Private Advertising Technology

Where Goes Advertising, There Goes the Web
Ads power the web
Digital Advertising Soared 35% to $189 Billion in 2021 According to the IAB

Digital Ad Spending Worldwide, 2019-2024

<table>
<thead>
<tr>
<th>Year</th>
<th>Digital Ad Spending</th>
<th>% Change</th>
<th>% of Total Media Ad Spending</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>$35.60</td>
<td>51.0%</td>
<td></td>
</tr>
<tr>
<td>2020</td>
<td>$37.16</td>
<td>58.2%</td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td>$45.30</td>
<td>60.9%</td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td>$52.31</td>
<td>63.6%</td>
<td></td>
</tr>
<tr>
<td>2023</td>
<td>$58.96</td>
<td>65.9%</td>
<td></td>
</tr>
<tr>
<td>2024</td>
<td>$64.80</td>
<td>67.8%</td>
<td></td>
</tr>
</tbody>
</table>

Note: includes advertising that appears on desktop and laptop computers as well as mobile phones, tablets, and other internet-connected devices, and includes all the various formats of advertising on those platforms; excludes SMS, MMS, and P2P messaging-based advertising.

Source: eMarketer
And They Break It
Why top publishers are still stuck distributing fake news

DECEMBER 13, 2016 by Lucia Moses

The prominence of fake and misleading news has shed light on how programmatic advertising, facts like Play-Doh, trying to shape them to their ends, but they were still acknowledging, and working with, the same shared underlying realities.
$23 Billion
Projected loss to ad fraud in 2019

From: https://www.campaignlive.co.uk/article/unilever-were-miles-ahead-pack-tackling-ad-fraud/1592052
Privacy is the Future & It’s Coming at You Fast
This is complicated

So let’s equip you to develop and contribute by examining:

● What is going on and why

● High level understandings of the related proposals

● The underlying concepts

● How to get involved
Browser and Standards Concerns

Security/Anti tracking policy

Tracking is the collection of data regarding a particular user's activity across multiple websites, sharing of data derived from that activity with parties other than the first party on whose website the user is interacting is characterized by a deliberate action, such as clicking a link, submitting a form, or performing an action that constitutes an intention to interact. Interactions with other parties are considered third party actions.

A first party is a resource or a set of resources on the web operated by the same organization that has the ability to influence the interaction with the user. A third party is any party that does not fall within the definition of first party above.

Tracking We Will Block

1. Cross-site tracking

Cookie-based cross-site tracking, Cookies, DOM storage, and other types of stateful identifiers are often used by third parties to build profiles of those users, in violation of the user's expectation.

Regulations are here

A look at Canada's new federal privacy legislation, Bill C-27
With Privacy Changes for Ads
Other Parts of the Web are Forced to Change As Well
Federated Credential Management (FedCM)

Last Update: Mar 08, 2022

Introduction

Over the last decade, identity federation has played a central role in raising the bar for authentication on the web, in terms of ease-of-use (e.g. password-less single sign-in), security (e.g. improved resistance to phishing and credential stuffing attacks) and trustworthiness compared to per-site usernames and passwords. In identity federation, a **RP (relying party)** relies on an **IDP (identity provider)** to provide the user an account without requiring a new username and password.

Unfortunately, the mechanisms that identity federation was designed on (iframes, redirects and cookies) are being abused to track users across the web. A user agent isn’t able to differentiate between identity federation and tracking, the mitigations for the various types of abuse make identity federation more difficult.

The Federated Credential Management API provides a use case specific abstraction for federated identity flows on the web. The
Improving user privacy and developer experience with User-Agent Client Hints

User-Agent Client Hints are a new expansion to the Client Hints API, that enables developers to access information about a user's browser in a privacy-preserving and ergonomic way.

Jun 25, 2020 — Updated Sep 10, 2021

Available in: Deutsch, English, Español, Français, Português, Русский, 中文, 日本語, and 한국어

Appears in: Safe and secure

Rowan Merewood

Yoav Weiss
Trust Tokens

An API to convey a limited amount of information from one browsing context to another (for example, across sites) to help combat fraud, without passive tracking.

Published on Tuesday, May 18, 2021 • Updated on Thursday, March 31, 2022

Translated to: Español, Português, 한국어, 中文, Русский, 日本語, Français, Deutsch

Sam Dutton
Developer Advocate, Google Chrome
Cookies Having Independent Partitioned State (CHIPS)

Allow developers to opt-in a cookie to "partitioned" storage, with a separate cookie jar per top-level site.

Published on Tuesday, February 15, 2022 • Updated on Friday, June 10, 2022
Translated to: 日本語

Milica Mihajlija
Milica is a technical writer at Chrome.

Partitioned

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

If a user visits site C as a top level website, the partitioned cookie that C set when it was embedded in A will not be sent in that request either.
The Storage Access API

A Work Item of the Privacy Community Group.

Editors:

- Benjamin VanderSloot
- Johann Hofmann
- John Wilander

Participate

- https://github.com/privacycg/storage-access/issues

---

Client-Side Storage Partitioning

---

Introduction

Browsers may block third-party resources from accessing cookies and other storage for privacy and security reasons. The most popular reason is cross-site tracking prevention. Such blocking breaks authenticated cross-site embeds such as commenting widgets, embedded payment providers, and subscribed video services.

The Storage Access API provides a means for authenticated cross-site embeds to check their blocking status and request access to storage if they are blocked.

---

Introduction

User agent state that is keyed by a single origin or site is an acknowledged privacy and security bug. Through side-channels or more directly, this allows:

1. A top-level site https://site-a.example A to infer that a user is also visiting top-level site https://site-b.example B, by embedding resources or documents from B in A. Beyond visiting, it can also allow A to infer specific state from B that depends on the user, thereby revealing many aspects of the user. Timing Attacks on Web Privacy, XS-Leaks, and COSI discuss this in more detail.

2. Conversely, it allows a site https://tracker.example whose resources might be embedded on many different sites, to track the end user across these sites.

To solve a key aspect of this, any such user agent state needs to be keyed by more than a single origin or site.

From: https://github.com/privacycg/storage-access, https://github.com/privacycg/storage-partitioning
Privacy Tech Concepts
Browser Mediation

A great example of how a complex browser mediated operation works can be examined in the FLEDGE proposal.

https://github.com/WICG/turtledove/blob/main/FLEDGE.md#2-sellers-run-on-device-auctions
Federated Learning

Read More:
https://federated.withgoogle.com/
Secure Multi-party Computation

A USER-GENERATED VALUE  DIVIDE THE VALUE  TWO NON-COLLUDING SERVERS  COMBINE AGGREGATES  ANONYMIZED INSIGHT

From: https://divviup.org/about/
Privacy Mechanisms
Differential Privacy: Obscure and Delay
K-anonymity: Lost in the crowd
Ad-Tech-Focused Privacy Proposals
Protected Execution
Ad Flows
Design Elements

Ads can be targeted at interest groups. As in the original TURTLEDOVE proposal, the browser is responsible for knowing which interest groups it has joined.

Every interest group has an owner who will act as a buyer in an on-device ad auction. The owner is ultimately responsible for the group's membership and usage, but can delegate those tasks to third parties if they so desire. Many sorts of entities might want to be owners of interest groups. Some examples include:

- An advertiser (or a third party working on the advertiser's behalf) might create and own an interest group of people whom they believe are interested in that advertiser's product. Classical remarketing/retargeting use cases fall under this example.
- A publisher (or a third party working on the publisher's behalf) might create and own an interest group of people who have read a certain type of content on their site. Publishers can already use first-party data to let advertisers target their readers on the publisher site. A publisher-owned interest group could let publishers do the same even when those people are browsing other sites. Publishers would presumably charge for the ability to target this list.
- A third-party ad tech company might create and own an interest group of people whom they believe are in the market for some category of item. They could use that group to serve ads for advertisers who work with that ad tech company and sell things in that category.

- Assign users interest groups that are held by the browser
- Assign a trusted server that can operate on that data to decide if it wants to target ads.
- Browser mediation handles ad decision.
- Ad is rendered in a secure space that has no page access.

From: https://github.com/WICG/turtledove/blob/main/FLEDGE.md
PARAKEET

At a high level:

1. The browser, working together with the browser-provided service, will apply modifications to the ad request before it is sent to the ad network. It will:
   i. Anonymize the context provided by the publisher.
   ii. Augment the ad request with the browser-provided anonymized user’s ad interests, having ensured the request meets privacy requirements around identifiability and user control.
   iii. Anonymize the user’s geographic information and other client-specific context where possible by making information coarser and/or adding randomization to meaningfully reduce the ability to deidentify the client.
   iv. Support user interest inference models for advertisers based on the activities on their site.
   v. Use differential privacy and service-assisted global context to enforce limits on the identifiability of user interest information and contextual signals sent in ad requests.

2. The ad network will perform ad matching, ranking and auction with contextual and user interest information provided in the privacy-anonymized ad request.

- Assign users interest groups that are held by the browser
- Assign a trusted server that can manage bidding on ad positions.
- Ad is rendered in a secure space that has no page access.

From: https://github.com/WICG/privacy-preserving-ads/blob/main/Parakeet.md
Fenced Frames

iFrames + Sandboxing on Steroids

- Could replace the iFrame for displaying ads
- Allow operation internal to the domain which hosts it
- Do not allow operations with the embedding domain

From: https://github.com/WICG/fenced-frame/tree/master/explainer
Private Measurement
Apple’s PCM

Delayed, ephemeral HTTP POST to
social.example/.well-known/private-click-measurement/report-attribution/

From: https://github.com/WICG/fenced-frame/tree/master/explainer
Google’s Attribution Reporting

Event-level reports

Event-level reports associate an ad click or view with coarse conversion data.

Summary reports

Summary reports (formerly known as aggregate reports) offer more detailed conversion data and more flexibility for joining click/view data and conversion data.

Learn more about in Attribution Reporting: summary reports.

Mozilla & Meta - Interoperable Private Attribution (IPA)

From: https://docs.google.com/document/d/1KpdSKD8-Rx0bWP7jUJiK5ks0yy2j22pA5SrAD9av4s/edit?usp=sharing
Tools for Thinking About Privacy
Priority of Constituencies @ W3C

User needs come before the needs of web page authors,
which come before the needs of user agent implementers,
which come before the needs of specification writers,
which come before theoretical purity.

From: https://www.w3.org/TR/design-principles/#priority-of-constituencies
Privacy by Design

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric
Do You Need Personally Identifying Information? (PII)
Does the User Understand?
How to get Involved
Building the More Private Web
(via the W3C)
Payments:
To help ensure that the Web evolves to meet new industry needs, we’re convening e-commerce companies, payment service providers, card networks, banks, browser vendors, and others to shape the way Web Payments are developed.

Privacy Interest Group (PING):
“The Privacy Interest Group monitors ongoing privacy issues that affect the Web, investigates potential areas for new privacy work, and provides guidelines and advice for addressing privacy in standards development, including privacy considerations in specifications.”

Improving Web Advertising Business Group:
“The mission of the Improving Web Advertising Business Group is to identify areas where standards and changes in the Web itself can improve the ecosystem and experience for users, advertisers, publishers, distributors, ad networks, agencies and others, and to oversee liaison with existing Working Groups and to create new Working Groups as needed.”

Privacy Community Group:
“The mission of the Privacy Community Group, motivated by the W3C TAG Ethical Web Principles, is to incubate privacy-focused web features and APIs to improve user privacy on the web through enhanced browser behavior.”

Payments:
To help ensure that the Web evolves to meet new industry needs, we’re convening e-commerce companies, payment service providers, card networks, banks, browser vendors, and others to shape the way Web Payments are developed.
Federated Identity CG

“The purpose of the Federated Identity Community Group is to provide a forum focused on incubating web features that will both support federated identity and prevent untransparent, uncontrollable tracking of users across the web”

https://www.w3.org/community/fed-id/

WebAppSec

“The mission of the Web Application Security Working Group is to develop security and policy mechanisms to improve the security of Web Applications, and enable secure cross-site communication.”

https://www.w3.org/groups/wg/webappsec

WebAuthn Working Group

“The mission of the Web Authentication Working Group, in the Security Activity is to define a client-side API providing strong authentication functionality to Web Applications.”

https://www.w3.org/groups/wg/webauthn
Private Advertising Technology Community Group

Hi. We’re the Private Advertising Technology Community Group of the W3C.

The Private Advertising Technology CG is chartered “to incubate web features and APIs that support advertising while acting in the interests of users, in particular providing strong privacy assurances.” If that sounds interesting to you, please join us!

Participate

It’s easy to join the CG if you’d like to contribute to our work. Please note that, in order to join, you’ll need to request a W3C account if you don’t already have one.

We publish a list of current participants on our W3C page.

Our Work

We conduct all of our technical work in public, mainly in various GitHub repositories but also in periodic teleconferences and face-to-face meetings.

- We try to keep the list of our current work items in our charter up-to-date. You can follow links from there to each work item’s GitHub repository, where you can see the latest text, and file or comment on issues.
- We discuss new proposals in our proposals repository.
- We have teleconferences twice a month, and occasional face-to-face meetings throughout the year. We organize our meetings and publish the agendas and minutes from them in our meetings repository.
Give Feedback!

Origin-Trials and Public Specification create opportunities to get involved

The various W3C groups will make their recommendations and early specifications public on GitHub where anyone can comment on them and give feedback, regardless of membership.

All browsers run test releases of various features, testing and giving feedback via their sites is needed!
Read more:
https://context.center/topics/privacy/
Thank you!

Aram Zucker-Scharff
PATCG Co-Chair
Lead Privacy Engineer, The Washington Post
@Chronotope

Use this slideshow as a reference!
https://aramzs.me/w3cdevs