



# PrivacyTests.org

*Open source tests of web browser privacy*

Arthur Edelstein, PEPR, September 12, 2023

---

---

## In this talk

- Mass surveillance and browsers
- Design of PrivacyTests.org
- Examples of specific privacy tests and results
- Notable recent browser privacy progress
- What I have learned; future work

## Problem: the Web is a major target of mass surveillance

- The Web is a primary means of modern reading, writing, communication and commerce
- Most web browsers are heavily exposing their users to mass surveillance by corporations and governments

### **U.S. Spy Agencies Buy Vast Quantities of Americans' Personal Data, U.S. Says**

Commercially available data from cars, phones and web browsers rivals results from wiretaps, cyber espionage and physical surveillance

# How web browsers facilitate surveillance

- Browsers allow websites you visit and the trackers embedded in them to gather your browsing history
- Browsers fail to fully encrypt your network connections
- Browsers gather data on users (telemetry)



## Why are browsers (still) leaky?

- Web browser privacy leaks are hidden, technical, and complex
- Some major web browsers get their revenue from top trackers (Google, Bing), not from users
- Web compatibility concerns

Privacy has tended to be low priority for decision makers

## PrivacyTests.org: attempting to provide visibility

Try to make web browsers more accountable for protecting all web users from mass surveillance through:

- Detecting privacy leaks
- Monitoring those leaks over time
- Making the results public

# Challenges and design of PrivacyTests.org

Browser privacy leaks are invisible	Run tests and make results public
Browser privacy is highly technical	Present results as simple pass/fail
Results should be actionable	Compare browsers side-by-side
Browsers update ~1 month	Run tests and publish results weekly
Hard for readers to know who to trust	Open source; stick to facts
Many browser, many privacy leaks	Launch early, continue to add tests and browsers

# Building PrivacyTests.org

Proposed it at Tor 2018, slow progress

Started working on it independently full time in August 2021

First launched in October 2021

Iterative – it remains a work in progress!

The screenshot shows the PrivacyTests.org website. At the top, there is a navigation bar with a green checkmark logo, the site name "PrivacyTests.org", and links for "News", "About", and social media icons. Below the navigation bar, there is a header section with "No. 69", "Open-source tests of web browser privacy.", and "Updated 2023-09-07".

The main content area is titled "Desktop browsers" and features a table of browser privacy test results. The table has columns for different browser categories: Desktop private modes, Desktop private modes, iOS browsers, Android browsers, Nightly builds, and Nightly private modes. The rows list various tests, including State Partitioning tests, Navigation tests, and HTTPS tests. Each cell in the table contains a green checkmark (✓) for "Passed privacy test", a red X for "Failed privacy test", or a grey dash (--) for "No such feature".

Legend: ✓ = Passed privacy test, X = Failed privacy test, -- = No such feature. (Click anywhere for more info.)

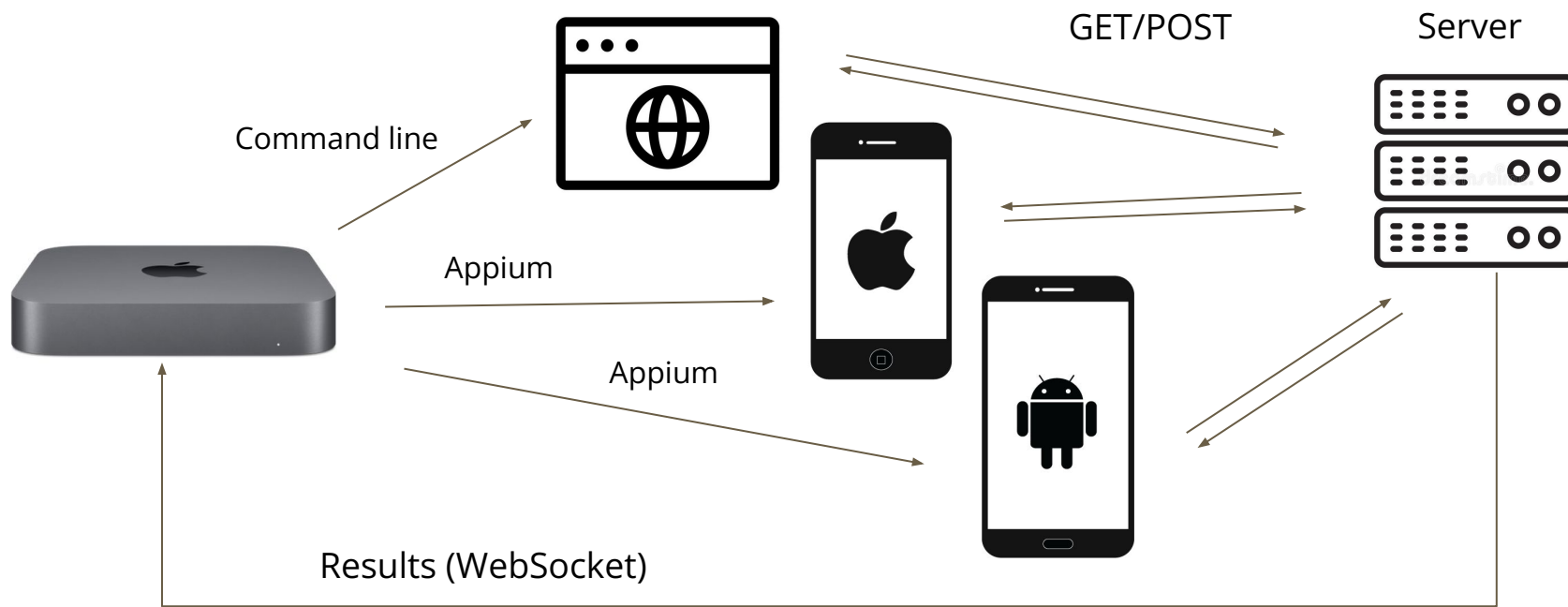
**Desktop Browsers** (default settings)

	Brave 1.57	Chrome 116.0	Edge 116.0	Firefox 117.0	Librewolf 117.0-1	Mulvad 12.5	Opera 101.0	Safari 16.6	Tor 12.5	Ungoogled 115.0	Vivaldi 6.2
<b>State Partitioning tests</b>											
Which browsers isolate websites to prevent them from sharing data to track you?											
Alt-Svc	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
blob	✓	X	X	X	X	✓	X	X	✓	X	X
BroadcastChannel	✓	X	X	X	X	✓	X	X	✓	X	X
CacheStorage	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
cookie (HTTP)	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
cookie (JS)	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
CookieStore	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
CSS cache	✓	X	X	✓	✓	✓	X	✓	✓	X	X
favicon cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
fetch cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
font cache	✓	X	X	✓	✓	✓	X	✓	✓	X	X
getDirectory	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
H1 connection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
H2 connection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
H3 connection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
HSTS cache	✓	X	X	✓	✓	✓	X	✓	✓	X	X
iframe cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
image cache	✓	X	X	✓	✓	✓	X	✓	✓	X	X
indexedDB	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
localStorage	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
locks	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
prefetch cache	✓	X	X	✓	✓	✓	X	✓	✓	X	X
ServiceWorker	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SharedWorker	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
TLS Session ID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web SQL Database	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
XMLHttpRequest cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>Navigation tests</b>											
Which browsers prevent websites from sharing tracking data when you click on a link?											
document.referrer	X	X	X	X	X	X	X	X	X	X	X
sessionStorage	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
window.name	✓	X	X	✓	✓	✓	X	✓	✓	✓	X
<b>HTTPS tests</b>											
Which browsers use encrypted network connections whenever possible?											
Insecure website	X	X	X	X	✓	✓	X	X	✓	X	X
Upgradable address	✓	X	X	X	✓	✓	X	X	✓	X	X
Upgradable hyperlink	✓	X	X	X	✓	✓	X	X	✓	X	X
Upgradable image	✓	✓	✓	X	✓	✓	✓	X	✓	✓	✓
Upgradable script	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

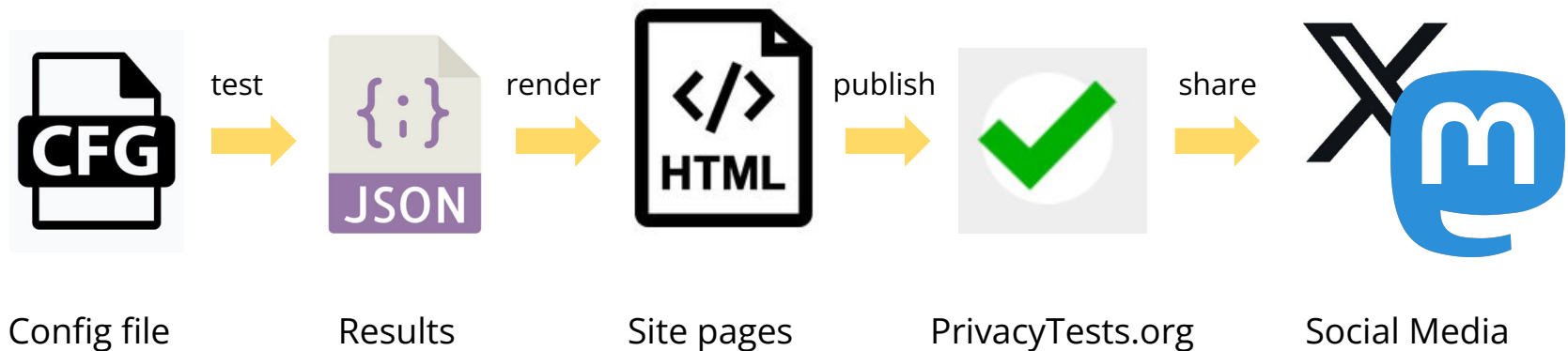


# PrivacyTests.org browser testing approach

Almost all JavaScript (NodeJS and in-browser)



# PrivacyTests.org testing pipeline

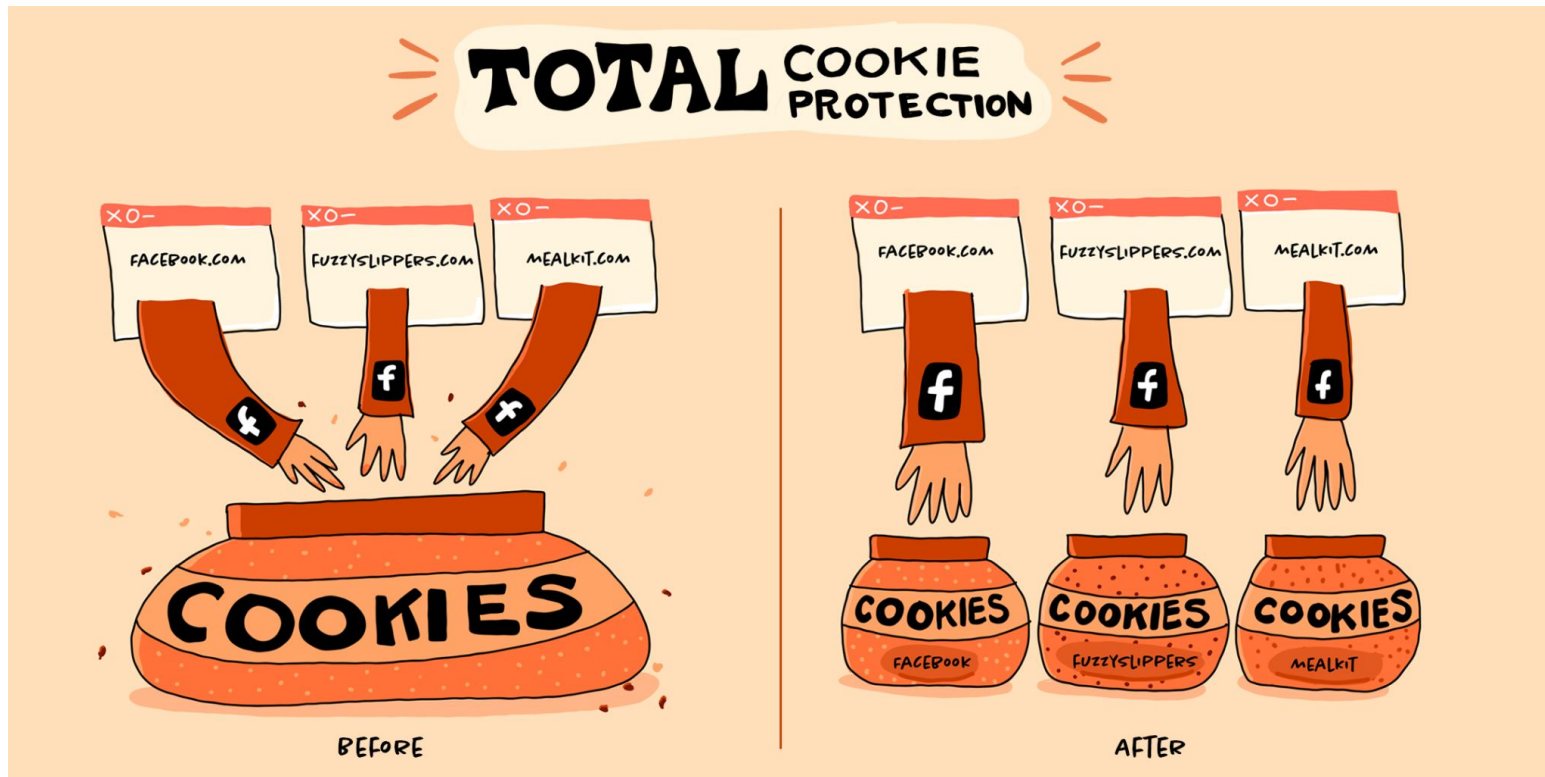


# Kinds of browser privacy leaks currently tested

- Stateful tracking
- Navigational tracking
- HTTPS incompleteness
- Fingerprinting
- Tracking query parameters
- Tracking content (scripts, pixels)
- Tracking cookies
- Cross-session tracking (first-party, third-party)
- Miscellaneous

# State partitioning

Credit: Megan Newell, [Mozilla](#)



# State partitioning

## Desktop Browsers

(default settings)



### State Partitioning tests

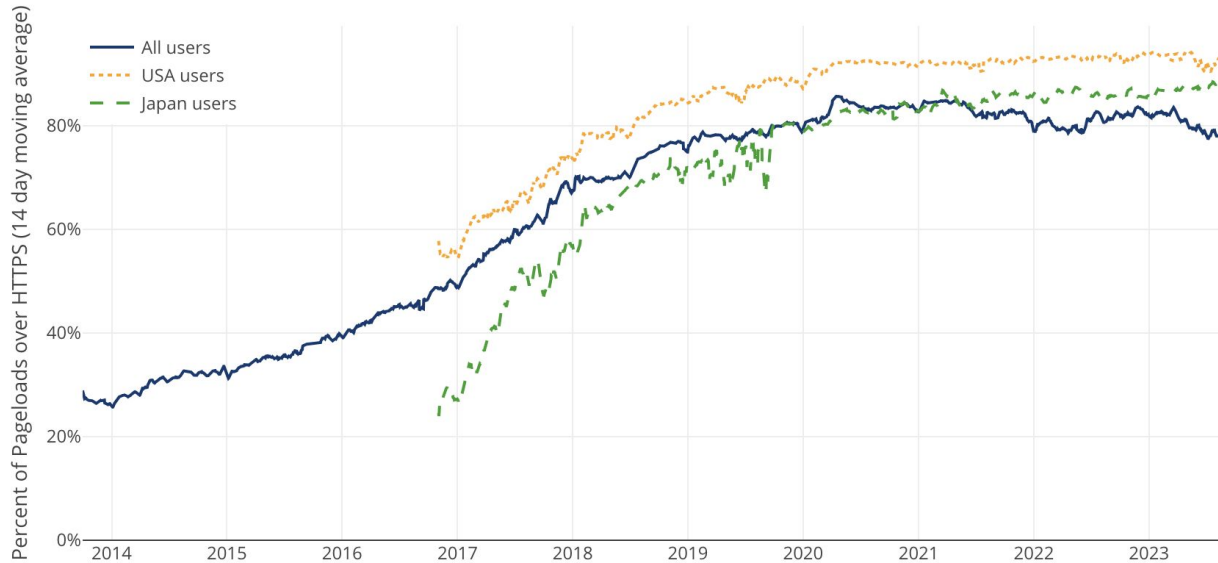
Which browsers isolate websites to prevent them from sharing data to track you?

	Brave 1.57	Chrome 116.0	Edge 116.0	Firefox 116.0	LibreWolf 116.0	Mullvad 12.5	Opera 101.0	Safari 16.6	Tor 12.5	Ungoogle 115.0	Vivaldi 6.1
Alt-Svc	✓	✓	✓	✓	✓	✓	✓	–	–	✓	✓
blob	✓	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗
BroadcastChannel	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗
CacheStorage	✓	✗	✗	✓	✓	–	✗	✓	–	✓	✗
cookie (HTTP)	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
cookie (JS)	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
CookieStore	✓	✗	✗	–	–	–	✗	–	–	✓	✗
CSS cache	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗
favicon cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
fetch cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
font cache	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗
getDirectory	✓	✗	✗	✓	✓	–	✗	–	–	✓	✗
H1 connection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
H2 connection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
H3 connection	✓	✓	✓	✓	✓	✓	✓	✓	–	✓	✓
HSTS cache	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗
iframe cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
image cache	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗
indexedDB	✓	✗	✗	✓	✓	–	✗	✓	–	✓	✗
localStorage	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
locks	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
prefetch cache	✓	✗	✗	✓	–	–	✗	–	–	✗	✗
ServiceWorker	✓	✓	✓	✓	✓	–	✓	✓	–	✓	✓
SharedWorker	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
TLS Session ID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web SQL Database	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
XMLHttpRequest cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

# HTTPS usage

## Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: [Firefox Telemetry](#))



# HTTPS usage

## Desktop Browsers

(default settings)



Brave  
1.57



Chrome  
116.0



Edge  
116.0



Firefox  
117.0



Librewolf  
117.0-1



Mullvad  
12.5



Opera  
101.0



Safari  
16.6



Tor  
12.5



Ungoogled  
115.0



Vivaldi  
6.2

## HTTPS tests

Which browsers use encrypted network connections whenever possible?

Insecure website	×	×	×	×	✓	✓	×	×	✓	×	×
Upgradable address	✓	×	×	×	✓	✓	×	×	✓	×	×
Upgradable hyperlink	✓	×	×	×	✓	✓	×	×	✓	×	×
Upgradable image	✓	✓	✓	×	✓	✓	✓	×	✓	✓	✓
Upgradable script	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

# Tracking cookies and tracking content

The screenshot shows the Whotracks.me website interface. At the top, there is a navigation bar with the site logo, a search bar, and links for Trackers, Websites, Blog, and Explorer. Below the navigation bar, the main content area displays the 'Trackers Rank' section, which lists the top 869 most prevalent trackers on the web. The list is sorted by Popularity. The top five trackers are:

1. Google Tag Manager (Google, Essential): 39.9% of web traffic is tracked by Google Tag Manager
2. Google Static (Google, Cdn): 39.1% of web traffic is tracked by Google Static
3. Google (Google, Advertising): 27.3% of web traffic is tracked by Google
4. Google Analytics (Google, Site Analytics): 25.9% of web traffic is tracked by Google Analytics
5. DoubleClick (Google, Advertising): 25.6% of web traffic is tracked by DoubleClick

Summary statistics for trackers are displayed in a purple-bordered box:

- 33.6% Trackers using cookies.
- 0.1% Trackers using fingerprinting.
- 1.6MB average data usage by trackers

[whotracks.me](https://whotracks.me)



# Tracking content and tracking cookies

## Desktop Browsers

(default settings)



### Tracker content blocking tests

Which browsers block important known tracking scripts and pixels?

	Brave 1.57	Chrome 116.0	Edge 116.0	Firefox 117.0	LibreWolf 117.0-1	Mullvad 12.5	Opera 101.0	Safari 16.6	Tor 12.5	Ungogged 115.0	Vivaldi 6.2
Adobe	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Adobe Audience Manager	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Amazon adsystem	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
AppNexus	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Bing Ads	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Chartbeat	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Criteo	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
DoubleClick (Google)	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Facebook tracking	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Google (third-party ad pixel)	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Google Analytics	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Google Tag Manager	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Index Exchange	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
New Relic	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Quantcast	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Scorecard Research Beacon	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Taboola	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Twitter pixel	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Yandex Ads	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗

## Desktop Browsers

(default settings)



### Tracking cookie protection tests

Which browsers block important known tracking cookies?

	Brave 1.57	Chrome 116.0	Edge 116.0	Firefox 117.0	LibreWolf 117.0-1	Mullvad 12.5	Opera 101.0	Safari 16.6	Tor 12.5	Ungogged 115.0	Vivaldi 6.2
Adobe	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
Adobe Audience Manager	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
Amazon adsystem	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
AppNexus	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
Bing Ads	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
Chartbeat	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
Criteo	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
DoubleClick (Google)	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
Facebook tracking	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
Google (third-party ad pixel)	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
Google Analytics	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
Google Tag Manager	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
Index Exchange	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
New Relic	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
Quantcast	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
Scorecard Research Beacon	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
Taboola	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
Twitter pixel	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
Yandex Ads	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗

# Tracking query parameters

[https://www.vrbo.com/travel/staycation?utm\\_campaign=vrbo:prog:usa-en:t:g:xxx:iroas&utm\\_medium=display&utm\\_source=dbm&utm\\_content=a:ban:dbm:xxx:pro:xxx:lake:xxx&utm\\_term=20193083|252013460|133520644|448385033&dclid=CNrN5PDpm\\_YCFRQTfQodiRAJuA](https://www.vrbo.com/travel/staycation?utm_campaign=vrbo:prog:usa-en:t:g:xxx:iroas&utm_medium=display&utm_source=dbm&utm_content=a:ban:dbm:xxx:pro:xxx:lake:xxx&utm_term=20193083|252013460|133520644|448385033&dclid=CNrN5PDpm_YCFRQTfQodiRAJuA)



Google "DoubleClick" ID

# Tracking query parameters

## Desktop Browsers

(default settings)



Brave  
1.57



Chrome  
116.0



Edge  
116.0



Firefox  
117.0



Librewolf  
117.0-1



Mullvad  
12.5



Opera  
101.0



Safari  
16.6



Tor  
12.5



Ungoogled  
115.0



Vivaldi  
6.2

## Tracking query parameter tests

Which browsers remove URL parameters that can track you?

__hsfp	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
__hssc	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
__hstc	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
__s	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗
__hsenc	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
__openstat	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
dclid	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
fbclid	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
gclid	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
hsCtaTracking	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
mc_eid	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
mkt_tok	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
ml_subscriber	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
ml_subscriber_hash	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
msclkid	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
oly_anon_id	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
oly_enc_id	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
rb_clickid	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
s_cid	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
vero_conv	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
vero_id	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
wickedid	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
yclid	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗

# Notable browser updates since October 2021

December 2021	Brave <a href="#">partitions network state</a>
August 2022	DuckDuckGo mobile <a href="#">blocks</a> Bing trackers
July 2022	Tor Browser <a href="#">introduces</a> HTTPS-Only Mode by default
Fall of 2022	Firefox <a href="#">ships</a> Total Cookie Protection (full partitioning) by default
Spring 2023	Chrome rolls out network state partitioning <a href="#">by default</a> and other Chromium-based browsers follow
June 2023	Brave <a href="#">ships</a> HTTPS by Default
June 2023	Safari 17 <a href="#">blocks</a> tracking query parameter links in Private Browsing
August 2023	<a href="#">Firefox</a> and <a href="#">Safari</a> partition Blob URL API
Late 2023	Chrome <a href="#">rolling out</a> third-party storage partitioning

# What have we learned so far?

- All 3 browser engines (Chromium, WebKit, Gecko) have already been substantially hardened for privacy in some browsers
- Nearly all browser engineering teams are interested in testing results and want to fix privacy leaks
- Lots of users are very interested in browser privacy!



# Future work ideas

- More network leak tests (e.g. DoH, OCSP)
- More fingerprinting tests
- Telemetry tests
- Disk forensic tests
- “Privacy Sandbox” and other attribution APIs
- More browsers
- Browser Extensions

# Acknowledgments

Ryan Brown

Steven Englehardt

Aleksey Khoroshilov

Simon Mainey

Jasper Rebane

Shivan Kaul Sahib

Sukhbir Singh

Peter Snyder

John Wilander

– Many people on Github and Twitter

# Thank you!

Reach me at:

[contact@privacytests.org](mailto:contact@privacytests.org)

[@privacytests](https://twitter.com/privacytests) (Twitter)

<https://mastodon.social/@privacytests>

<https://github.com/privacytests/privacytests.org>