position information about the outer frame becomes a hindrance to viewability measurement. This, in turn, has a cascading effect on ad performance evaluation and optimization. The competitive landscape of the advertising industry means that these challenges impact businesses of all sizes, making it imperative for advertisers to navigate these issues effectively.

For Publishers and Media Companies
Legal and operational challenges may arise, especially concerning contracts and agreements with advertisers. Publishers may find themselves in disputes regarding ad viewability and performance metrics, potentially leading to financial repercussions. Smaller and mid-sized publishers, who often rely heavily on advertising revenue, could face significant difficulties if they cannot assure advertisers of accurate ad measurement and viewability. The planned removal of support for iframes (which will not be before 2026) also affects publishers, as it limits their ability to provide valuable metrics to advertisers and could impact their competitiveness in the market. In summary, the failure to support the resolution of ads within fenced frames poses challenges across business, legal, financial, and operational aspects, affecting companies of all sizes in the advertising ecosystem.

Reporting by Deal ID

Temporarily Supported
While deal ids may be used to decide in real time, the lack of reporting will make it more difficult to troubleshoot technical issues when/if they exist. It will not be possible to identify technical issues that result in no bid or not winning the auction.

Implications

For Brands and Media Agencies

Without detailed insights into impressions, wins, and other key metrics tied to Deal IDs, advertisers may struggle to optimize their campaigns effectively. This lack of granularity hinders the ability to gauge the performance of specific deals, potentially resulting in inefficient spending and missed opportunities. Smaller to mid-sized businesses, with limited resources, may find it particularly challenging to compete without this level of data, and cause financial uncertainties, operational hurdles, and difficulties in troubleshooting technical issues related to bid outcomes or winning auctions.

For Publishers and Media Companies

It becomes difficult to offer transparency and value to advertisers, potentially leading to strained relationships and revenue loss. Financially, revenue streams may dwindle as advertisers hesitate to invest in ad inventory without robust reporting. Operationally, maintaining strong partnerships becomes challenging, with smaller publishers struggling to meet advertisers' demands for transparency and facing difficulties in troubleshooting technical issues related to bid outcomes or winning auctions..

Billable Metrics - CPA

Not Supported

Protected Audience auctions are not appropriate for Advertisers running Cost per Click or Cost per Acquisition campaigns, but traditional OpenRTB will have continued support, just without the use of cookies (once deprecated). If PAAPI offers the only solution for audience targeting, this diminishes the possibility of a positive ROI for performance-based advertising.

Implications

Regardless of whether advertisers are transacting on CPA or simply calculating the Cost Per Acquisition (CPA), the absence of reliable conversion data has significant implications for advertisers, publishers and affiliate partners, with notable consequences for small to mid-sized companies. This situation can disrupt the advertising ecosystem, leading to financial inefficiencies, disputes, and legal challenges. Small to mid-sized companies may experience more pronounced difficulties, affecting their competitiveness and financial stability in the digital advertising landscape. Finding solutions to ensure accurate tracking and reporting of conversion data remains a critical priority for the industry and businesses across the spectrum.

For Brands and Media Agencies

Cost Per Acquisition (CPA) is a pivotal metric that shapes and informs where advertisers invest their resources. Whether they are transacting directly based on it or using it as an internal performance benchmark, CPA serves as the cornerstone for gauging campaign efficacy. The absence of dependable conversion data hinders their ability to make informed decisions regarding budget allocation. This can result in suboptimal spending decisions, where resources

are not directed towards campaigns that yield actual acquisitions, a concern particularly pressing for small to mid-sized companies with limited marketing budgets. In this context, CPA becomes the vital yardstick that these businesses rely on to justify their advertising investments, impacting their competitiveness and growth potential. Ultimately, CPA, whether used as a transaction model or a performance benchmark, guides advertisers in strategically allocating resources to execute efficient and effective advertising campaigns in the fiercely competitive digital landscape.

For Publishers and Media Companies
For publishers, especially within the realm of affiliate marketing, compensation based on Cost Per Acquisition (CPA) represents a prevalent and fundamental practice. The revenue of these publishers often hinges on their capacity to deliver tangible acquisitions for advertisers. However, in the absence of true conversion data, publishers encounter significant challenges when it comes to substantiating the value they contribute to advertising campaigns. Whether they engage in transactions based on CPA or other compensation models, publishers heavily rely on the ability to demonstrate their substantial contributions to advertisers' goals. The dearth of such critical data can instigate disputes and conflicts concerning payment terms, posing a potential threat to the financial stability of publishers. This situation is particularly daunting for small to mid-sized publishers, who may heavily rely on CPA-based compensation, as they face heightened uncertainty and the risk of revenue loss, thereby making it increasingly arduous to sustain their operations effectively.

Billable Metrics - CPC

Temporarily Supported
Currently, there is some uncertainty regarding how Privacy Sandbox handles click counting and whether it aligns with the IAB Click Measurement Guidelines, a crucial aspect for MRC accreditation. It's important to note that Privacy Sandbox's approach to combating Invalid Traffic (IVT) is seen as impractical, and the method for counting clicks remains unclear. As a result, the endorsement of clicks as a billable metric, particularly in the context of Cost Per Click (CPC), is regarded as being in a state of temporary support. This situation raises questions about the compatibility of Privacy Sandbox with established industry standards and practices.

Implications
For Brands and Media Agencies
The practice of charging and remunerating based on clicks, commonly known as Cost-Per-Click (CPC), has remained a billable metric for many advertising campaigns and affiliate programs over the years. However, if the mechanisms for counting and attributing clicks to specific sources like affiliates, exchanges, and publishers aren't fully supported, it could have significant ramifications for businesses. Click data holds immense importance for advertisers as it serves as a key KPI for measuring ad performance and determining the optimal allocation of their budgets.

To bill based on clicks, adherence to industry standards, which includes robust Invalid Traffic (IVT) filtration, is absolutely crucial. The challenge arises from the fact that the inner workings of how Privacy Sandbox measures clicks remain somewhat opaque. This opacity could potentially leave advertisers grappling with an incomplete understanding of their actual click volumes and the return on investment from their advertising expenditures. This, in turn, might lead to less than optimal decisions regarding budget allocation.

Within the realm of affiliate marketing, the intricacies of link decorations associated with click tags take on a heightened significance. These link decorations play a crucial role in accurately attributing clicks to their respective sources,which are vital for affiliate marketers. If the mechanisms supporting link decorations or URLs are truncated or inadequately supported, it can lead to significant challenges in the attribution process. Affiliate marketers heavily depend on these attributes to be compensated for driving leads effectively. Without support for this kind of link decoration, the implications can range from inaccurate counting of clicks to disputes over compensation. It underscores the critical importance of robust mechanisms for preserving some forms of link decoration in the affiliate marketing landscape.

For Publishers and Media Companies
The ability to charge advertisers for clicks represents a fundamental practice for both publishers and affiliate partners. There are companies and individuals that rely on click to not only showcase their value to advertisers at driving quality traffic to their web sites but also to ensure fair compensation. In cases where the mechanisms for passing crucial auction-time information are not fully supported, affiliate partners may confront formidable challenges in proving their pivotal role. In order to bill on clicks, strict adherence to MRC/IAB measurement guidelines for clicks is expected, which includes the vital filtering of Invalid Traffic (IVT). These limitations can have cascading effects, resulting in disputes and conflicts over payment terms that directly impact the financial stability of both publishers and affiliate partners. Small to mid-sized publishers and affiliate partners, who often heavily rely on CPC-based compensation models, find themselves at a heightened risk of revenue uncertainty, making it arduous to sustain their operations effectively. The absence of comprehensive support for click attribution and compliance with industry standards could exacerbate strained relationships and lead to contractual disputes between publishers, advertisers, AdTech systems, and affiliate partners, thereby adding complexity to the operational landscape and the affiliate marketing ecosystem.

Billable Metrics - CPM

Degraded
Currently, there is some uncertainty regarding how Privacy Sandbox handles impression counting and whether it aligns with the MRC Desktop Display Impression Measurement Guidelines, a crucial aspect for MRC accreditation. It's important to note that Privacy Sandbox's approach to combating Invalid Traffic (IVT) is seen as impractical, and the method for counting

impressions remains unclear. As a result, the endorsement of impressions as a billable metric, particularly in the context of Cost Per Thousand (CPM), is regarded as being in a state of temporary support. This situation raises questions about the compatibility of Privacy Sandbox with established industry standards and practices.

Implications

For Brands and Media Agencies

The practice of billing and compensating based on Cost Per Thousand (CPM) impressions has been a staple for countless advertising campaigns over the years. However, if the mechanisms for accurately counting and attributing CPM impressions to specific sources, such as exchanges and publishers, are not comprehensively supported, it could have profound implications for businesses. CPM data plays a pivotal role for advertisers as a critical Key Performance Indicator (KPI) for evaluating ad efficiency and determining how best to allocate their advertising budgets.

To bill based on CPM, strict adherence to industry standards is paramount, including robust filtering mechanisms for addressing Invalid Traffic (IVT). The challenge arises from the lack of transparency regarding how Privacy Sandbox precisely counts impressions, leaving advertisers grappling with incomplete insights into their impression volumes delivered to humans. This lack of clarity may lead to suboptimal decisions regarding budget allocation, potentially affecting advertising campaign performance.

For Publishers and Media Companies

The counting and reporting of impressions, alongside the ability to attribute them to specific sources, are pivotal for revenue generation and equitable compensation, aligning with the expectations set forth by MRC/IAB guidelines. This holds true within the context of programmatic advertising, where CPM is dynamically variable. Publishers heavily rely on this data to showcase their value to advertisers and secure fair payments. When this capability is not fully supported, publishers, including those of smaller and mid-sized stature, encounter significant hurdles in justifying their contributions to the advertising ecosystem. Potential disputes over payment terms can arise, posing financial stability challenges for publishers who often depend on accurate impression data for revenue accrual. Additionally, the absence of a standardized industry approach to noise levels and aggregation methods exacerbates the situation, making it challenging for publishers, particularly smaller ones, to independently validate the accuracy of impression counts. This lack of independent validation, coupled with the absence of accreditation from trusted third parties, creates operational and financial uncertainties within the publishing landscape, in alignment with industry principles.

Attribution Reports

Degraded

Additional costs are imposed on DSPs for less accurate reporting. Real-time campaign optimization based on any kind of behavior or purchase attribution as it is traditionally understood will not be possible.

Implications

For Brands and Media Agencies

The Attribution Reporting API (ARA) revolutionizes digital advertising by enabling the understanding of user interactions and their resulting actions like purchases. However, it introduces far-reaching implications across various domains, including business, legal, financial, and operational aspects. Small to mid-sized enterprises may confront particular hurdles in adapting to these changes. Notably, ARA restricts Demand-Side Platforms (DSPs) from setting impression cookies, impacting access to vital data such as conversion price or value information. This limitation can impede cost-effectiveness assessments, a critical concern for smaller businesses operating on tight budgets. The inclusion of noise in event-level reports, with some amount of records being fake, adds unpredictability, making informed decision-making more challenging. Limited browser support further compounds the situation, affecting campaign reach and effectiveness, which disproportionately impacts smaller enterprises. In parallel, the shift towards summary level reports, while informative, necessitates adjustments in assessing campaign effectiveness and ROI, demanding adaptive analytical approaches. In essence, ARA presents a dual challenge and opportunity, urging businesses, regardless of size, to navigate this evolving landscape to ensure their advertising strategies remain competitive and effective in the dynamic digital advertising arena.

For Publishers and Media Companies

The importance of robust attribution reporting extends beyond advertisers' needs. If advertisers are not confident that where they place their ads are delivering leads or conversions due to limited attribution support, they are likely to shift their investments elsewhere. This shift could result in reduced demand for ad placements, leading to lower ad revenue for publishers and media companies. Furthermore, without the ability to provide detailed attribution insights, publishers may find it challenging to attract advertisers and may lose out on valuable partnerships. Ultimately, the degradation of attribution reporting can hamper the financial success and growth potential of publishers and media companies in the competitive advertising landscape, making it crucial to uphold robust attribution standards for all stakeholders in the industry.

Multi-touch Attribution

Not Supported

Privacy Sandbox is designed to remove all support for cross site and/and device device attribution. Constituents of the programmatic Supply Chain employing multi-touch attribution are encouraged to evaluate the ability to attribute actions like clicks and conversions without cookies (once deprecated) using traditional OpenRTB against the addressability offerings provided by Protected Audience Auctions.

Implications

For Brands and Media Agencies
Limitations within the Attribution Reporting API have widespread implications for advertisers across various aspects of their operations. The lack of support for timeliness requirements, including rapid optimization after ad exposures, can result in missed opportunities for immediate customer engagement, particularly for vital "next-click" actions occurring within seconds. This can have an impact on campaign performance, particularly for smaller to mid-sized advertisers with limited resources, who may encounter heightened challenges in competing effectively in this fast-paced environment, potentially impacting their ability to achieve real-time results and conversions. Secondly, the absence of support for accuracy requirements may lead to suboptimal media budget allocation decisions, risking budget misallocation. This misallocation can harm the return on investment (ROI) and hinder the efficiency of ad campaigns, with smaller businesses facing heightened financial vulnerability due to inaccurate resource allocation. Additionally, the scale requirements present challenges for advertisers of all sizes, as a lack of comprehensive coverage across publishers' properties can impede their reach and campaign effectiveness. Lastly, legal and privacy concerns tied to data accuracy and noise addition algorithms may result in compliance issues and potential legal repercussions, underscoring the need for clear data handling practices and privacy compliance for all advertisers. Therefore, addressing the limitations in attribution flexibility within the API is essential for advertisers to gain a more comprehensive understanding of the value that each publisher brings to the conversion process.

The limitations of Privacy Sandbox's inability to support different attribution models like "first-touch," "linear," or "time-decay," can pose a significant challenge for those advertisers who look beyond the last-click attribution model. This constraint hampers advertisers' ability to effectively assess the contributions of various touchpoints to conversions based on their preferred attribution approach, potentially leading to misconceptions about certain publishers' roles in the conversion process. It restricts advertisers from gaining a nuanced understanding of conversion attribution and impacts their decision-making processes.

For Publishers and Media Companies
The absence of support for key requirements in the Attribution Reporting API can have several implications for publishers. Firstly, it can strain relationships with advertisers due to the lack of timely and accurate reporting, potentially leading to disputes over ad performance and budgets. Smaller publishers, in particular, may struggle to attract advertisers compared to larger platforms with better reporting capabilities.

Publishers may face a competitive disadvantage when competing for advertising partnerships. Smaller publishers, in particular, may find it challenging to compete with larger platforms offering superior reporting capabilities, affecting their ability to secure advertising deals and grow their businesses.

Publishers may need to allocate resources to adapt to evolving industry standards and compliance requirements, with larger publishers having more resources to navigate these

changes while smaller ones may struggle to stay compliant and competitive in the dynamic digital advertising landscape.

Measure Bot Impressions

Not Supported
Sandbox APIs are rife with exploits to generate non-human traffic after a user has been added to an Interest Group. Users are expected to work with their Verification Vendors to identify solutions that provide trust and safety in the digital ecosystem.

Implications
For Brands and Media Agencies
The absence of support for verifying impressions originating from data centers, headless browsers, or bots can have significant business, legal, financial, and operational ramifications. On the business front, advertisers aim to ensure that their ads reach genuine human audiences, and without the ability to discern fraudulent impressions, they risk paying for ad placements that never actually reach an actual human. This challenge is particularly detrimental to small to mid-sized companies, as they often have limited advertising budgets and cannot afford wasteful spending. From a legal perspective, advertisers may find themselves in disputes with publishers over payment for non-human impressions, potentially leading to costly litigation. Financially, the impact is substantial, as budget constraints can hamper their ability to achieve desired outcomes. Operationally, the lack of support means advertisers may struggle to effectively allocate their resources and optimize their campaigns, hindering their overall advertising efforts.

For Publishers and Media Companies
The consequences of not supporting the verification of impressions hold similar weight. In the absence of mechanisms to confirm that impressions are genuine and from actual human users, publishers risk damaging their reputation with advertisers. Small to mid-sized publishers are particularly vulnerable, as they heavily rely on advertiser trust to secure partnerships and revenue. From a legal standpoint, disputes may arise over payments, potentially resulting in financial losses and strained relationships. Additionally, publishers may find it challenging to attract premium advertisers if their platforms are perceived as unreliable in filtering out non-human traffic. Financially, this could lead to revenue declines. Operationally, publishers may struggle to meet the expectations of advertisers who demand transparency and authenticity in their ad placements, impacting their competitiveness in the market. In summary, the implications of not supporting impression verification affect both advertisers and publishers across all scales, with potential business, legal, financial, and operational consequences.

Multiple Attribution Reports Recipients

Degraded
Even though multiple participants may receive reporting, they must be manually added to the report event and it is unclear what the upper limit of report recipients will be.

See Publisher Revenue Accrual and Validation and Billable Metrics - CPM for additional details.

Implications

For Brands and Media Agencies

Advertisers are required to manually register multiple recipients to receive reports for the same impression, which can lead to a more granular understanding of the attribution process. This means that advertisers can track attribution events from various sources and triggers, enabling them to optimize their ad campaigns based on comprehensive data. From a legal perspective, it's essential for advertisers to ensure compliance with privacy regulations and user consent when collecting and sharing attribution data with multiple recipients. From a financial standpoint, the increased granularity of reports may lead to more efficient budget allocation and better return on investment (ROI). However, for small to mid-sized companies, implementing and managing this level of attribution tracking may require additional resources and expertise, potentially posing operational challenges.

For Publishers and Media Companies

Publishers register multiple recipients to receive reports for the same impression, enhancing their ability to collaborate with advertisers and provide detailed insights. This can lead to stronger partnerships with advertisers and potentially higher revenue opportunities. However, publishers must carefully manage and protect user data to comply with legal requirements and privacy regulations. From a financial perspective, offering advanced attribution reporting capabilities can be a selling point for publishers, attracting more advertisers and potentially increasing revenue. For smaller to mid-sized publishers, implementing and maintaining these reporting features may require investment in technology and staff training, which could be a significant operational consideration.

Reporting Impressions by Host Domain

Temporarily Supported

Advertisers will be able to report on websites where their ads ran at the host domain level (e.g. www.website.com). It should be noted that there is a process to set up this reporting correctly and implementers are strongly encouraged to test prior to any campaign being launched.

Implications

For Brands and Media Agencies

This allows advertisers to gain insights into the specific websites or domains where their ads are being served. This information is invaluable for assessing the performance of ad placements and optimizing ad campaigns. For larger advertising firms, this data may streamline their decision-making processes and provide a competitive edge. However, for small to mid-sized companies, it offers an understanding of where their ad budget is being spent, which can help them make more informed budget allocation decisions, ensuring efficient spending. Legally, this

kind of reporting can be crucial in cases of ad placement disputes or compliance with industry regulations, ensuring that ads are not displayed on inappropriate or unauthorized domains.

For Publishers and Media Companies
Operationally, it requires the implementation of reporting infrastructure that can accurately capture and relay domain-level data to advertisers. This can be resource-intensive, especially for smaller publishers with limited technical capabilities or financial resources. From a business perspective, domain-level reporting can be a selling point for publishers, especially those with high-quality and brand-safe domains. It can attract premium advertisers willing to pay more for ad placements on specific domains, potentially boosting revenue. However, for smaller publishers, this could mean more competition and a need for higher standards in content quality to attract advertisers. Legally, publishers need to ensure they have the rights and permissions to share domain-level data with advertisers while complying with privacy regulations to protect user information.

Reporting by URL

Not Supported
Evaluation or optimization of inventory at any level lower than the host URL will not be possible. For example, reporting will work for www.website.com but not for www.website.com/example. There are other non-normative mechanisms that may functionally accomplish this goal, all of which require operational lift and additional testing.

Implications
For Brands and Media Agencies
From a business perspective, not knowing the full page URL where their ads are served can limit advertisers' ability to assess the context in which their ads appear. This lack of transparency may lead to brand safety concerns, as advertisers may unknowingly have their ads displayed on pages with brand-unsuitable content. This issue is particularly challenging for small to mid-sized companies that may lack the resources to invest in extensive brand safety measures, potentially resulting in reputational damage and decreased consumer trust. Legally, failing to provide URL reporting could expose advertisers to compliance issues, especially in regions with strict regulations governing ad placement. Financially, it can result in wasted ad spend and reduced ROI, as advertisers cannot optimize their campaigns effectively without this crucial information. Operationally, the inability to access URL data hampers advertisers' ability to make informed decisions and impacts their overall advertising strategy. Advertisers typically lean towards having the URL passed through the browser rather than relying on a publisher's macro. This practice provides a higher level of transparency and instills greater trust in the ad placement process.

For Publishers and Media Companies
The lack of support for reporting by URL can also have significant repercussions across various aspects of their business. From a business perspective, not being able to provide advertisers

with full page URL data may deter potential advertisers who prioritize transparency and brand safety. This can particularly affect smaller to mid-sized publishers, as they may face increased competition in securing ad partnerships. Legally, publishers could face contractual disputes if they cannot deliver on promises of transparency and data sharing, which may lead to legal ramifications. Financially, the absence of URL reporting can hinder publishers' ability to negotiate higher CPMs with advertisers who demand such data, impacting revenue potential. Operationally, it could require publishers to implement additional systems and processes to meet advertisers' demands for transparency, potentially straining their resources.

Report on Information Gleaned from Macros

Not Supported

Implementors leveraging information obtained through the use of macros should evaluate other methods of optimization for decisioning, optimization and reporting in Protected Audience. It should be noted that they will continue to have full support in traditional OpenRTB auctions, they just won’t be able to use cookies (once deprecated) to address their audience.

Implications

For Brands and Media Agencies

This report allows advertisers to assess the effectiveness of their ad campaigns, optimize their targeting strategies, and allocate budgets more efficiently. It provides crucial insights into which key value pairs are driving results and helps in making informed decisions. On a legal front, not supporting this feature could lead to potential disputes between advertisers and publishers regarding the accuracy of billed impressions and the delivery of promised results. Financially, without this support, advertisers, especially small to mid-sized companies, may face increased ad spend wastage as they won't have the granular data needed to fine-tune their campaigns, impacting their ROI. Operationally, lacking the ability to generate reports with Macros can result in a less streamlined process, affecting the overall competitiveness of smaller players in the industry.

For Publishers and Media Companies

The absence of support for generating reports with Macros limits their ability to provide detailed insights to advertisers about the performance of their ad inventory. This could lead to a loss of trust and potential revenue as advertisers may seek other platforms that offer more transparent reporting. From a legal standpoint, not supporting this feature may expose publishers to contractual disputes with advertisers who expected accurate and detailed reporting. Financially, smaller to mid-sized publishers may be particularly affected as they heavily rely on advertiser trust and may lose valuable ad revenue. Operationally, without this support, publishers may find it challenging to differentiate themselves in a competitive market, potentially leading to a loss of market share. It's crucial for both advertisers and publishers that the industry addresses this issue to ensure a fair and thriving advertising ecosystem.

Reporting by Creative URL

Not Supported
Publishers will need to spend significantly more FTE time in ad operations evaluating creative assets. Risk averse publishers will need to move from exclusion to inclusion lists of approved advertisers and manually review each creative in addition to holding a mapping table outside of the bidstream of approved creative ids to be used in their scoreAd function.

Implications
For Brands and Media Agencies
The absence of support for reporting by Creative URL has significant implications for troubleshooting, identifying problematic creatives, and aiding in identifying discrepancies. This includes challenges like pinpointing redirects and determining which ads are in rotation, especially in programmatic advertising, where multiple creatives may be bundled within a single creative tag. Advertisers face difficulties diagnosing and resolving issues without detailed creative information, increasing operational complexity and risking wasted ad spend. Smaller to mid-sized companies, focused on cost-efficiency, are particularly vulnerable to these challenges due to resource constraints.

For Publishers and Media Companies
The absence of support for reporting by Creative URL poses legal, financial, and operational risks. Identifying problematic creatives, whether due to redirects, rotation issues, or reconciliation discrepancies, and addressing them becomes a more arduous task, requiring additional resources and tools. Overall, the absence of Creative URL reporting not only hampers troubleshooting efforts but also presents substantial challenges for smaller to mid-sized companies, affecting their budget-conscious decisions, revenue streams, and operational efficiency within the dynamic landscape of digital advertising.

Measure Multiple Conversions from Multiple Ads

Degraded
Under-reporting is expected, particularly for destination sites that have multiple brands such as Financial Services (Credit card major advertising for different brands of credit card), Retail with different in-house brands and Travel sites advertising for 100’s of hotel and airline brands.

Implications
For Brands and Media Agencies
This issue primarily affects advertisers who promote multiple brands that may convert on the same domain. When customers convert for multiple brands on the same destination site, the Chrome ARA algorithm under-reports conversions. This under-reporting can lead to inaccurate attribution and a loss of valuable insights. It may result in suboptimal allocation of resources and missed opportunities for growth, ultimately affecting their competitiveness in the market. The degradation to algorithms can lead to the possibility of credit being applied to the wrong brand

and/or campaign. Without the ability to measure attribution across these campaigns, credit for a conversion may be erroneously assigned, skewing the algorithms used to optimize. This can result in misallocation of budgets, leading to suboptimal performance and missed opportunities.

For Publishers and Media Companies
When advertisers face challenges in measuring attribution for multiple conversions from multiple ads, publishers may experience reduced demand for their ad inventory. This can impact their revenue and overall business performance. Publishers may struggle to maintain profitability and competitiveness when dealing with these issues, if advertisers lack the ability to attribute multiple conversions across multiple ads. The issue extends beyond general attribution challenges; conversions for specific campaigns and/or creatives may be skewed and/or under/over-reported. This can result in a disconnect between the perceived performance of individual campaigns and/or creatives and their contribution to conversions and revenues. For publishers, such discrepancies can have financial repercussions, as they may find it challenging to bid accurately and/or attract advertisers.

This underscores the critical need for a robust attribution system that ensures fair and transparent reporting for all parties involved.

Technology and Interoperability

Managing Infrastructure Costs

Not Supported
Corporations have spent billions of dollars to stand up and maintain current ad tech infrastructure. Companies wanting to employ Privacy Sandbox will need to ensure that they can provide advertising services with a similar cost and scaling models to existing auctions by leveraging existing infrastructure and processing the new demands of PAAPI with a minimum of new compute and network load on the system.

Implications
For Brands and Media Agencies
Failing to optimize infrastructure costs can lead to a significant increase in operational expenses, negatively affecting profitability. This is especially critical for small to mid-sized companies that may have limited resources to absorb such cost increases. The lack of transparency regarding new services and infrastructure required to support Privacy Sandbox specifications can result in uncertainty and potential legal disputes with publishers and/or their ad tech or measurement partners. The exclusive reliance on Google or Amazon for Trusted Execution Environments (TEE) can lead to legal challenges related to market dominance and antitrust concerns, particularly impacting small players in the industry. The inefficient infrastructure to manage can lead to increased operational costs and resource issues, which

may not be sustainable for smaller businesses. Failure to address the scalability and cost issues associated with infrastructure can hinder the ability of advertisers and agencies alike, to adapt to the evolving demands of the ad tech ecosystem, potentially leading to a loss of competitiveness in the market and increased financial burden.

For Publishers and Media Companies
Inadequate scaling of resources and inefficient infrastructure management can lead to increased overhead costs. Legally, the lack of clarity regarding the cost forecasts for adopting and supporting new infrastructure and services can result in disputes and contractual challenges, especially for smaller publishers with limited legal resources. The requirement to use specific TEEs controlled by Google or Amazon can create financial dependencies for them, reducing negotiating power for smaller companies and potentially leading to less commercially favorable terms. The massive duplication of data due to the TEE requirement can strain the operational capabilities of companies, causing inefficiencies and affecting the quality of their services.

Privileged Signals

Not Supported
Commercially sensitive information, such as CPMs will be openly accessible to all parties. Businesses will need to weigh the ability to keep business information private in traditional OpenRTB in cookieless environments (once deprecated) against the addressability functionality provided by Privacy Sandbox APIs.

Implications
For Brands and Media Agencies
The traditionally confidential pricing rules, such as commercially sensitive rates bidded on or purchase price, are now openly accessible to competitors and partners alike. This shift not only comprises the confidentiality of these rates but also levels the playing field, making it harder for advertisers and agencies to maintain a competitive edge in pricing strategies. As rates become transparent, advertisers may find it challenging to negotiate favorable terms, potentially leading to higher costs for ad placements, especially as they pertain to preferred deals, private marketplace deals and automated guaranteed deals. It can lose their efficacy as they are applied within the browser, rendering them less effective in safeguarding brand safety and suitability. These changes lead to legal considerations, potentially necessitating renegotiation of contracts and agreements.

For Publishers and Media Companies
The open accessibility of what is considered confidential pricing rules, such as commercially sensitive rates, poses challenges for the sell-side. While it introduces transparency, it can also have unintended consequences, potentially leading to lower rates paid by advertisers, as they

gain more insight into the pricing strategies of their competitors. Publishers may find themselves under pressure to justify their pricing structures in more transparent environments.

The hierarchical top-level auctions and component auction system introduced by PAAPI can compromise the protection of data that was previously secure in server-side auctions. As they now navigate potential data security concerns, they may face particular challenges in maintaining data integrity and confidentiality when dealing with partners who may not have the same level of security infrastructure. Publishers may need to reevaluate their operational practices and invest in additional security measures to protect their data.

Data Guarantees

Not Supported
Without clear contractual frameworks that include provisions for such things as limitation of liability, representations and warranties, force majeure events, etc., disputes can escalate into protracted legal battles, financial burdens, and strained business relationships.

Implications
The absence of contractual and commercial mechanism within the Privacy Sandbox and its APIs give rise to a perplexing legal landscape, including issues related to limitation of liability, representations and warranties, force majeure, make goods or compensation, indemnification, non-disclosure, data usage, data ownership and compliance with laws. All parties - advertisers, publishers, ad agencies, ad tech, data providers, measurement companies, and more - have agreements in place with each of their partners, ensuring there are clear responsibilities and obligations, as well as accountability for any issues that may arise. However, without these mechanisms directly with Chrome and its Privacy Sandbox APIs, issues such as glitches, reporting discrepancies, delayed services/reporting, and other operational challenges can create a state of uncertainty regarding who bears the liability between parties, including with Chrome

Algorithm Integrity Guarantee

Not Supported
Companies across the ecosystem face financial risks, as they invest resources without assurance of fair and unbiased algorithmic decision-making. The absence of an Algorithm Integrity Guarantee affects all across various aspects of their operations, and can hinder a company's ability to compete effectively.

Implications
Typically when services are provided by any counterparty, contractual obligations govern data usage and processing, providing a sense of security. However, within the Privacy Sandbox framework, the lack of guarantee that algorithms, such as PAAPI, adhere faithfully to public

specifications and material instructions raises concerns. Many companies lack the resources to independently verify algorithmic compliance, and this can jeopardize campaign effectiveness and trigger legal issues related to data privacy.

The potential economic repercussions cannot be overlooked if for any reason, these algorithms error in a way that negatively impacts a company's ability to generate revenue. The question of liability becomes paramount. The intricacies of determining responsibility in such cases can be complex, potentially involving multiple parties, including Chrome, the platforms using them, and even regulatory bodies. The need for comprehensive safeguards and transparency within the digital advertising ecosystem becomes not only a matter of business ethics but also a crucial component of global economic stability.

References

Fenced Frames - https://web.archive.org/web/20231023112116/https://wicg.github.io/fenced-frame/#fencedframeconfig

Protected Audience API (PAAPI) - https://web.archive.org/web/20231121101019/https://wicg.github.io/turtledove

FLEDGE - https://github.com/WICG/turtledove/blob/820763e161fb3accdf69b728be502551472ff538/FLEDGE.md

Attribution Reporting Specification (ARA) [17th November 2023] - https://web.archive.org/web/20231117171857/https://wicg.github.io/attribution-reporting-api/

Private State Token API Specification (PST) [21th November 2023] - https://web.archive.org/web/20231121152412/https://wicg.github.io/trust-token-api/

