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

YOHAN BEUGIN & PATRICK MCDANIEL
HotPETS - July 19, 2024
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:

1. **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.

2. **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.

3. **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

Limit covert tracking

- Private State Tokens
- 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

<table>
<thead>
<tr>
<th>2022</th>
<th>2023</th>
<th>2024</th>
<th>2025</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
</tr>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
</tr>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
</tr>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
</tr>
</tbody>
</table>

- 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

Third-Party Cookies (3PC) and Testing

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

* Subject to resolving any remaining concerns with the CMA.

https://privacysandbox.com

https://ps-charts.glitch.me/
2. Overview of Analyses
## Overview (*incomplete*)

<table>
<thead>
<tr>
<th>Objective</th>
<th>Proposal Name</th>
<th>Resources from Google</th>
<th>Other analyses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fight spam and fraud on the Web</td>
<td>Private State Tokens</td>
<td>Documentation - Explainer</td>
<td>NDS23</td>
</tr>
<tr>
<td>Show relevant content and ads</td>
<td>FLoC API (deprecated)</td>
<td>Documentation - Explainer</td>
<td>Mozilla Brave CCS22, PETS23</td>
</tr>
<tr>
<td>Show relevant content and ads</td>
<td>Topics API</td>
<td>Documentation - Explainer - White Paper, SecWeb&amp;SIGMOD&amp;RegMLNeuriPS'23, WPES'23</td>
<td>Mozilla - Apple - Brave - PETS23, PETS24, SecWeb'24, CCS'24</td>
</tr>
<tr>
<td>Show relevant content and ads</td>
<td>Protected Audience API</td>
<td>Documentation - Explainer</td>
<td>Mozilla - PETS24, USENIX Sec'24</td>
</tr>
<tr>
<td>Measure digital ads</td>
<td>Attribution Reporting API</td>
<td>Documentation - Explainer - PETS24, PETS24</td>
<td>NCC Group report - Pre-print</td>
</tr>
<tr>
<td>Strengthen cross-site privacy boundaries</td>
<td>Related Website Sets</td>
<td>Documentation - Explainer</td>
<td>Mozilla</td>
</tr>
<tr>
<td>Strengthen cross-site privacy boundaries</td>
<td>Shared Storage API</td>
<td>Documentation - Explainer</td>
<td>Mozilla</td>
</tr>
<tr>
<td>Strengthen cross-site privacy boundaries</td>
<td>CHIPS</td>
<td>Documentation - Explainer</td>
<td>Mozilla</td>
</tr>
<tr>
<td>Limit cover tracking</td>
<td>User-Agent Client Hints</td>
<td>Documentation</td>
<td>WPES'23, WPES'23</td>
</tr>
<tr>
<td>Limit cover tracking</td>
<td>User-Agent Reduction</td>
<td>Documentation</td>
<td>WPES'23, WPES'23</td>
</tr>
</tbody>
</table>
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