# The Need for a (Research) Sandstorm through the Privacy Sandbox

Yohan Beugin & Patrick McDaniel

HotPETS - July 19, 2024

Computer Sciences
SCHOOL OF COMPUTER, DATA & INFORMATION SCIENCES
UNIVERSITY OF WISCONSIN–MADISON

MADS&P

# Outline

1. What is the Privacy Sandbox?

2. Overview of Analyses

3. Research Opportunity

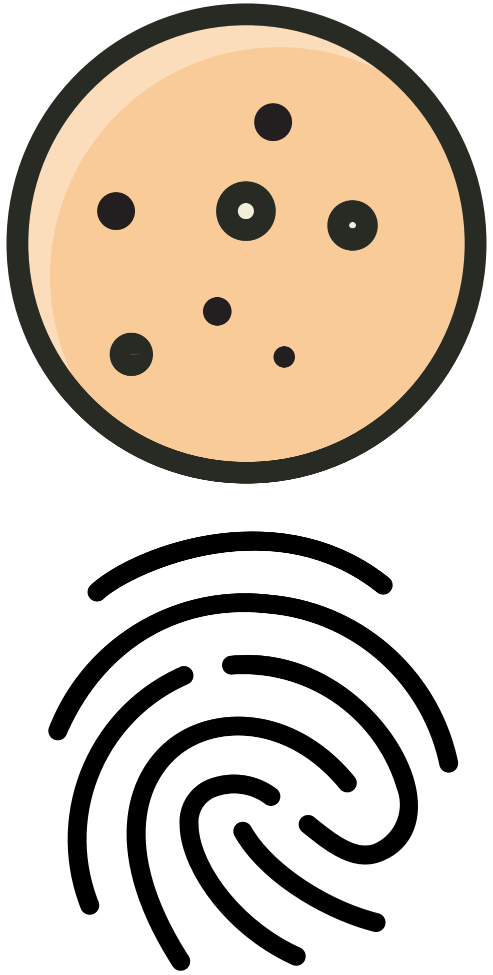
4. Discussion

# 1. What is the Privacy Sandbox?

# The Privacy Sandbox from Google

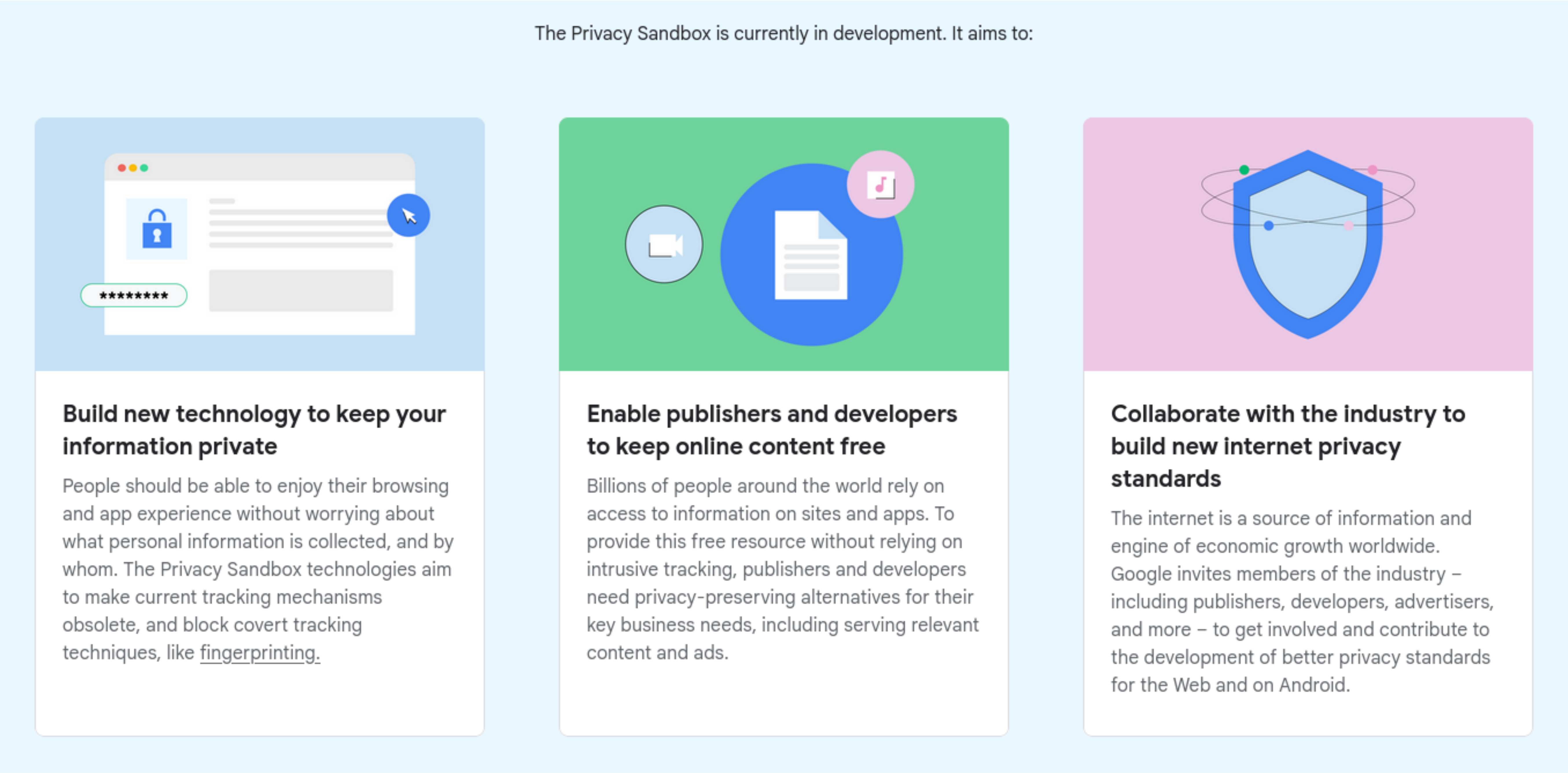
Privacy Sandbox

Creating a more private internet



https://privacysandbox.com

# 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.

https://privacysandbox.com

# Proposals for the Web and Android

## Show relevant content and ads

- FLoC API (deprecated)
- Topics API +
- Protected Audience API (FLEDGE) +

## Measure digital ads

- Attribution Reporting API +

## Strengthen cross-site privacy boundaries

- Related Website Sets
- Shared Storage API
- CHIPS
- Fenced Frames API
- Federated Credential Management

## Fight Spam and Fraud on the Web

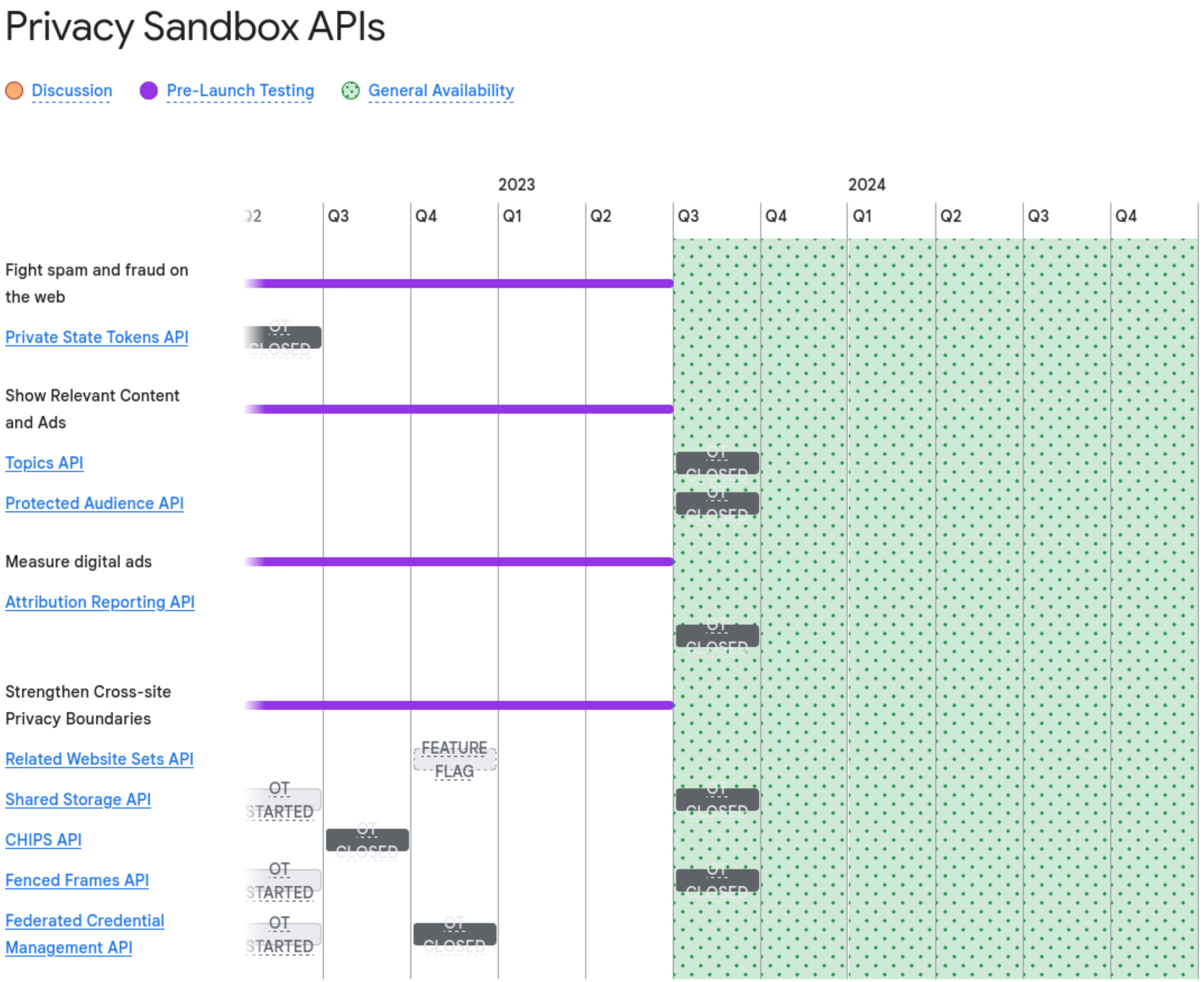
- Private State Tokens

## Limit covert tracking

- User-Agent Client Hints
- User-Agent Reduction
- DNS-over-HTTPS
- IP Protection
- Privacy Budget
- Storage Partitioning
- Network State Partitioning
- Bounce Tracking Mitigations
- SDK Runtime

...

# Timelines



Privacy Sandbox APIs

● Discussion ● Pre-Launch Testing ● General Availability

Fight spam and fraud on the web

Private State Tokens API

Show Relevant Content and Ads

Topics API

Protected Audience API

Measure digital ads

Attribution Reporting API

Strengthen Cross-site Privacy Boundaries

Related Website Sets API

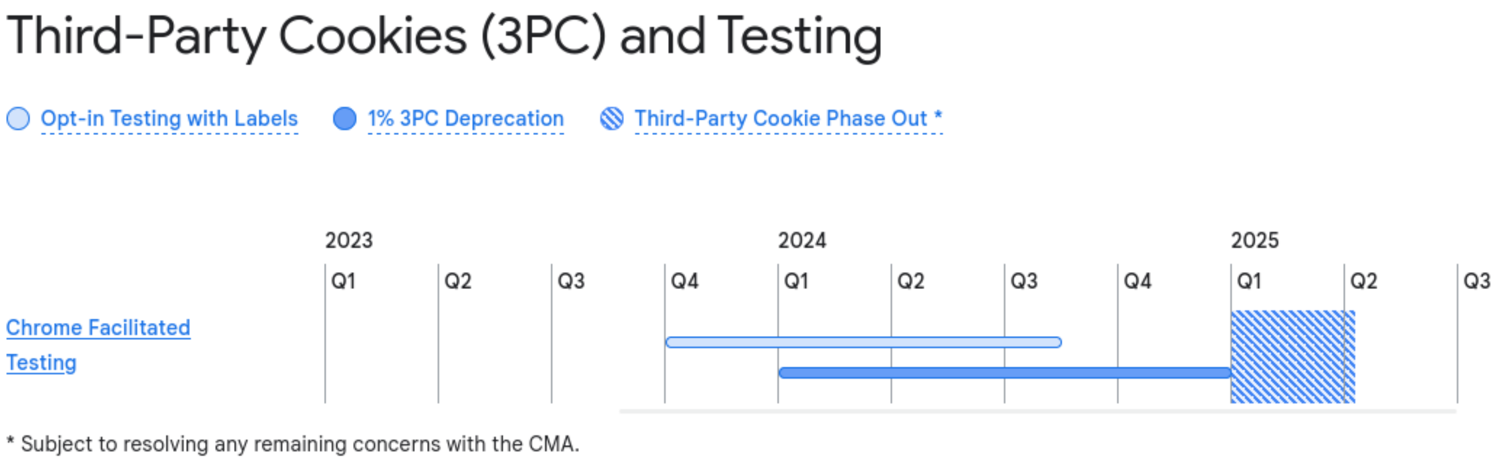
Shared Storage API

CHIPS API

Fenced Frames API

Federated Credential Management API

https://privacysandbox.com

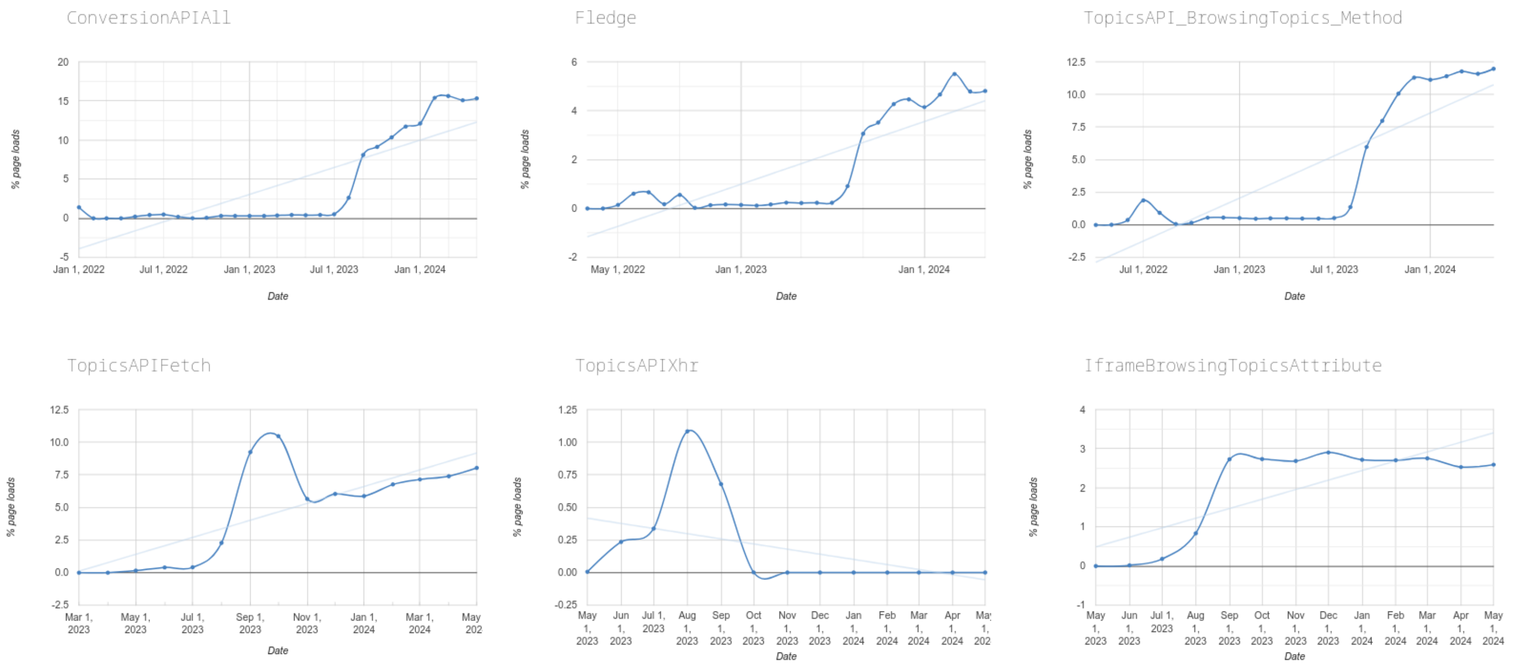


Third-Party Cookies (3PC) and Testing

○ Opt-in Testing with Labels ● 1% 3PC Deprecation ▨ Third-Party Cookie Phase Out *

Chrome Facilitated Testing

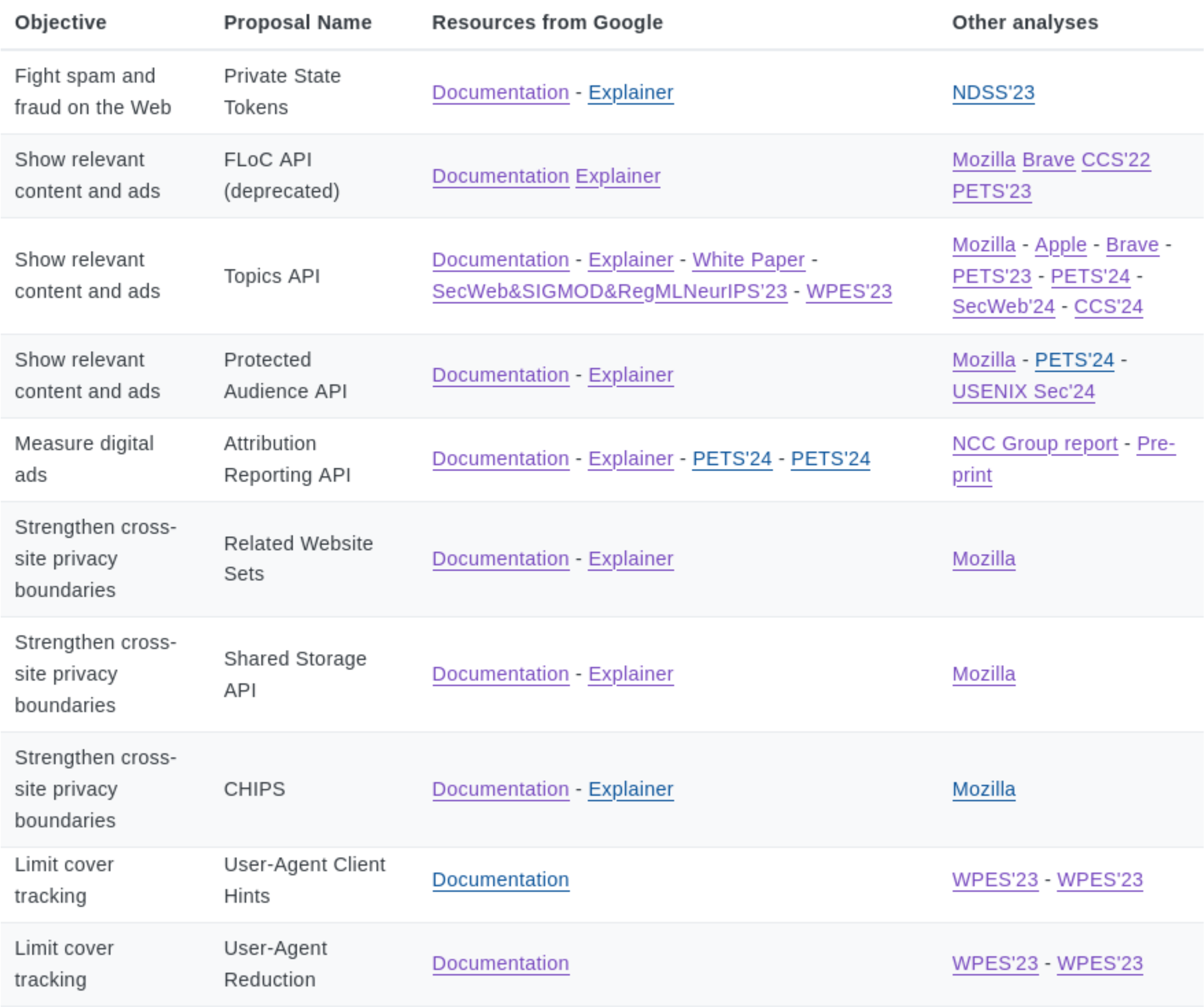
* Subject to resolving any remaining concerns with the CMA.



https://ps-charts.glitch.me/

# 2. Overview of Analyses

# Overview (*incomplete)



| Objective | Proposal Name | Resources from Google | Other analyses |
|---|---|---|---|
| Fight spam and fraud on the Web | Private State Tokens | Documentation - Explainer | NDSS'23 |
| Show relevant content and ads | FLoC API (deprecated) | Documentation Explainer | Mozilla Brave CCS'22 PETS'23 |
| Show relevant content and ads | Topics API | Documentation - Explainer - White Paper - SecWeb&SIGMOD&RegMLNeurIPS'23 - WPES'23 | Mozilla - Apple - Brave - PETS'23 - PETS'24 - SecWeb'24 - CCS'24 |
| Show relevant content and ads | Protected Audience API | Documentation - Explainer | Mozilla - PETS'24 - USENIX Sec'24 |
| Measure digital ads | Attribution Reporting API | Documentation - Explainer - PETS'24 - PETS'24 | NCC Group report - Pre-print |
| Strengthen cross-site privacy boundaries | Related Website Sets | Documentation - Explainer | Mozilla |
| Strengthen cross-site privacy boundaries | Shared Storage API | Documentation - Explainer | Mozilla |
| Strengthen cross-site privacy boundaries | CHIPS | Documentation - Explainer | Mozilla |
| Limit cover tracking | User-Agent Client Hints | Documentation | WPES'23 - WPES'23 |
| Limit cover tracking | User-Agent Reduction | Documentation | WPES'23 - WPES'23 |

Web Proposals

# 3. A Research Opportunity

# Our Vision

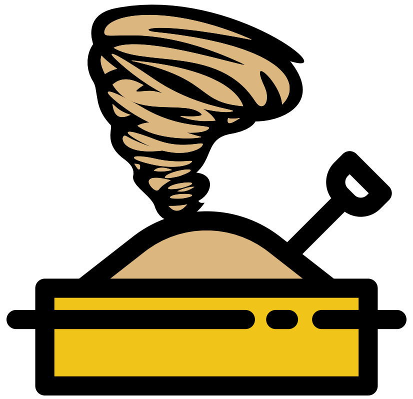
## Observations

- Disconnect objectives/evaluations
- Flaws and limitations are being uncovered…
- …but still being deployed to real users

## What now?

- True understanding of these nascent tools
- Forecast potential consequences
- More multidisciplinary approaches needed

## A (Research) Sandstorm through the Privacy Sandbox



- Research portal with resources
- Provide visibility to research results
- Basis for collaboration

https://privacysandstorm.com

# 4. Discussion

# Objectives

## This is about …

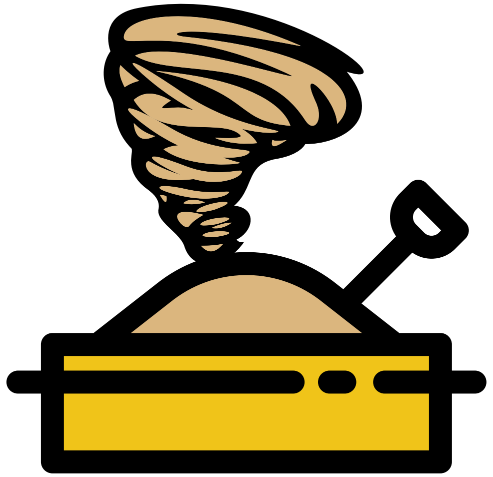
- Starting a discussion among the PETS community
- Brainstorming about concrete and actionable steps
- List research questions and resources
- Opportunity to have real impact based on facts
- Ultimately protect users' privacy

## … and not

- Pointing fingers
- "wait and see"

# Some Questions & Points to Discuss

- Potential research questions to focus on?
- Resources needed (datasets, tools, etc.)?
- How to provide more visibility to research results?
- What other things can we do as a community?
- How to get organized and coordinate these efforts? (Slack, online seminar?)
- Anything else?
- …



https://privacysandstorm.com

# Conclusion

- Complex modifications & potential unforeseen consequences
- Opportunity to truly protect users and impact changes
- Start of discussion and interaction: keep it going
- Community-based effort: open-source contributions

Thanks!

🌐 https://privacysandstorm.com

✉ yohan@beugin.org 🏠 https://yohan.beugin.org