



Privacy  
Sandbox

# Privacy Sandbox resources

Dec 2024



# Introduction

# Privacy Sandbox **relevance** & **measurement\*** APIs support the needs of businesses while providing privacy safeguards



## Topics API

Enables interest-based advertising informed by the sites a user recently visited, without sharing specific browsing history across the web



## Protected Audience API

Supports remarketing by enabling site owners to create custom audiences, without exposing personal information



## Attribution Reporting API

Facilitates measurement by matching ad views and clicks with conversions, without identifying people at an individual level

# Privacy Sandbox **relevance** & **measurement\*** APIs support the needs of businesses while providing privacy safeguards



## Topics API

Enables interest-based advertising informed by the sites a user recently visited, without sharing specific browsing history across the web

**Use Case:** Prospecting

Enable relevant, on-device audience selection across ad tech providers, resulting in better match rates and improving reach and performance (DSP) or and increasing demand and yield (SSP)



## Protected Audience API

Supports remarketing by enabling site owners to create custom audiences, without exposing personal information

**Use Case:** Custom audience creation



## Attribution Reporting API

Facilitates measurement by matching ad views and clicks with conversions, without identifying people at an individual level

**Use Case:** Campaign measurement

Ensure the outcomes you drive are measured effectively

# Privacy Sandbox APIs support the needs of businesses while providing privacy safeguards



## Cookies Having Independent Partitioned State (CHIPS)

Enables third-parties to maintain embedded site functionality on sites by allowing access only to specific, compartmentalized information in a way that prevents tracking

**Example:** A chat bot provider might use this to ensure user chats are remembered between page reloads



## Related Website Sets

Allows limited data sharing within small groups of affiliated sites that declare and meet specific criteria, preventing tracking and data leakage

**Example:** A company might use this if they have domains for different countries (example.com, example.co.uk, example.rs)



## Federated Credentials Management (FedCM)

Makes “Sign in with...” login solutions more private by shielding people's information to prevent passive tracking

**Example:** An identity provider might use this to enable people to connect the same identity across different services

# Private Sandbox APIs support the needs of businesses while providing privacy safeguards



## Storage Access API (SAA)

Enables third-parties to share information across sites only when user interaction and permission requirements are met, preventing unwanted tracking



## Private State Tokens (PST)

Protects sites from bots and fraudulent traffic by using the browser to convey user trust signals, without revealing that person's information



# How They Work

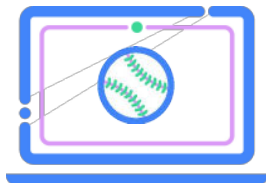
# Topics API

Reach relevant audiences powered by anonymized insights

1

## Topics assignment

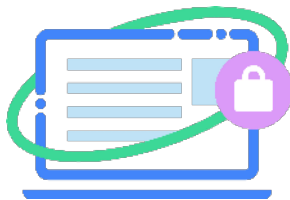
When someone browses the internet, the sites they visit are used to infer their generalized interest topics, such as **sports**.



2

## Data management & protection

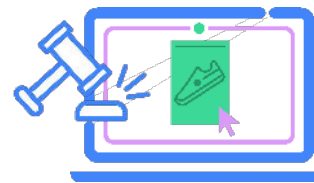
These Topics are refreshed regularly and made available to API callers, without ever surfacing specific browsing information.



3

## Bidding on private signals

Marketers can then bid on the chance to serve ads to audiences with a particular topic, without identifying a specific person.





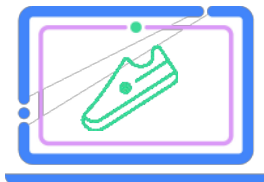
# Protected Audience API

Re-engage relevant audiences powered by anonymized insights

1

## Interest group assignment

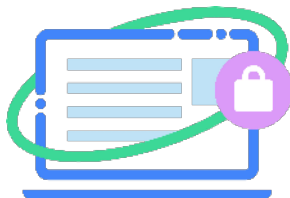
Site owners can assign visitors to pre-defined, anonymized interest groups based on on-site behavior, such as "in-market for shoes".



2

## Data protection and management

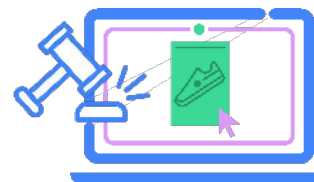
The browser then stores the assigned interest group so that site owners can utilize it for use cases such as remarketing.



3

## Bidding on private signals

Marketers can then bid on the chance to reach a particular interest group, but not an identifiable person.



# Attribution Reporting API

Enable effective ad measurement with privacy-preserving technologies

1

## Recording ad interactions

When someone views or clicks an ad where Attribution Reporting API is in place, the API caller records their interactions in the browser.



2

## Recording on-site conversions

If they later visit that advertiser's site and perform an action that is recognized as a conversion, this is also recorded by the API caller.



3

## Report generation

Before campaign data reaches the advertiser, privacy preserving techniques like noise, aggregation, and encryption are used to protect individual identity.



# Cookies Having Independent Partitioned State (CHIPS) API:

## Facilitate seamless site experiences while safeguarding privacy

1

Someone visits a site with a feature that is enabled by a third-party service, like a weather widget.



2

The CHIPS API allows the third-party widget to set and read its own cookies, but only when it's embedded on this particular first-party site, so it can remember user details, like the location they've entered.



3

The person's information is kept compartmentalized and separate from any other sites, ensuring that the cookies cannot be used for cross-site sharing.



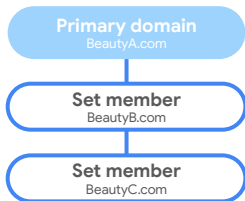
# Using Related Website Sets (RWS) with Storage Access API (SAA)

## Facilitate seamless experiences across sites while safeguarding privacy

1

### RWS creation

A beauty company with multiple sites adds its domains to a Related Website Set.

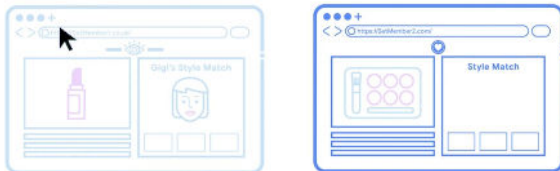


2

### Cross-site navigation

A person visits a site in that set, BeautyA.com, and searches for makeup.

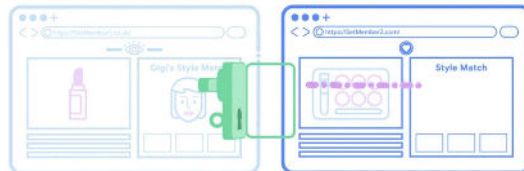
Later, that person visits another site, BeautyB.com, also from that set.



3

### Site experience optimization

BeautyB.com relies on cookies from BeautyA.com to manage things like log-in and customized product recommendations. When the site loads, BeautyA.com uses SAA to request access to its cookies. Since the sites are in the same RWS, access is automatically granted.



# Federated Credential Management

## Facilitate seamless sign-in while safeguarding privacy

1

If a site requires login, the visitor can either set up an account with that specific site or log in using existing credentials with a third-party Identity Provider, like Google, Facebook, or others.



2

With FedCM in place, Identity Providers offered as login options no longer automatically receive information about the site that person is visiting, which helps prevent profiling.

Once the person has chosen to log in, the site and the identity provider can share information to enable a seamless sign in experience.

