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

WSJ, 2023-06-12

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

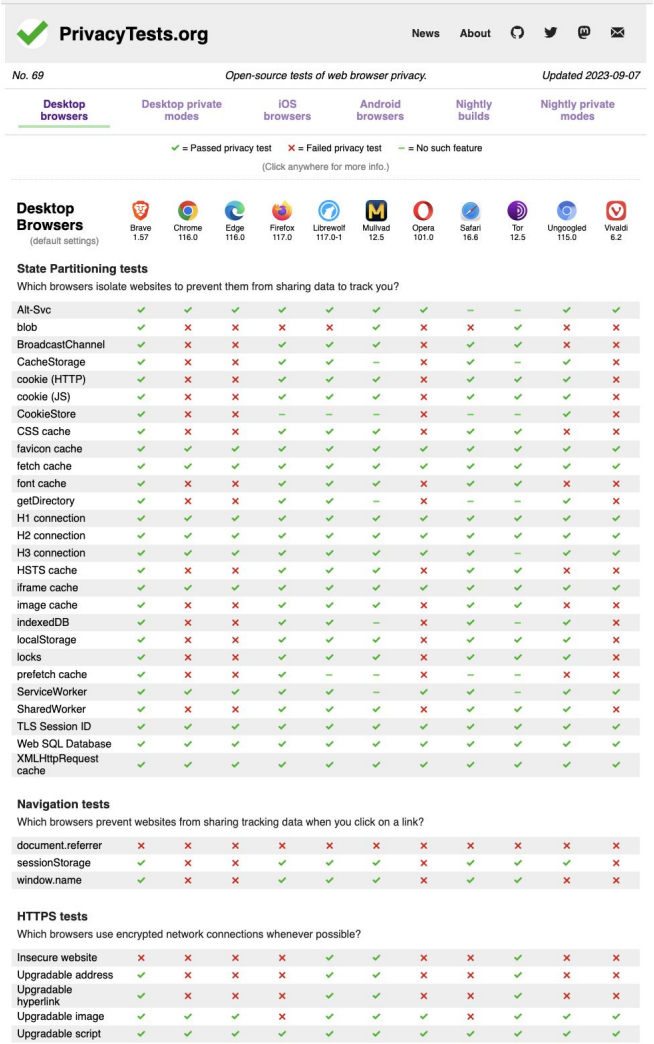
Building PrivacyTests.org

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!



PrivacyTests.org

News About

No. 69 — Open-source tests of web browser privacy. — Updated 2023-09-07

Desktop browsers | Desktop private modes | iOS browsers | Android browsers | Nightly builds | Nightly private modes

✓ = Passed privacy test ✗ = Failed privacy test – = No such feature

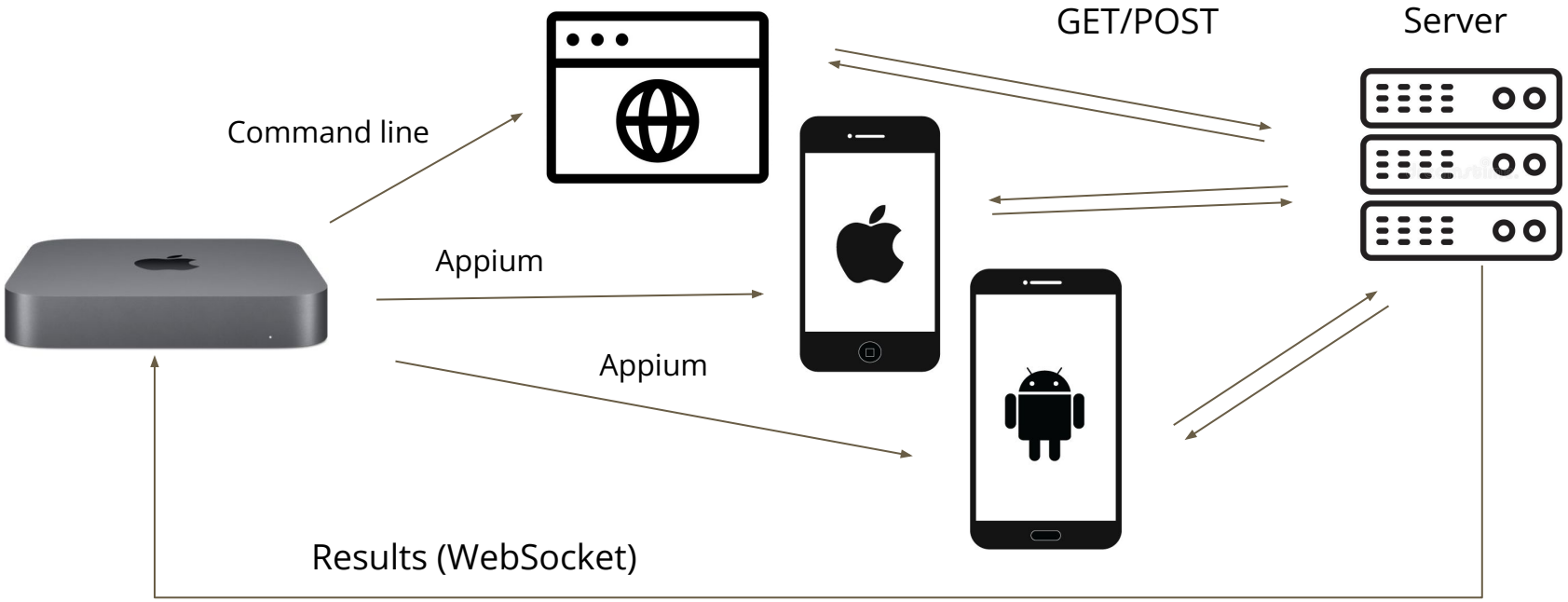
(Click anywhere for more info.)

Desktop Browsers (default settings)

	Brave 1.57	Chrome 116.0	Edge 116.0	Firefox 117.0	Librewolf 117.0-1	Mullvad 12.5	Opera 101.0	Safari 16.6	Tor 12.5	Ungoogled 115.0	Vivaldi 6.2
State Partitioning tests											
Which browsers isolate websites to prevent them from sharing data to track you?											
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	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Navigation tests											
Which browsers prevent websites from sharing tracking data when you click on a link?											
document.referrer	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
sessionStorage	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
window.name	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗
HTTPS tests											
Which browsers use encrypted network connections whenever possible?											
Insecure website	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
Upgradable address	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
Upgradable hyperlink	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
Upgradable image	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓
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

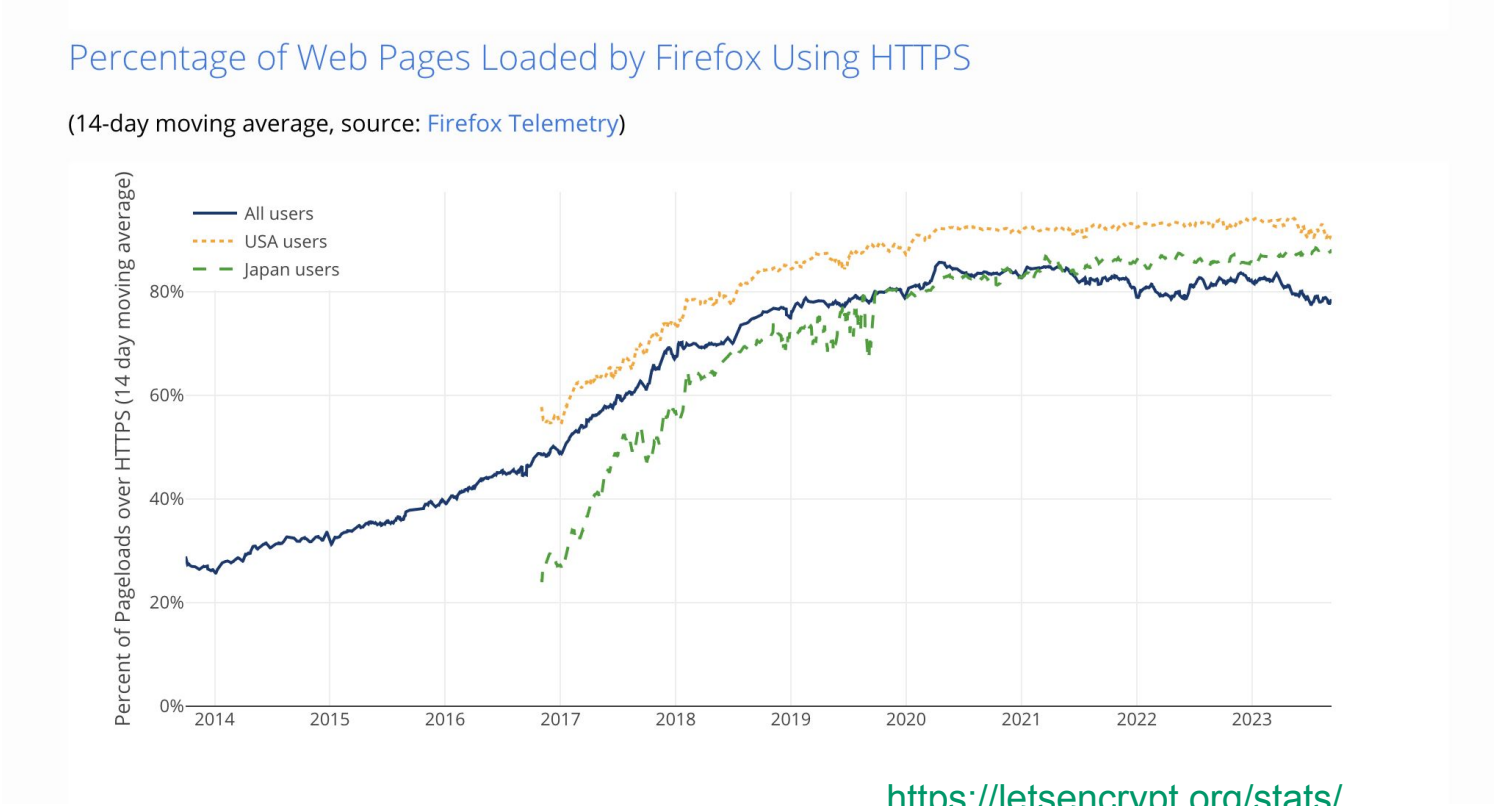
Desktop Browsers
(default settings)

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	Ungoogled 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



https://letsencrypt.org/stats/

HTTPS usage

Desktop Browsers
(default settings)

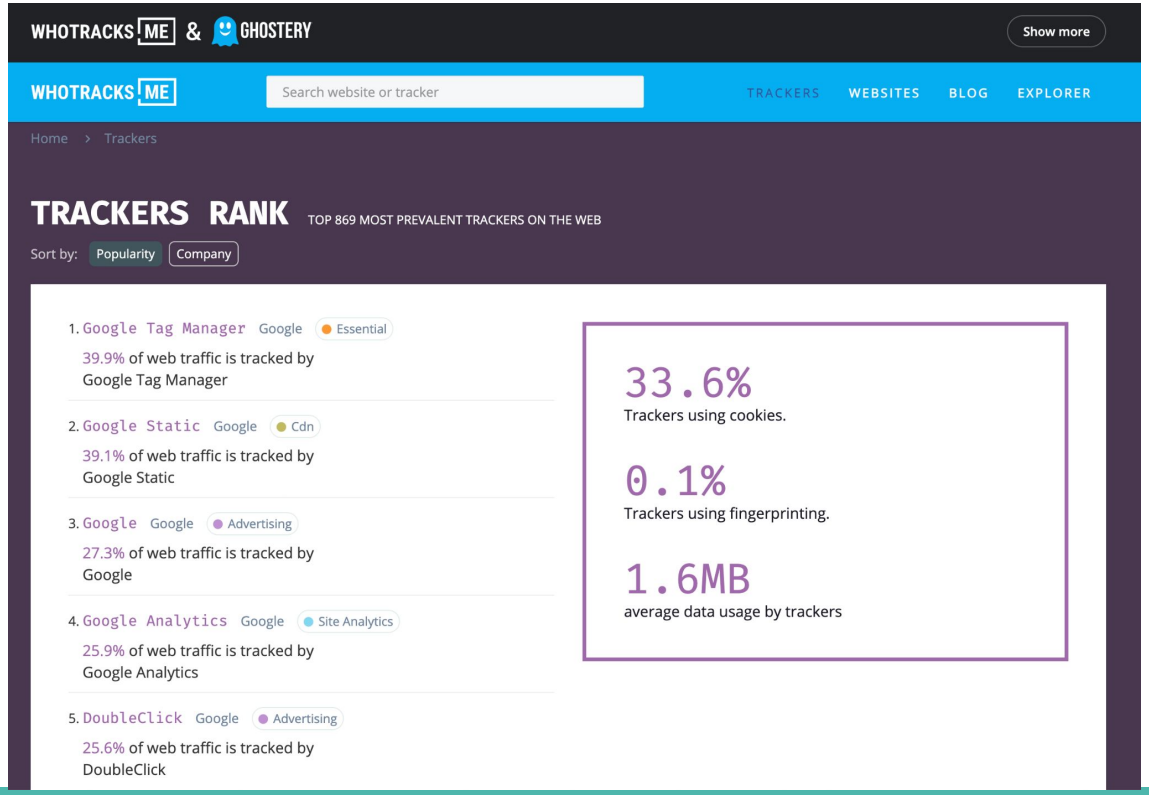
Brave 1.57	Chrome 116.0	Edge 116.0	Firefox 117.0	Librewolf 117.0-1	Mullvad 12.5	Opera 101.0	Safari 16.6	Tor 12.5	Ungoogled 115.0	Vivaldi 6.2

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



whotracks.me

Tracking content and tracking cookies

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
Tracker content blocking tests											
Which browsers block important known tracking scripts and pixels?											
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)

	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 cookie protection tests											
Which browsers block important known tracking cookies?											
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

Google “DoubleClick” ID

Tracking query parameters

Desktop Browsers
(default settings)

Tracking query parameter tests

Which browsers remove URL parameters that can track you?

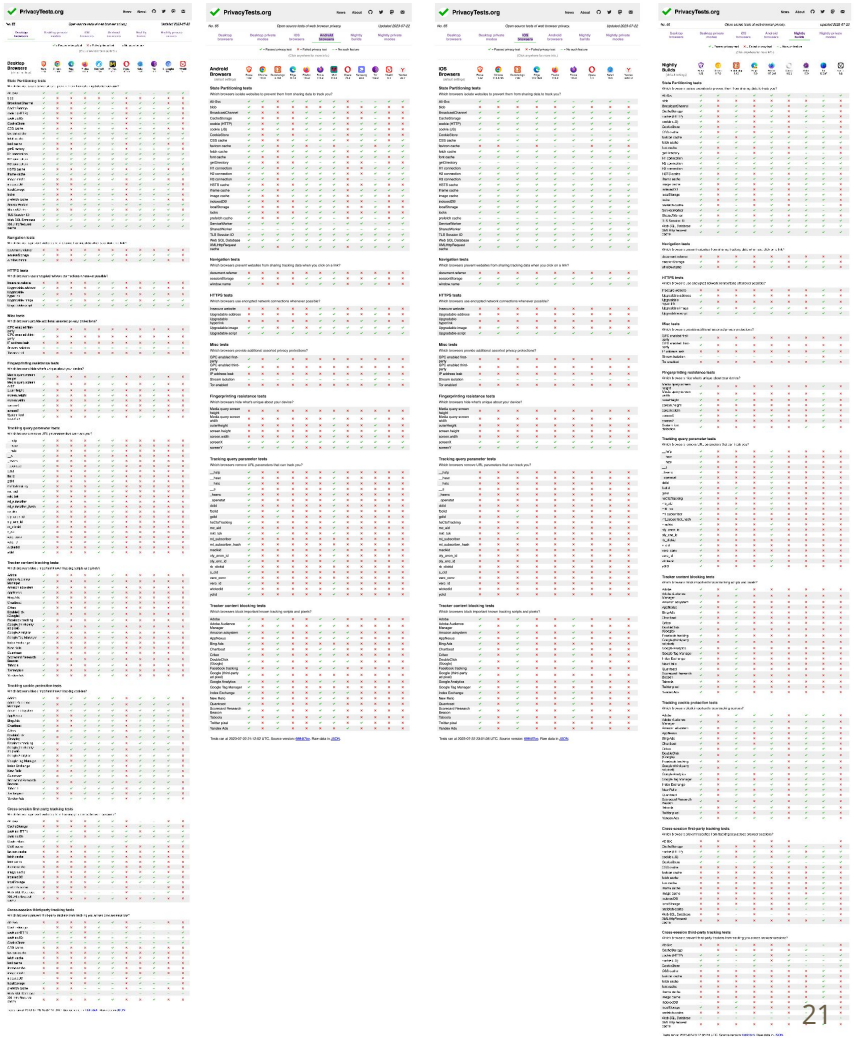
	Brave 1.57	Chrome 116.0	Edge 116.0	Firefox 117.0	Librewolf 117.0-1	Mullvad 12.5	Opera 101.0	Safari 16.6	Tor 12.5	Ungoogled 115.0	Vivaldi 6.2
__hsfp	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
__hssc	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
__hstc	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
__s	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗
_hsenc	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
_openstat	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
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 partitions network state
August 2022	DuckDuckGo mobile blocks Bing trackers
July 2022	Tor Browser introduces HTTPS-Only Mode by default
Fall of 2022	Firefox ships Total Cookie Protection (full partitioning) by default
Spring 2023	Chrome rolls out network state partitioning by default and other Chromium-based browsers follow
June 2023	Brave ships HTTPS by Default
June 2023	Safari 17 blocks tracking query parameter links in Private Browsing
August 2023	Firefox and Safari partition Blob URL API
Late 2023	Chrome rolling out 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

@privacytests (Twitter)

https://mastodon.social/@privacytests

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