

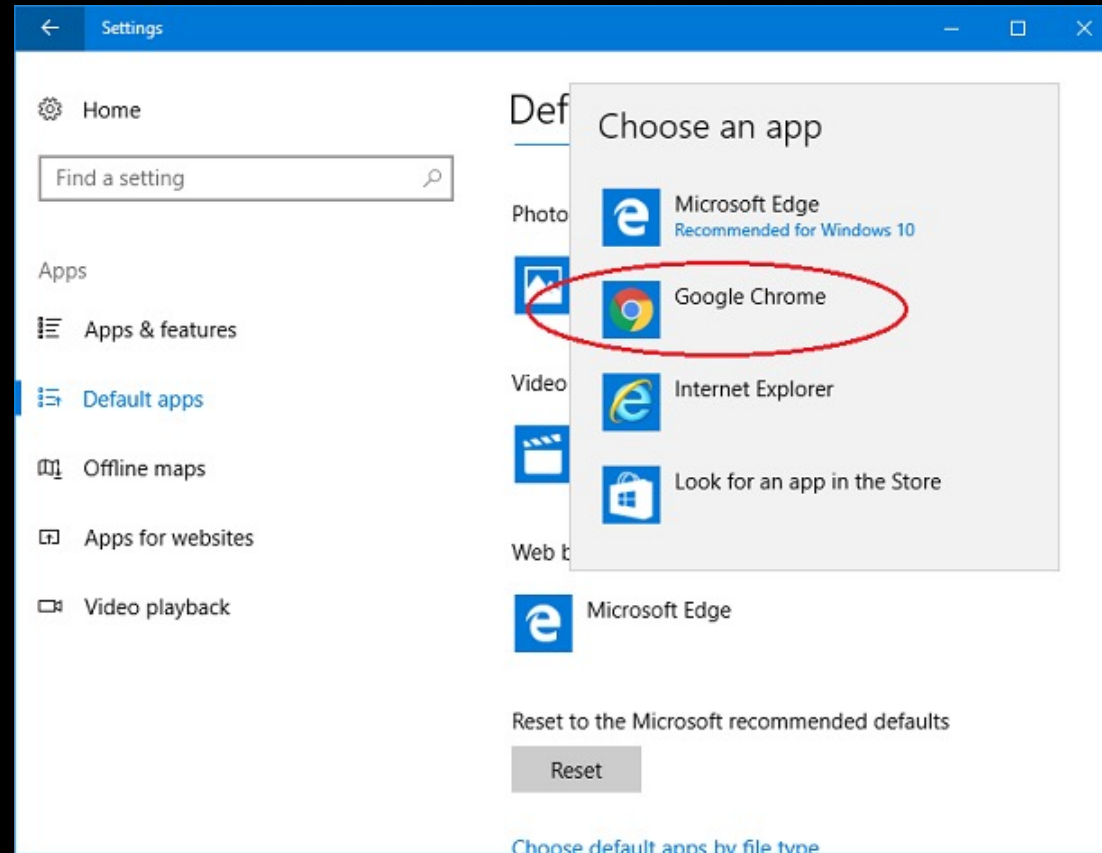
How Privacy Sandbox broke the web, but promised to fix it

Denis Rybin, Head of AppSec Mail.ru



Disclaimer #1

We are talking about Chrome by default



What does the average pentester know about browsers?

Junior:

- Basic XSS
- CSRF
- Cookie
HTTPOnly/Secure
- SOP (really good
Junior)

What does the average pentester know about browsers?

Junior:

- Basic XSS
- CSRF
- Cookie
HTTPOnly/Secure
- SOP (really good Junior)

Middle:

- Tricky XSS
- CORS/preflight
- CSP
- More APIs
 - PostMessage
 - LocalStorage
 - WebCache
 - etc

What does the average pentester know about browsers?

Junior:

- Basic XSS
- CSRF
- Cookie
 HTTPOnly/Secure
- SOP (really good Junior)

Middle:

- Tricky XSS
- CORS/preflight
- CSP
- More APIs
 - PostMessage
 - LocalStorage
 - WebCache
 - etc

Senior:

- Tricky CSP
- Cookie __Host-
- Site != origin
- Latest exotic stuff
 - CORB
 - COOP
 - CORP
 - COEP
 - etc

What does the average pentester know about browsers?

Junior:

- Basic XSS
- CSRF
- Cookie
 HTTPOnly/Secure
- SOP (really good Junior)

Middle:

- Tricky XSS
- CORS/preflight
- CSP
- More APIs
 - PostMessage
 - LocalStorage
 - WebCache
 - etc

Senior:

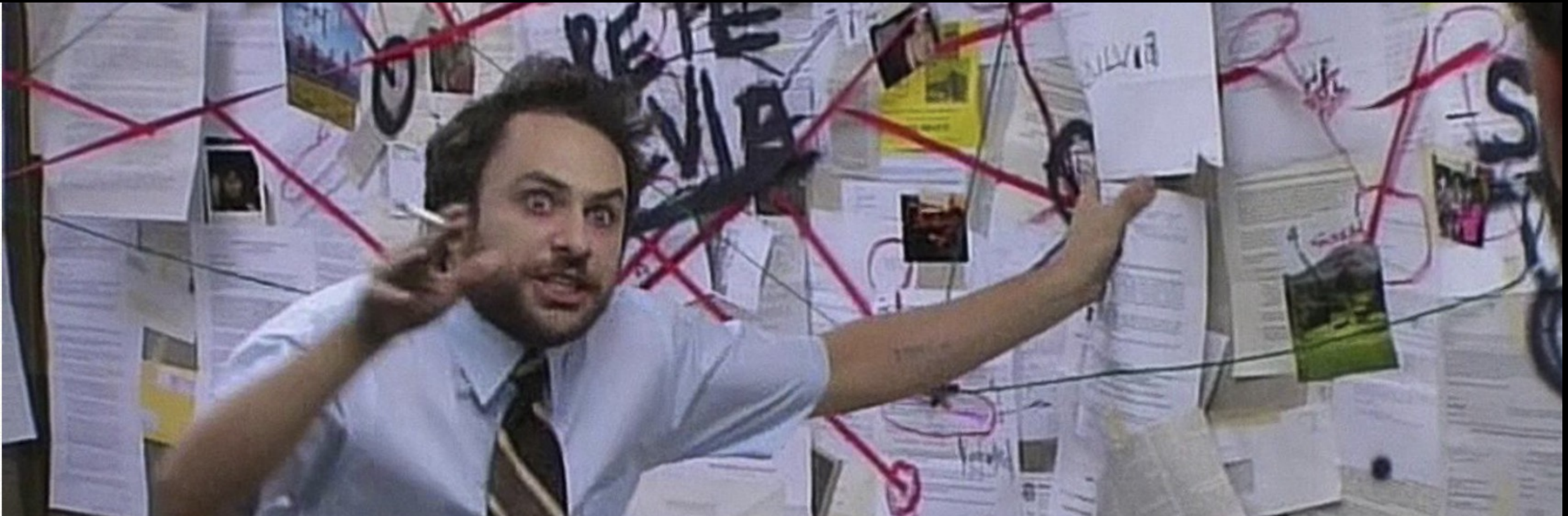
- Tricky CSP
- Cookie __Host-
- Site != origin
- Latest exotic stuff
 - CORB
 - COOP
 - CORP
 - COEP
 - etc

Secret level (Principal):

- Proposals
- Origin Trials
- Thinks about problems, not technology
- Knows how new ideas change the whole context

Disclaimer #2

I'll look like this for the next 30 minutes



Privacy Sandbox

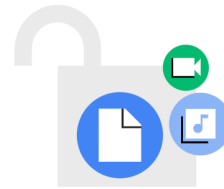
The goals of the Privacy Sandbox

The Privacy Sandbox is currently in development. It aims to:



Build new technology to keep your information private

People should be able to enjoy their browsing and app experience without worrying about what personal information is collected, and by whom. The Privacy Sandbox technologies aim to make current tracking mechanisms obsolete, and block covert tracking techniques, like [fingerprinting](#).



Enable publishers and developers to keep online content free

Billions of people around the world rely on access to information on sites and apps. To provide this free resource without relying on intrusive tracking, publishers and developers need privacy-preserving alternatives for their key business needs, including serving relevant content and ads.



Collaborate with the industry to build new internet privacy standards

The internet is a source of information and engine of economic growth worldwide. Google invites members of the industry – including publishers, developers, advertisers, and more – to get involved and contribute to the development of better privacy standards for the Web and on Android.

The goals of the Privacy Sandbox

The Privacy Sandbox is currently in development. It aims to:

The Privacy Sandbox is currently in development. It aims to:

private

People should be able to enjoy their browsing and app experience without worrying about what personal information is collected, and by whom. The Privacy Sandbox technologies aim to make current tracking mechanisms obsolete, and block covert tracking techniques, like [fingerprinting](#).

online content free

Billions of people around the world rely on access to information on sites and apps. To provide this free resource without relying on intrusive tracking, publishers and developers need privacy-preserving alternatives for their key business needs, including serving relevant content and ads.

internet privacy standards

The internet is a source of information and engine of economic growth worldwide. Google invites members of the industry – including publishers, developers, advertisers, and more – to get involved and contribute to the development of better privacy standards for the Web and on Android.

Privacy Sandbox on Android (Easy part)



Proposed Solutions

Android will introduce new platform features that support mobile advertising while enhancing user privacy. You can review the current proposals for each of these features and provide feedback to help improve them.

DESIGN PROPOSAL

SDK Runtime

A safer way for apps to integrate with third-party advertising SDKs

DESIGN PROPOSAL

Topics

Enable interest-based ads personalization without relying on user-level identifiers

DESIGN PROPOSAL

FLEDGE on Android

A new way to serve customized ads to users based on previous app engagement, without third-party data sharing

DESIGN PROPOSAL

Attribution Reporting

Measure ads performance and optimize based on this data, while limiting user-level information sharing

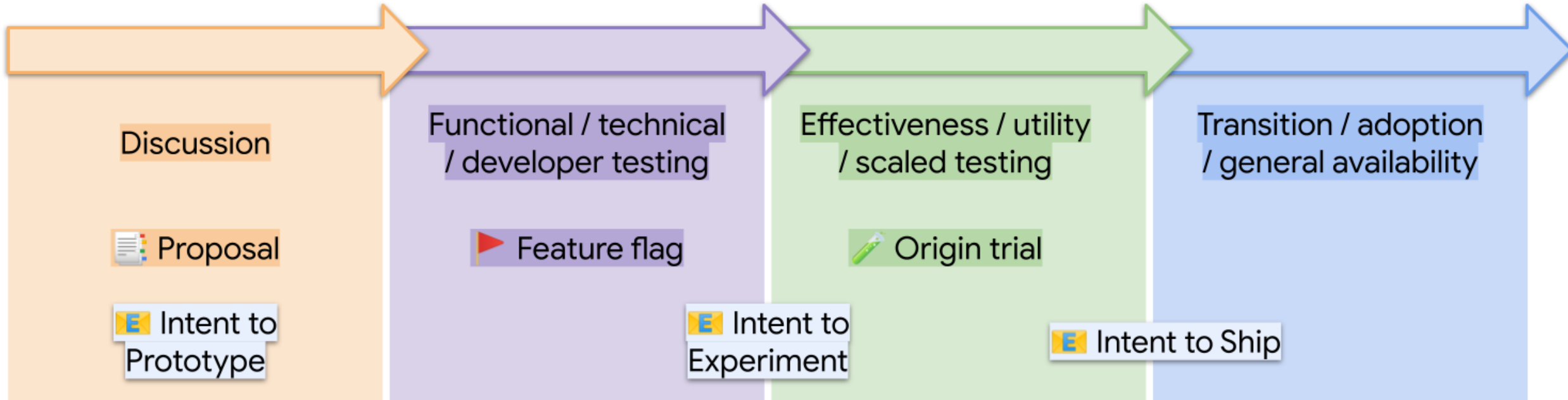
Privacy Sandbox for the Web

Privacy Sandbox for the Web will phase out [third-party cookies](#) by using the latest privacy techniques, like [differential privacy](#), [k-anonymity](#), and [on-device processing](#).

Privacy Sandbox also helps to limit other forms of tracking, like [fingerprinting](#), by restricting the amount of information sites can access so that your information stays private, safe, and secure.



Lifecycle Overview



Proposal

Ideas and Proposals (links outside this repo)

- [Private fraud prevention](#)
- [Conversion measurement API](#)
- [Ad click attribution](#)
- [Trust token API](#)
- [Tracking prevention policy](#)
- [Privacy budget](#)
- [First party sets](#)
- [Privacy considerations](#)
- [Aggregate reporting API](#)
- [IP Blindness](#)
- [FLoC: Federated Learning of Cohorts](#)
- [PIGIN: Private Interest Groups, Including Noise](#) (deprecated in favor of TURTLEDOVE)
- [TURTLEDOVE](#)
- [Product-level TURTLEDOVE](#) (extension feasible for TURTLEDOVE & SPARROW)
- [Outcome-based TURTLEDOVE](#) (extension introducing in Turtledove outcome-based approach - monitor and validate bidding outcomes, not inputs)
- [TURTLEDOVE-js demo](#) (demo implementation of TURTLEDOVE - based on available technologies)
- [isLoggedIn](#)
- [SPARROW](#)
- [Gatekeeper](#)
- [Proprietary Cohorts](#)
- [Fenced Frame](#)
- [TERN](#) (TURTLEDOVE Enhancements with Reduced Networking)
- [PARRROT](#) (PARRROT: The Publisher Auction Responsibility Retention Revision of TurtleDove)
- [PELICAN](#) (Private Learning and Inference for Causal Attribution)
- [PUFFIN](#) (Personal User Floors For Impression Negotiations)
- [SPURFOWL](#) (Sandboxed Private User Reporting Functions Operating Within Limits) and other [NextRoll proposals](#) including MURRE.
- [TEETAR](#)(TEETAR: Testing Environment Enabling Truthful and Actionable Results)



Feature flag

Experiments

104.0.5112.79

WARNING: EXPERIMENTAL FEATURES AHEAD! By enabling these features, you could lose browser data or compromise your security or privacy. Enabled features apply to all users of this browser. If you are an enterprise admin you should not be using these flags in production.

Interested in cool new Chrome features? Try our [beta channel](#).

Available	Unavailable
-----------	-------------

Temporarily unexpire M102 flags.

Temporarily unexpire flags that expired as of M102. These flags will be removed soon. – Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros

[#temporary-unexpire-flags-m102](#)

Default

Temporarily unexpire M103 flags.

Temporarily unexpire flags that expired as of M103. These flags will be removed soon. – Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros

[#temporary-unexpire-flags-m103](#)

Default

Override software rendering list

Overrides the built-in software rendering list and enables GPU-acceleration on unsupported system configurations. – Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros

[#ignore-gpu-blocklist](#)

Disabled

Accelerated 2D canvas

Enables the use of the GPU to perform 2d canvas rendering instead of using software rendering. – Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros

[#disable-accelerated-2d-canvas](#)

Enabled

Select HW overlay strategies

Select strategies used to promote quads to HW overlays. – Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros

[#overlay-strategies](#)

Default


Tint composited content


Tint contents composited using Viz with a shade of red to help debug and study overlay support. – Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros

Disabled



Origin Trials


Chrome Origin Trials


Sign in

Origin trials allow developers to try out new features and give feedback. [Learn more.](#)

Active Trials


My Registrations


Completed Trials

AnonymousIframe	Anonymous iframes give developers a way to load documents in third pa...	
Conditional Focus	An API that allows the Web-applications to control whether, when tab-cap...	REGISTER
Cookies Having Independent Partitioned State (CHIPS)	Given that Chrome plans on obsoleting third-party cookies, we want to gi...	REGISTER
Federated Credentials Management API (FedCM for short)	A Web Platform API that allows users to login to websites with their feder...	REGISTER
getCurrentBrowsingContextMedia	Allow capturing the current tab (subject to the user's confirmation). Distin...	REGISTER
Launch Handler	A web app manifest field to control how your app is launched, e.g. wheth...	REGISTER
MSE in Dedicated Workers	Enable Media Source Extensions usage from DedicatedWorker contexts f...	REGISTER
Privacy Sandbox Relevance and Measurement	The shared origin trial includes the following APIs to facilitate advertising...	REGISTER
Private Network Access from non-secure contexts	Allows non-secure contexts to make requests to the private network, in s...	REGISTER
Region Capture	Crop MediaStreamTracks produced by a call to getDisplayMedia.	REGISTER
Secure Payment Confirmation - Opt-Out Support	Adds an 'opt-out' flow to Secure Payment Confirmation. When the (option...	REGISTER
Shared Element Transitions for SPAs	A new API that allows a simple set of transitions in Single-Page Applicati...	REGISTER

NO
FF
ONE
2022

Origin Trials

 Chrome Origin Trials

 Sign in

Origin trials allow developers to try out new features and give feedback. [Learn more.](#)

Active Trials

My Registrations


Completed Trials

NO
FF
ONE
2022

Origin trials



Анонимный опрос

12% Я знаю что это такое



88% Я не знал что это такое до того как загрузил

83 голоса

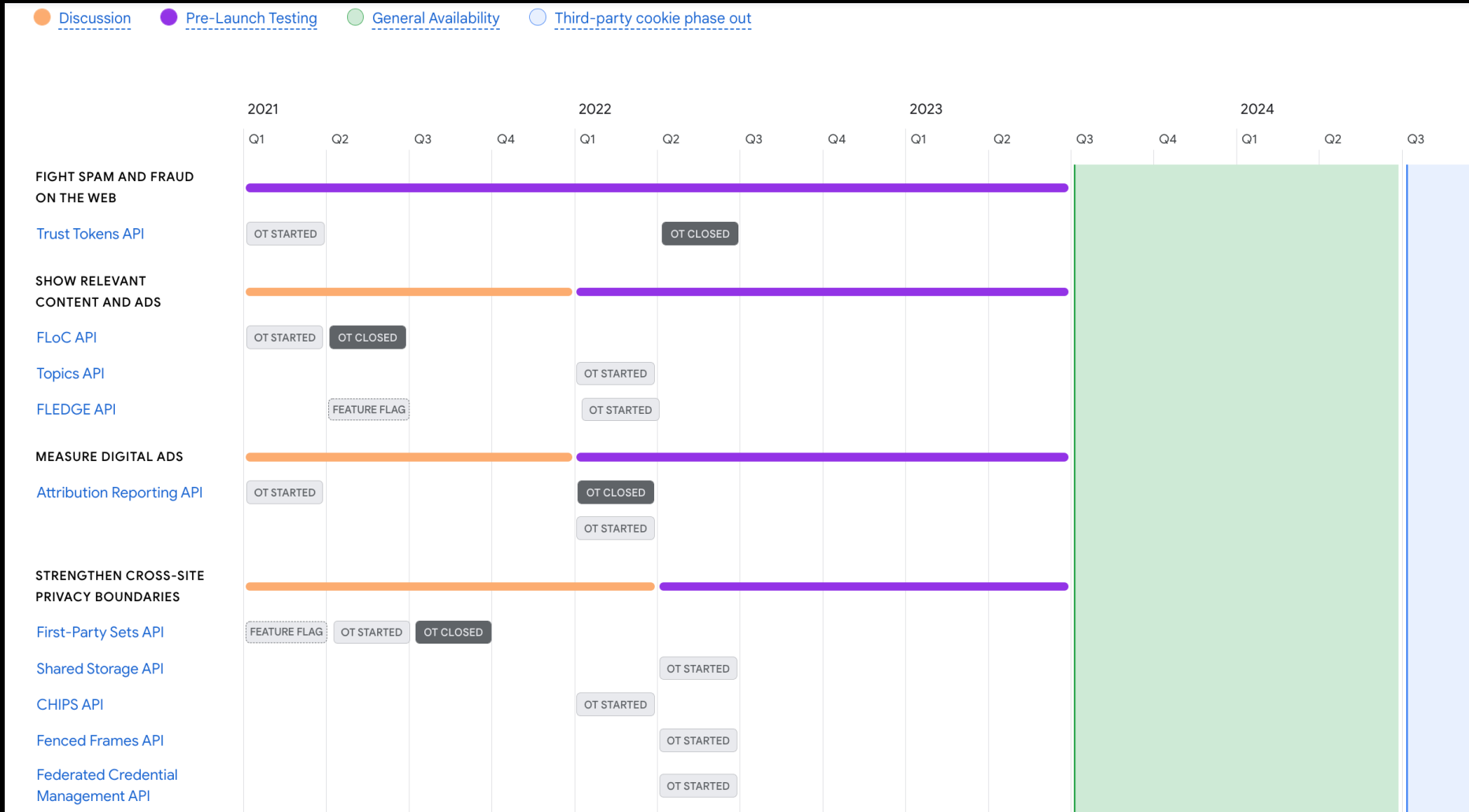
 4 18:37 

General Availability

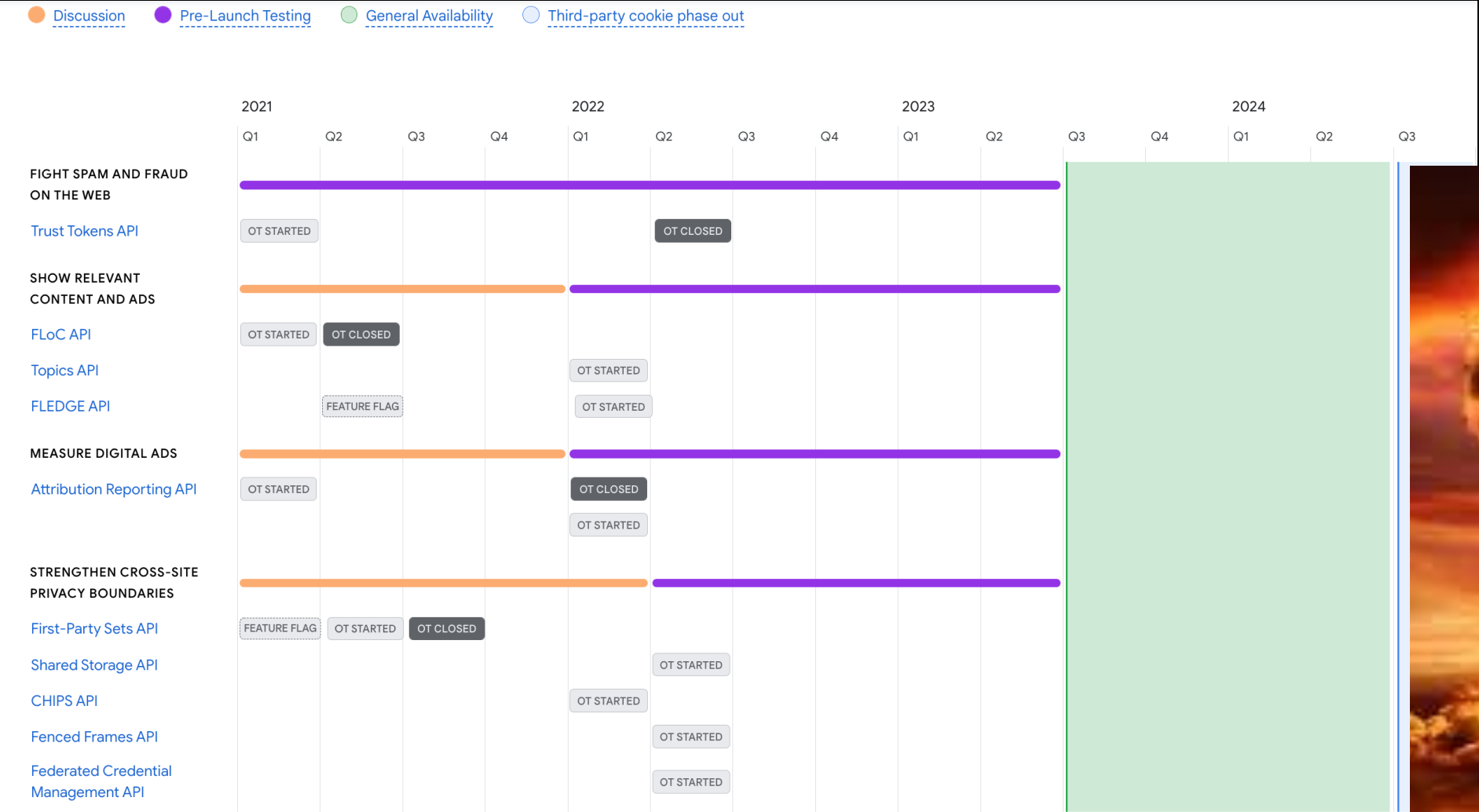
NO
FF
ONE
2022



Privacy Sandbox for the Web. Timeline

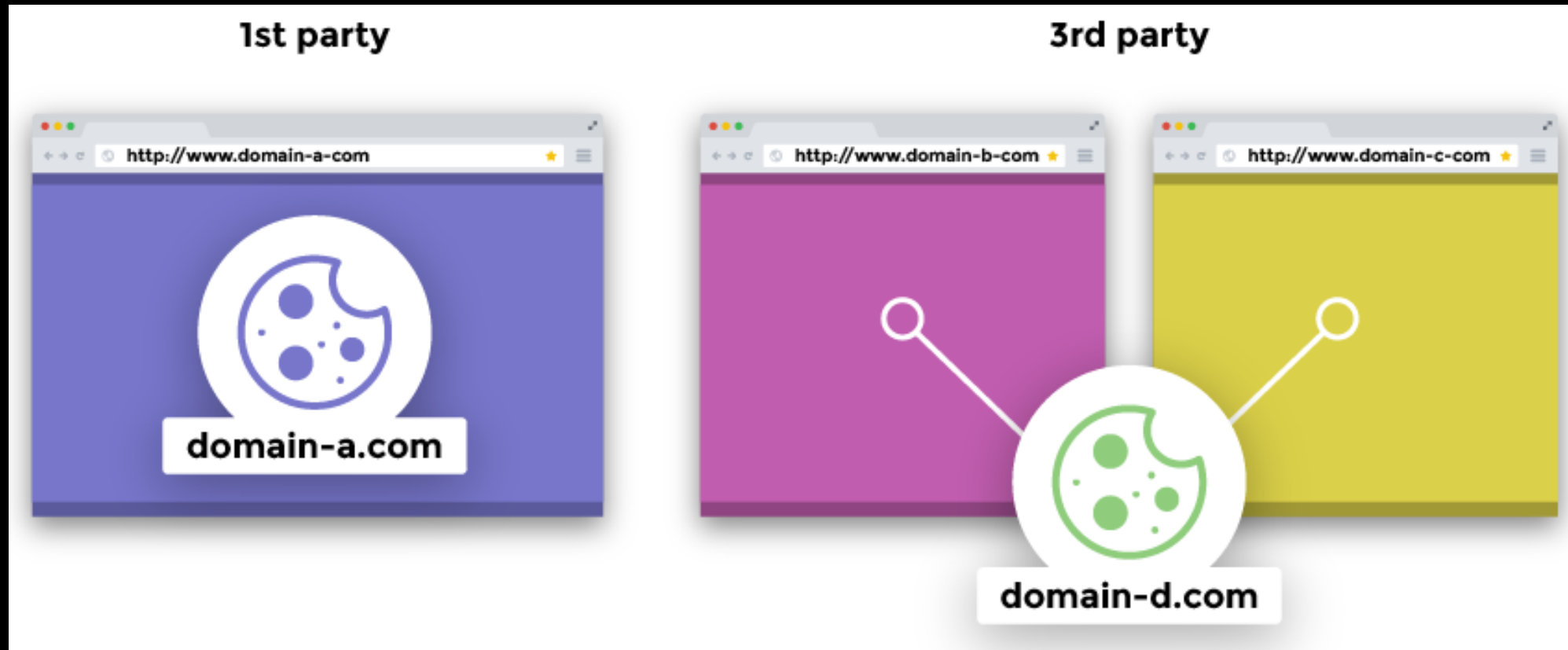


Privacy Sandbox for the Web. Timeline



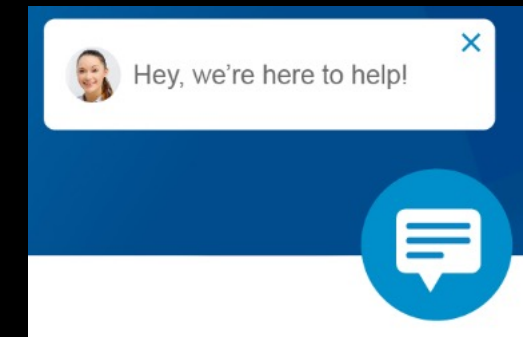
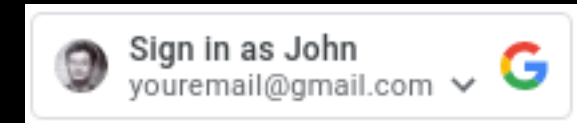
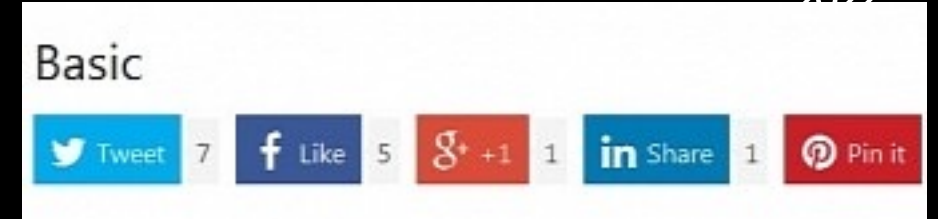
What is 3rd party?

Third-Party Cookies are cookies that are stored under a different domain than you are currently visiting.



There are many scenarios for the legal use of 3rd party cookies

- Social widgets
- Some OIDC cases
- Personalized login buttons
- Embedded support chat and other integrations
- Sharing data and actions cross domains
 - Country-specific domains to enable localization (google.co.in, google.co.uk)
 - Brand domains (uber.com, ubereats.com)
- Etc



Privacy Sandbox on Web



1. Strengthen cross-site privacy boundaries
2. Limit covert tracking
3. Measure digital ads
4. Show relevant content and ads
5. Fight spam and fraud

Privacy Sandbox on Web



- 1. Strengthen cross-site privacy boundaries**
2. Limit covert tracking
3. Measure digital ads
4. Show relevant content and ads
5. Fight spam and fraud

Privacy Sandbox on Web



Strengthen cross-site privacy boundaries:

- CHIPS
- First Party Set
- FedCM
- Shared Storage API
- Storage Partitioning
- Fenced Frames API
- Network State Partitioning

Privacy Sandbox on Web



Strengthen cross-site privacy boundaries:

- **CHIPS**
- **First Party Set**
- **FedCM**
- Shared Storage API
- Storage Partitioning
- Fenced Frames API
- Network State Partitioning

First Party Set

```
// https://a.example/.well-known/first-party-set
{
  "owner": "a.example",
  "members": ["b.example", "c.example"],
  ...
}

// https://b.example/.well-known/first-party-set
{
  "owner": "a.example"
}

// https://c.example/.well-known/first-party-set
{
  "owner": "a.example"
}
```


Example use cases for FPS



- App domains - a single application may be deployed over multiple domains, where the user may seamlessly navigate between them as a single session.
 - office.com, live.com, microsoft.com
 - lucidchart.com, lucid.co, lucidspark.com, lucid.app
- Brand domains
 - uber.com, ubereats.com
- Country-specific domains to enable localization
 - google.co.in, google.co.uk

First Party Set Subsets

Proposing changes to First-Party Sets based on community feedback



Open krgovind opened this issue 26 days ago · 1 comment



krgovind commented 26 days ago

Collaborator



Summary of proposed changes:

Based on feedback received during the incubation of First-Party Sets in the Privacy Community Group, we are proposing changes to the proposal. Following is a high-level summary of the changes, on which we invite community feedback. Please review the linked sections below for additional detail.

All of these changes are part of PR [#91](#) which we will review on an upcoming WICG call (see issue [#89](#))

- Define a set through [use-case-specific "subsets"](#). Each subset category will have its own requirements, and browser handling approach.
- [Leverage the Storage Access API](#) for sites to request cross-site cookie access, instead of the SameParty attribute.
- Abandon development of the [SameParty cookie attribute](#), which allowed synchronous cookie access on subresource requests, and, for the most part, allowed legacy same-party flows to continue functioning with minimal adoption costs involved for web developers. However, it prevents browsers' ability to mediate these flows and potentially intervene on behalf of users.

Benefits of proposed changes:

- Allows for more granular use-case specific requirements and browser handling policies that are more likely to align with user expectations.
- Achieves alignment and interoperability with other browsers' approach to mediate cross-site cookie access via Storage Access API.

Challenges:

- SAA involves greater adoption costs for web developers, compared to the SameParty cookie attribute. We hope to alleviate this to some extent via our [proposed extension to SAA](#).

Open question(s):

- We recognize that these changes also necessitate re-examining how [CHIPS integrates with](#) First-Party Sets. We are working on technical changes to that design as well, and will share updates when we have a proposal.



3

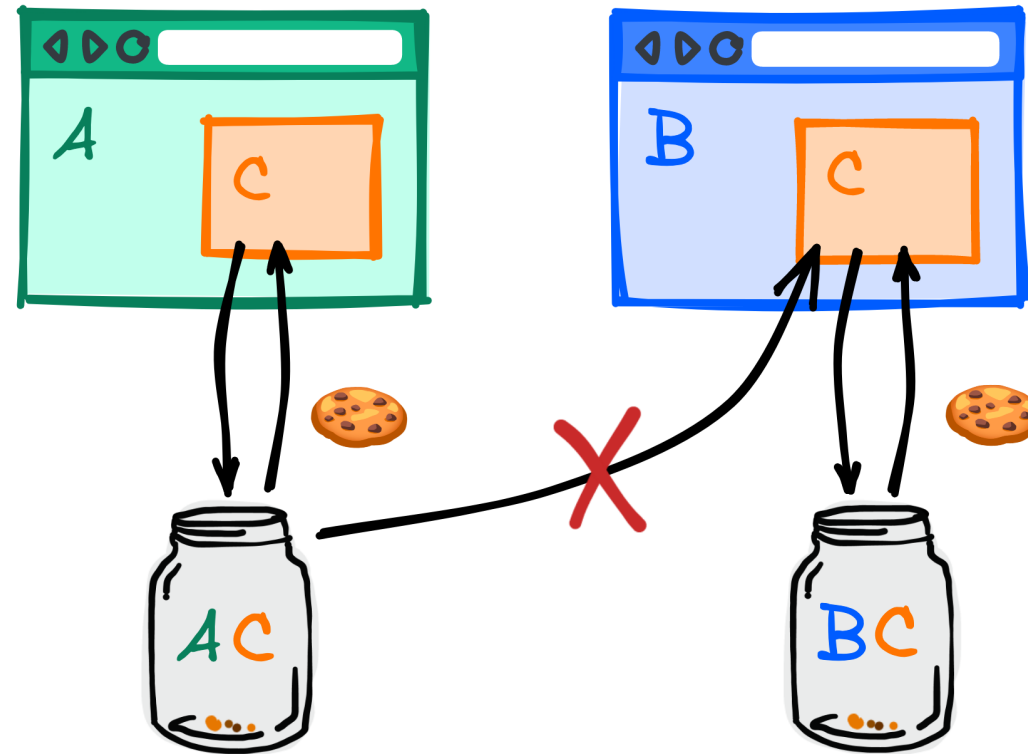


First Party Set Subsets

Subset type	Subset definition	Example browser handling policy
ccTLD (country code Top Level Domain)	Reserved for variations for a particular country or a geographical area. Requires common ownership.	No limit on domains, auto-grant access
common eTLD (effective Top Level Domain)	Reserved for domains that share a common eTLD as the set primary. These are not IANA-managed TLDs , but domains added to the PSL for improved security isolation. Requires common ownership.	No limit on domains, auto-grant access
service	Reserved for utility or sandbox domains. Requires common ownership.	No limit on domains, auto-grant access. Not allowed to be the top-level domain in a storage access grant.
associated	Reserved for domains whose affiliation with the set primary is clearly presented to users (e.g., an About page, header or footer, shared branding or logo, or similar forms).	Limit of 3* domains. If greater than 3, auto-reject access. * ^[1] exact number TBD

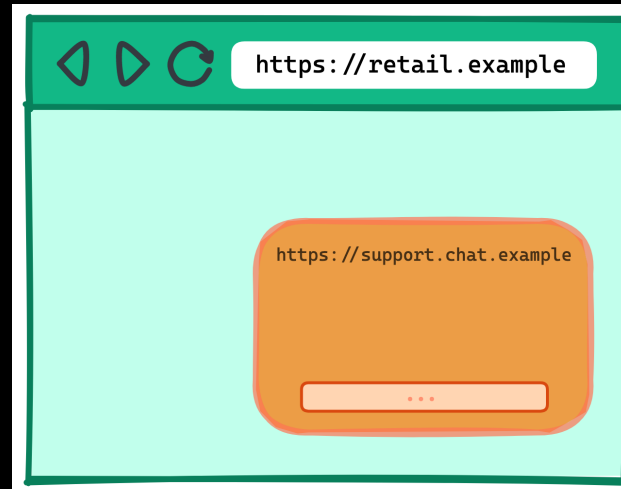
Cookies Having Independent Partitioned State (CHIPS)

Partitioned



A, B - top-level sites
C - embedded site

Cookies Having Independent Partitioned State (CHIPS)



Before CHIPS



key=("support.chat.example")

After CHIPS

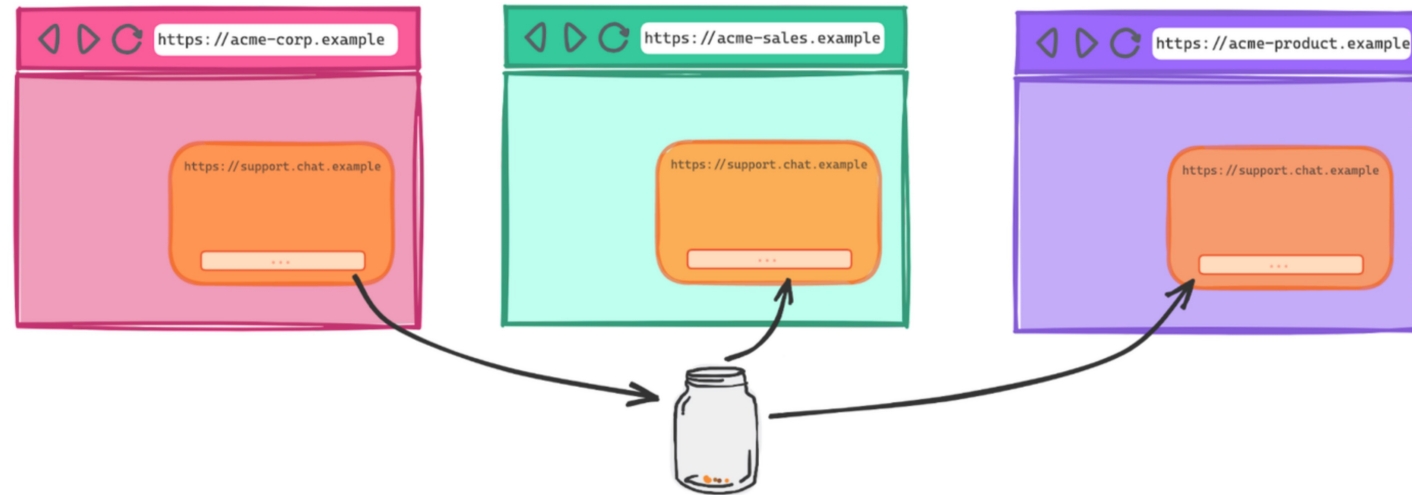


key={("https", "retail.example"),
("support.chat.example")}

CHIPS + FPS

Acme Corp owned and operated websites

```
owner: acme-corp.example  
member: acme-sales.example  
member: acme-product.example
```



```
key={("https", "acme-corp.example"),  
      ("support.chat.example")}
```


Example use cases for CHIPS

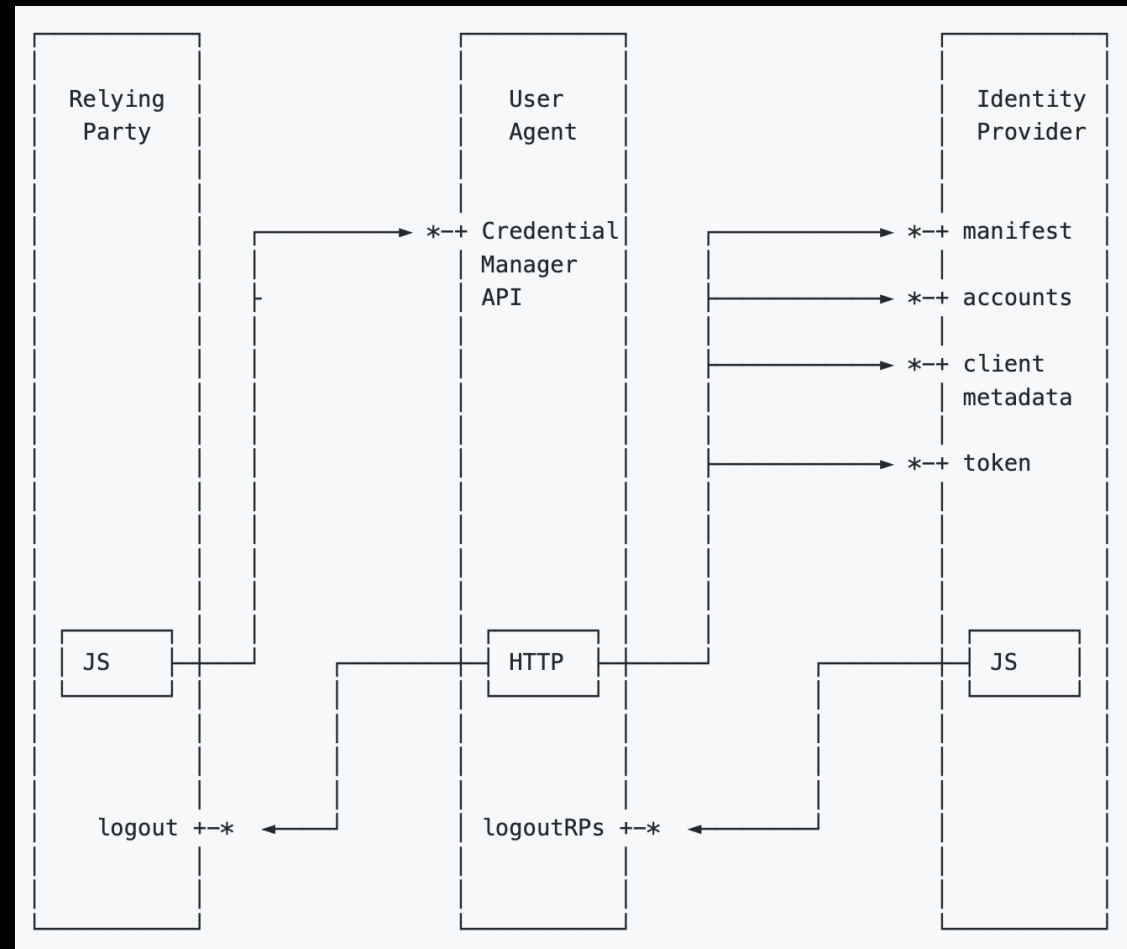
- Third-party chat embeds
- Third-party map embeds
- Subresource CDN load balancing
- Headless CMS providers
- Sandbox domains for serving untrusted user content (such as googleusercontent.com and githubusercontent.com)
- Third-party CDNs that use cookies to serve content that's access-controlled by the authentication status on the first-party site (for example, profile pictures on social media sites hosted on third-party CDNs)
- Front-end frameworks that rely on remote APIs using cookies on their requests
- Embedded ads that need state scoped per publisher (for example, capturing users' ads preferences for that website)

FedCM goals



- Enable all federated identity flows (including what will break) without the use of third-party cookies in a way that makes the web meaningfully more private and usable compared to the next best alternative
- Maximize backwards compatibility, especially for RPs
- Allow identity protocols to be extended independent of browser changes
- Reuse as much from OIDC / SAML / OAuth as possible

Federated Credential Management (FedCM)



Federated Credential Management (FedCM)

accounts_endpoint

The `accounts_endpoint` request is used to provide account information to be shown in the browser mediation dialogs.

For example:

```
GET /accounts HTTP/1.1
Host: idp.example
Accept: application/json
Cookie: 0x23223
Sec-FedCM-CSRF: ?1
```

```
{
  "accounts": [{
    "id": "1234",
    "given_name": "John",
    "name": "John Doe",
    "email": "john_doe@idp.example",
    "picture": "https://idp.example/profile/123",
    "approved_clients": ["123", "456", "789"]
  }, {
    "id": "5678",
    "given_name": "Johnny",
    "name": "Johnny",
    "email": "johnny@idp.example",
    "picture": "https://idp.example/profile/456",
    "approved_clients": ["abc", "def", "ghi"]
  }]
}
```

The information returned from the `accounts_endpoint` is not exposed to the RP, but instead used by the browser to render the mediated account chooser dialog.

Federated Credential Management (FedCM)

A screenshot of a web browser window. The address bar shows the URL 'fedcm-rp-demo.glitch.me'. The page has a green header with the text 'FedCM RP Demo'. Below the header, the main content area says 'Welcome to FedCM RP Demo' and features a green button labeled 'SIGN-IN ON IDP'. Below this button, there is instructional text: 'If you don't see a sign-in dialog, you need to sign-in on' and 'Use account ID of "multiple-accounts" to try multiple acc'. On the right side of the browser window, a sign-in dialog is open. The dialog title is 'Вход на сайт fedcm-rp-demo.glitch.me с учетными данными fedcm-idp-demo.glitch.me'. It shows a user profile for 'Janelle Murells demo' with a blue button labeled 'Продолжить как Janelle'. Below the button, there is a paragraph of Russian text explaining the process: 'Чтобы продолжить, fedcm-idp-demo.glitch.me передаст ваше имя, адрес электронной почты и фото профиля на этот сайт. Ознакомьтесь с его [политикой конфиденциальности](#) и [условиями использования](#).'

Typical privacy sandbox surfing



Read more ↗	
Federated Credential Management	Federated Credential Management aims to bridge the gap for the federated identity designs which relied on third-party cookies. The API provides the primitives needed to support federated identity when/where it depends on third-party cookies, from sign-in to sign-out and revocation. Read more ↗
Limit covert tracking	

Typical privacy sandbox surfing

FedID CG Federated Credentials Management

This is the repository for the W3C's FedID CG Federated Credentials Management API.

Explainer: [explainer.md](#)

Work-in-progress specification: <https://fedidcg.github.io/FedCM/>

Introduction

As the web has evolved there have been ongoing privacy-oriented changes ([example](#)) and underlying privacy [principles](#). With those changes some underlying assumptions of the web are changing. One of those changes is the deprecation of third-party cookies. While overall good for the web, third-party cookie deprecation leaves holes in how some existing systems on the web were designed and deployed.

Federated Credentials Management API aims to fill the specific hole left by the removal of third-party cookies on federated login. Historically this has relied on third-party cookies or navigational redirects in order to function as they were the primitives provided by the web.

The [explainer](#) and [spec](#) provide a potential API and the rational behind how that API was designed.

Contributing

Much of the FedCM specification has evolved due to the experimentation detailed in the [explorations](#). The

Typical privacy sandbox surfing

account_id=123&client_id=client1234

Related Work

This is a set of related work that we expect to be used in conjunction with this proposal.

First Party Sets

FedCM gathers the users consent to avoid [unwanted cross-contexts recognition](#) and deliberately leaves to each user agent the delineation of [partitions](#) and the [privacy boundary](#) they want to set for their users.

We expect this proposal to work well either in conjunction with, in the absence of or in coordination with [First Party Sets](#).

By that we mean that FedCM gathers the user's consent:

- at every [cross-party](#) data exchange, for browsers that adopt First Party Sets as a widening of the [machine enforceable contexts](#) or
- at every cross-site data exchange, for browsers that don't or
- at every cross-site data exchange but with wording that takes into account first party sets ([example](#))

FedCM is being designed to work under different privacy boundaries chosen by different browsers. While First Party Sets complements FedCM they are not required.

Enterprise Policies

Enterprise Policies are policies that administrators set for devices managed and supplied by their enterprise. While expected to cover a large set of devices, the community has stated there is a substantial number of employees that bring their own devices that need federation to work (mostly front channel based) in the absence of third party cookies.

Typical privacy sandbox surfing

- 1.1.2 Privacy Labour
- 1.2 Collective Governance
 - 1.2.1 Group Privacy
 - 1.2.2 Transparency and Research
- 1.3 People's Agents
- 1.4 Incorporating Different Privacy Principles

2. Principles for Privacy on the Web

- 2.1 Identity on the Web
 - 2.1.1 Unwanted cross-context recognition
 - 2.1.1.1 Same-site recognition
 - 2.1.1.2 Unwanted cross-site recognition
- 2.2 Personal Data
- 2.3 Sensitive Information
- 2.4 Data Rights
- 2.5 De-identified Data
- 2.6 Collective Privacy
- 2.7 Guardians and Device Owners
- 2.8 Harassment
- 2.9 Unwanted Information
- 2.10 Vulnerable People
- 2.11 Consent, Withdrawal of Consent, Opt-Outs, and Objections
- 2.12 Notifications and Interruptions
- 2.13 Non-Retaliation

A. Common Concepts

- A.1 People

in.

Sometimes this means the UA should ensure that one site can't learn anything about their user's behavior on another site, while at other times the UA should help their user prove to one site that they have a particular identity on another site.

To do this, [user agents](#) have to make some assumptions about the borders between [contexts](#). By default, [user agents](#) define a **machine-enforceable context** or **partition** as:

- A set of [environments](#) (roughly iframes (including cross-site iframes), workers, and top-level pages)
- whose [top-level origins](#) are in the [same site](#) (but see [\[PSL-Problems\]](#))
- being visited within the same user agent installation (and browser profile, container, or container tab for user agents that support those features)
- between points in time that the person or user agent clears that [site's](#) cookies and other storage (which is sometimes automatic at the end of each session).

Even though this is the default, [user agents](#) are free to restrict this context as people need. For example, some user agents may help people present different [identities](#) to subdivisions of a single [site](#).

ISSUE 1 (CLOSED): Figure out the default privacy boundary for the web [agenda+](#)

There is disagreement about whether [user agents](#) may also widen their [machine-enforceable contexts](#). For example, some user agents might want to help their users present a single [identity](#) to multiple [sites](#) that the user understands represent a single [party](#), or to a [site](#) across multiple installations.

[User agents](#) should prevent people from being [recognized](#) across [machine-enforceable contexts](#) unless they intend to be recognized. This is a "should" rather than a "must" because there are many cases where the user agent isn't powerful enough to prevent recognition. For example if two or more services that a person needs to

Much of the FedCM specification has evolved due to the experimentation detailed in the [explorations](#). The

Typical privacy sandbox surfing

1.1.2
1.2
1.2.1
1.2.2
1.3
1.4

2.
2.1
2.1.1
2.1.1.1
2.1.1.2
2.2
2.3
2.4
2.5
2.6
2.7
2.8
2.9
2.10
2.11

2.12
2.13

A.
A.1
A.2

FAQ

Should I use the Public Suffix List/eTLD+1 for ...

The answer is **no**. For anything new, you should **avoid** the Public Suffix List.

Wait, I wasn't finished!

That's not a question! However, the use case of the Public Suffix List has traditionally fallen on one of three dimensions: trying to solve for **privacy**, **security**, or **usability**. The problem is that it under-delivers and over-promises on all three of these dimensions, leading to privacy, security, or usability *issues*, often worse than the ones it was trying to resolve.

So what am I supposed to use instead?

In general, you'll have far fewer security and privacy issues if you adopt the Same Origin Policy instead. While more restrictive, the consistency with the existing Web Platform, particularly Javascript, is far more desirable, in that it simplifies reasoning about the feature and any of its interactions with the Web Platform.

Developers don't like how restrictive the SOP is. Are you sure it's the right idea?

It's true, the SOP is a mighty hammer to wield, and it's far more restrictive than simply eTLD+1. As it's used today, eTLD+1 is often trying to be a shorthand for "associated with the same organization", and alternative expressions of such associations (such as explored by DBOUND or First Party Sets) may be stepping stones towards more flexible expressions. However, using eTLD+1 to try and approximate that does not work, because it defaults to an insecure state of assuming different origins are related, requiring sites to opt-out in order to maintain security or privacy boundaries, and can be easily circumvented through adding to the PSL or through the use of CNAMEs to bypass any intended restrictions.

What are we going to do about cookies then?

Hope for the best, and that clever folks can find a path to deprecating cookies' big assumption? It's important to

Typical privacy sandbox surfing

FAQ



What are we going to do about cookies then?

Hope for the best, and that clever folks can find a path to deprecating cookies' big assumption? It's important to

Thanks for your attention

