PrivacyTests.org

Open source tests of web browser privacy

Arthur Edelstein, July 28, 2023

PEARG

In this talk

- My past work on browser privacy
- The high-level approach to PrivacyTests.org
- Overview of specific privacy tests and results
- Notable recent browser privacy progress
- What I have learned
- Future work
- Questions!

My background

Developer for Tor Browser (2014-2018)

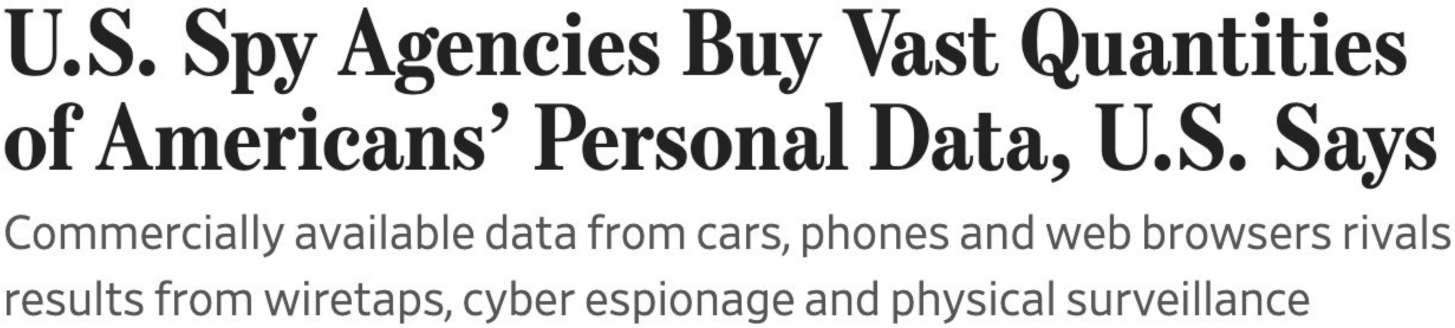
Product Manager for Firefox Privacy and Security (2018-2021)

PrivacyTests.org (2021-Present)

Research and Privacy Engineer at Brave (2022-Present)

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 governments and corporations



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 leak a lot of unnecessary data that can be used to track users
- Browsers fail to encrypt your network connections, allowing your ISP or other network eavesdroppers to watch your browsing

Why are browsers (still) leaky? Opacity, bad incentives

- Web browser privacy leaks are hidden, technical, and complex: meaning they are largely invisible to the public and, even invisible to engineers and managers in browser companies
- Privacy has not been a priority for most browsers, but marketing rhetoric has often given people a false or exaggerated sense that they are being protected
- Some major web browsers get their revenue from top trackers (Google, Bing), not from users

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
- Informing the public
- Informing browser makers
- Facilitating competition over privacy

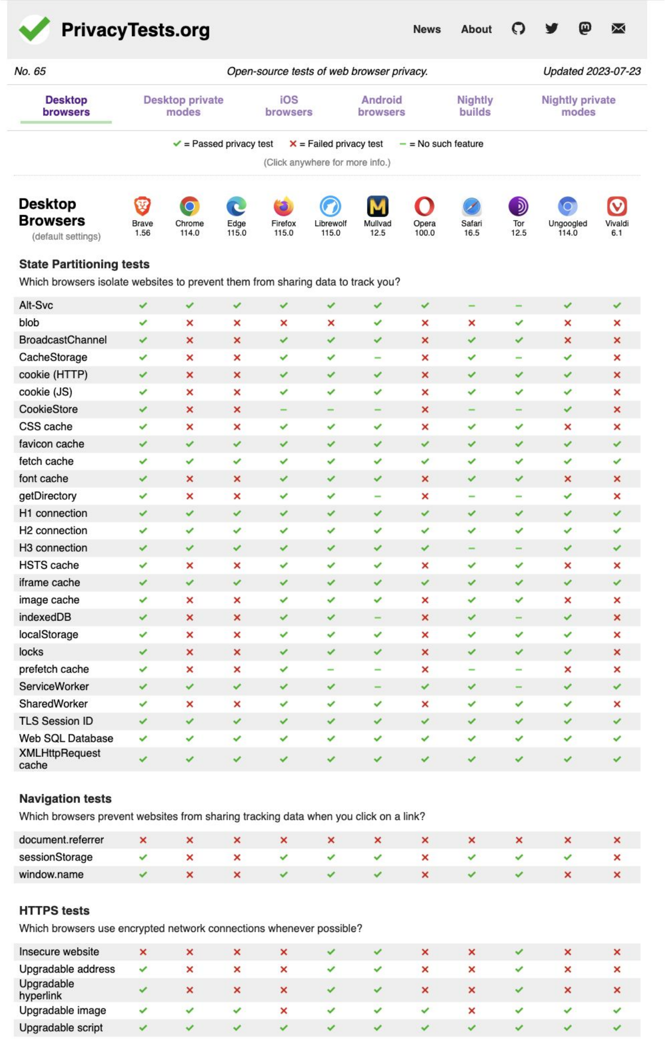
Building PrivacyTests.org

Proposed it at Tor 2018, and started (slowly) putting some tests together

Started working on it independently full time in August 2021

First launched in mid-October 2021; Android and iOS in December

Iterative – it remains a work in progress!



PrivacyTests.org

No. 65 *Open-source tests of web browser privacy.* Updated 2023-07-23

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

(Click anywhere for more info.)

Desktop Browsers (default settings)	Brave 1.56	Chrome 114.0	Edge 115.0	Firefox 115.0	Librewolf 115.0	Mullvad 12.5	Opera 100.0	Safari 16.5	Tor 12.5	Ungoogled 114.0	Vivaldi 6.1

State Partitioning tests

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

	Brave	Chrome	Edge	Firefox	Librewolf	Mullvad	Opera	Safari	Tor	Ungoogled	Vivaldi
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?

	Brave	Chrome	Edge	Firefox	Librewolf	Mullvad	Opera	Safari	Tor	Ungoogled	Vivaldi
document.referrer	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
sessionStorage	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗
window.name	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✗

HTTPS tests

Which browsers use encrypted network connections whenever possible?

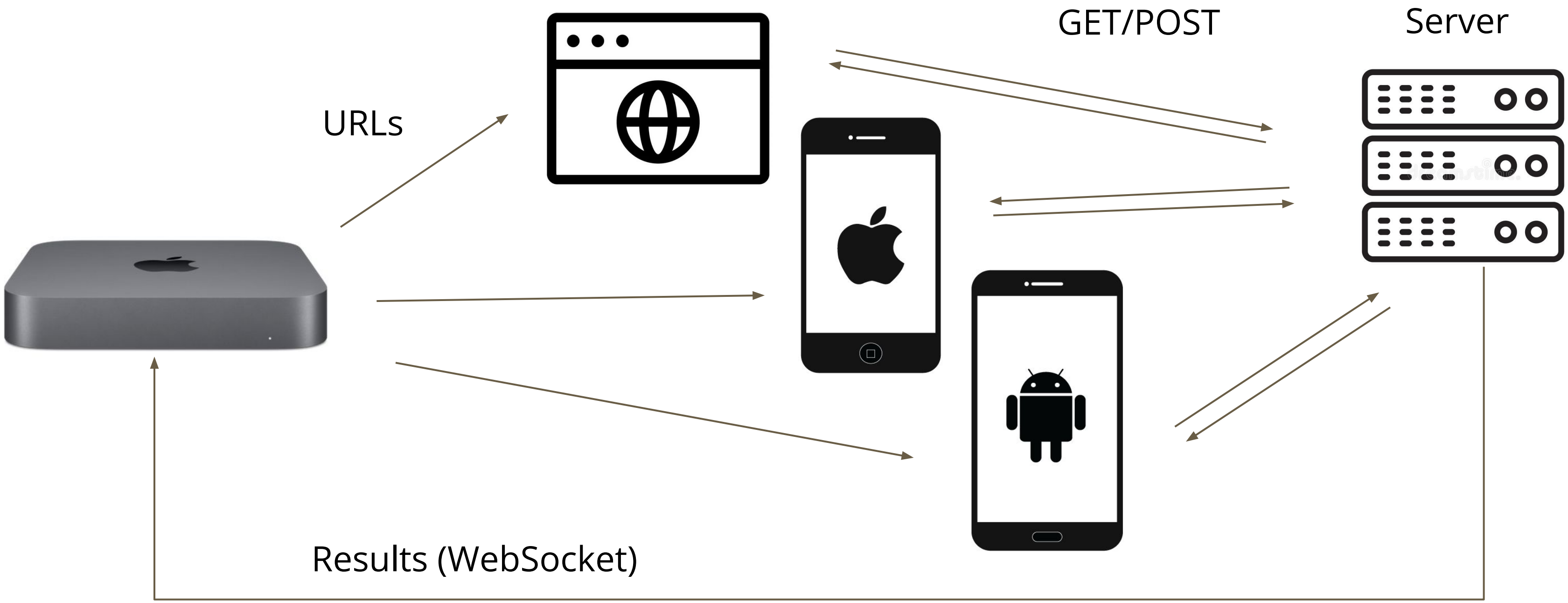
	Brave	Chrome	Edge	Firefox	Librewolf	Mullvad	Opera	Safari	Tor	Ungoogled	Vivaldi
Insecure website	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
Upgradable address	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
Upgradable hyperlink	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
Upgradable image	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓
Upgradable script	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Challenges and design

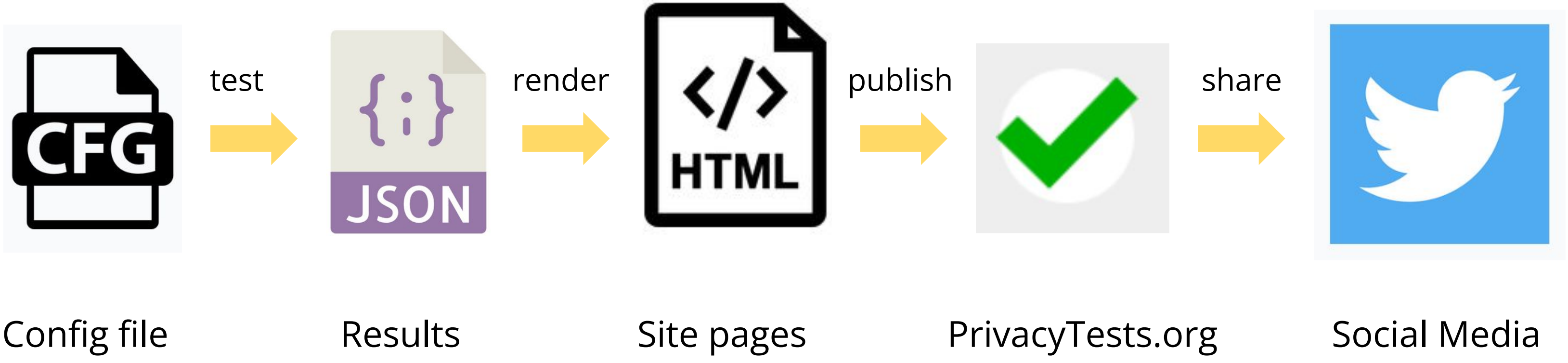
Browser privacy leaks have been unquantified and unknown to most people	Run objective automated tests and make results public
Browsers update ~1 month	Run and publish results every week
Results should be actionable	Show side-by-side comparison
Privacy leaks are too technical for most readers	Simplify results to pass/fail
Hard for readers to know who to trust	Make tests open source; stick to facts and make no recommendations
Many browser, and many privacy leaks	Launch early, continue to add tests and browsers

PrivacyTests.org browser testing framework

Almost all JavaScript (NodeJS and in-browser)



PrivacyTests.org data pipeline



test

render

publish

share

Config file

Results

Site pages

PrivacyTests.org

Social Media

PrivacyTests.org platform coverage

Platform	Device	Control	Browser windows
Desktop (MacOS)	Mac Mini	Browser command-line arguments	Regular, Private, Nightly, Nightly Private
Android	Samsung phone	Appium	Regular, Private
iOS	iPhone	Appium	Regular, Private

Kinds of browser privacy leaks currently tested

Stateful tracking (e.g. Cookies)

Navigational tracking (referrer, sessionStorage, window.name)

Miscellaneous (IP address, Tor, stream isolation, GPC)

Network leaks (HTTPS)

Fingerprinting (Fonts, screen size)

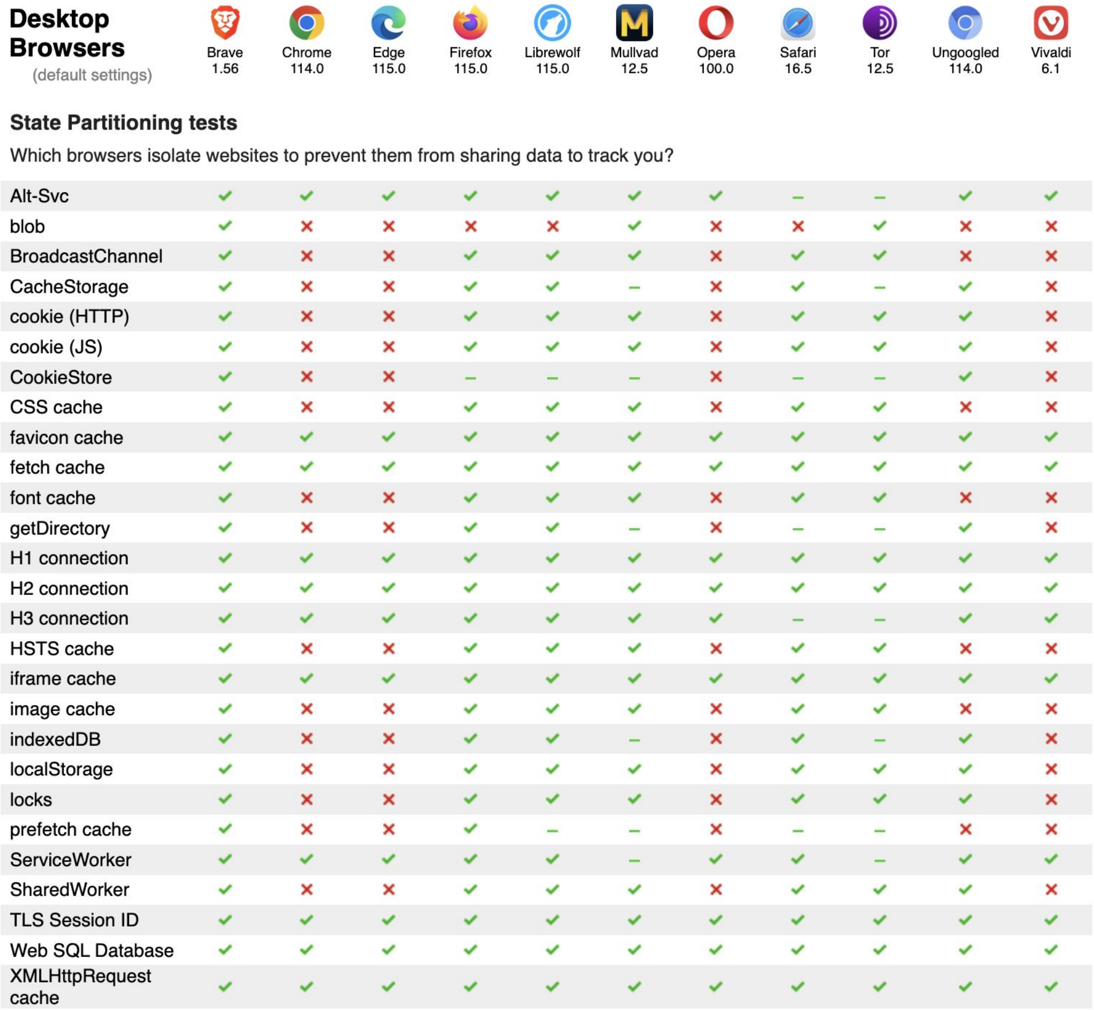
Tracking query Parameters

Tracking content (scripts, pixels)

Tracking cookies

Cross-session tracking (first-party, third-party)

State partitioning



Desktop Browsers (default settings)

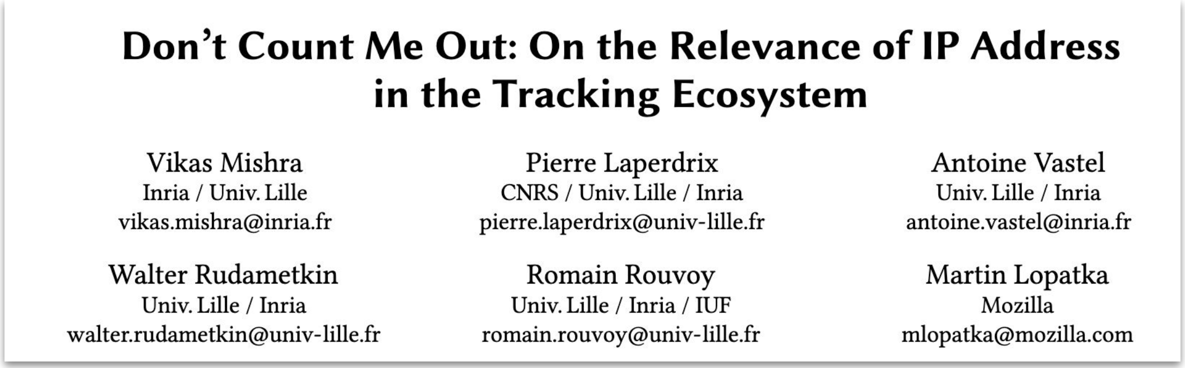
State Partitioning tests

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

	Brave 1.56	Chrome 114.0	Edge 115.0	Firefox 115.0	Librewolf 115.0	Mullvad 12.5	Opera 100.0	Safari 16.5	Tor 12.5	Ungoogled 114.0	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	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

IP Address tracking

IP addressed tracking is a big problem!



Don't Count Me Out: On the Relevance of IP Address in the Tracking Ecosystem

Vikas Mishra
Inria / Univ. Lille
vikas.mishra@inria.fr

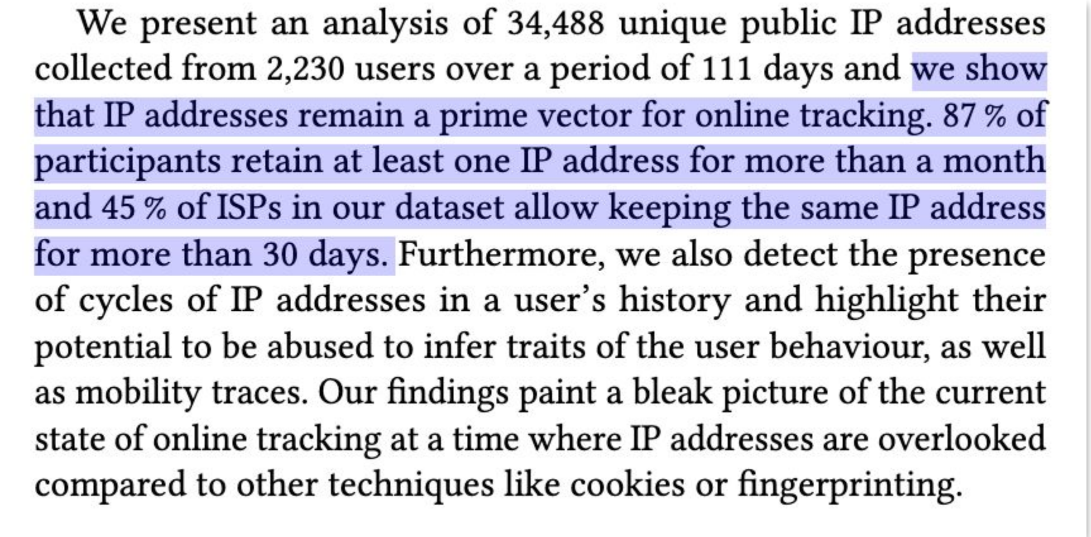
Pierre Laperdrix
CNRS / Univ. Lille / Inria
pierre.laperdrix@univ-lille.fr

Antoine Vastel
Univ. Lille / Inria
antoine.vastel@inria.fr

Walter Rudametkin
Univ. Lille / Inria
walter.rudametkin@univ-lille.fr

Romain Rouvoy
Univ. Lille / Inria / IUF
romain.rouvoy@univ-lille.fr

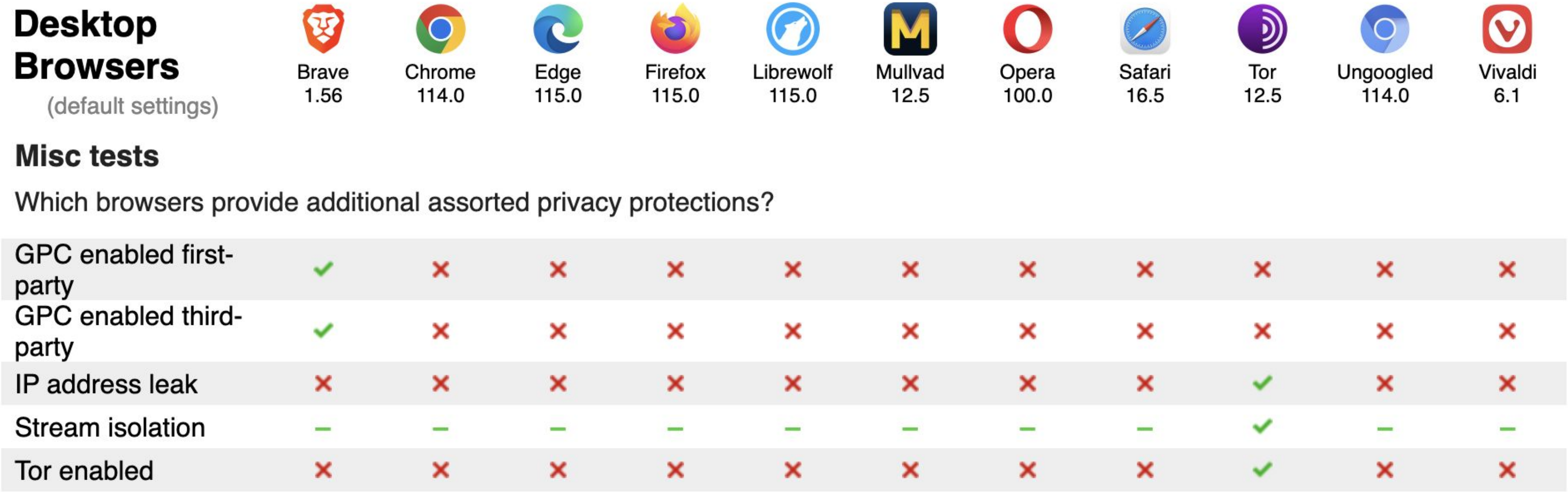
Martin Lopatka
Mozilla
mlopatka@mozilla.com



We present an analysis of 34,488 unique public IP addresses collected from 2,230 users over a period of 111 days and we show that IP addresses remain a prime vector for online tracking. 87 % of participants retain at least one IP address for more than a month and 45 % of ISPs in our dataset allow keeping the same IP address for more than 30 days. Furthermore, we also detect the presence of cycles of IP addresses in a user's history and highlight their potential to be abused to infer traits of the user behaviour, as well as mobility traces. Our findings paint a bleak picture of the current state of online tracking at a time where IP addresses are overlooked compared to other techniques like cookies or fingerprinting.

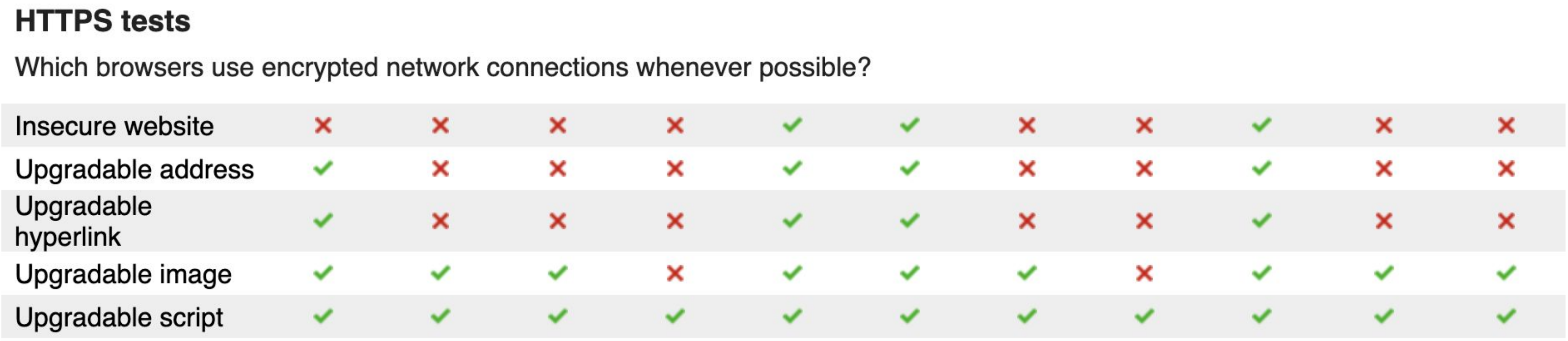
https://hal.inria.fr/hal-02435622/document

IP Address tracking



Desktop Browsers (default settings)	Brave 1.56	Chrome 114.0	Edge 115.0	Firefox 115.0	Librewolf 115.0	Mullvad 12.5	Opera 100.0	Safari 16.5	Tor 12.5	Ungoogled 114.0	Vivaldi 6.1
Misc tests											
Which browsers provide additional assorted privacy protections?											
GPC enabled first-party	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
GPC enabled third-party	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
IP address leak	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
Stream isolation	–	–	–	–	–	–	–	–	✓	–	–
Tor enabled	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗

HTTPS usage

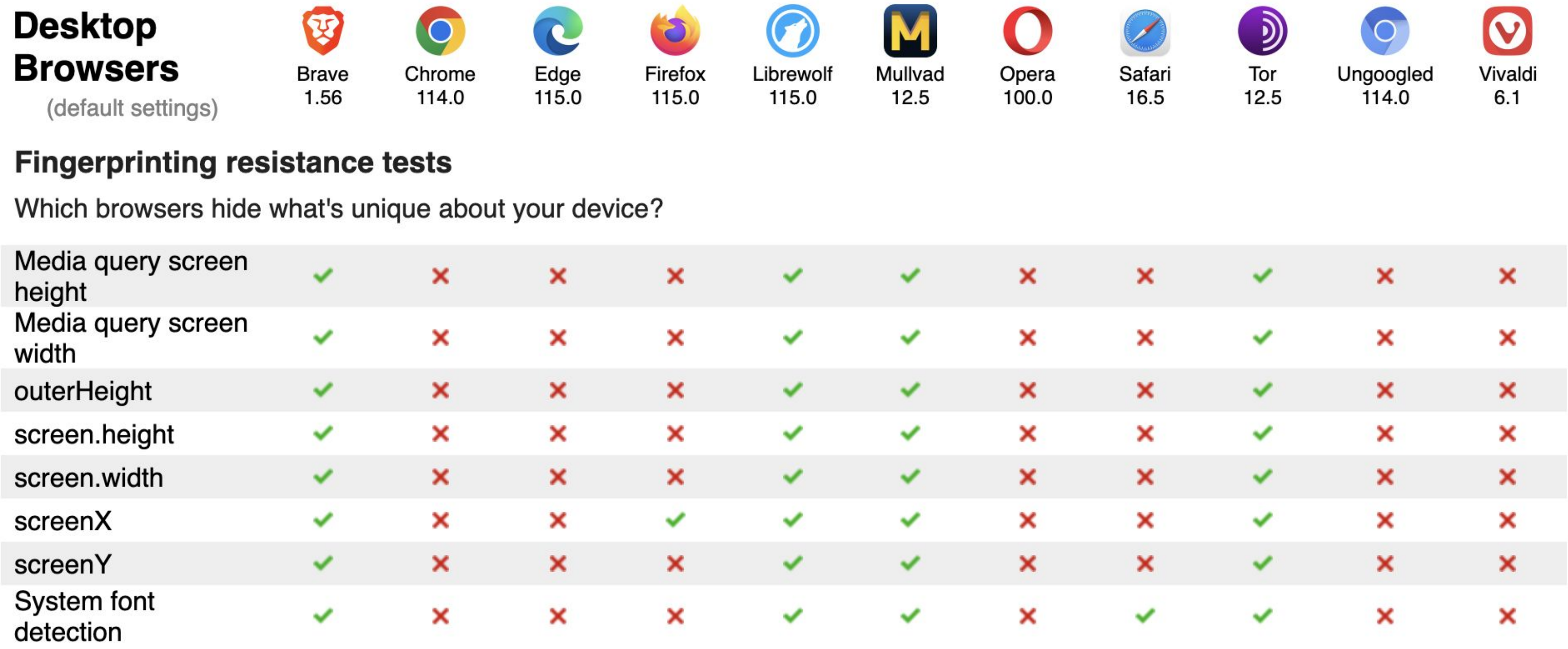


HTTPS tests

Which browsers use encrypted network connections whenever possible?

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

Fingerprinting



Desktop Browsers
(default settings)

Fingerprinting resistance tests

Which browsers hide what's unique about your device?

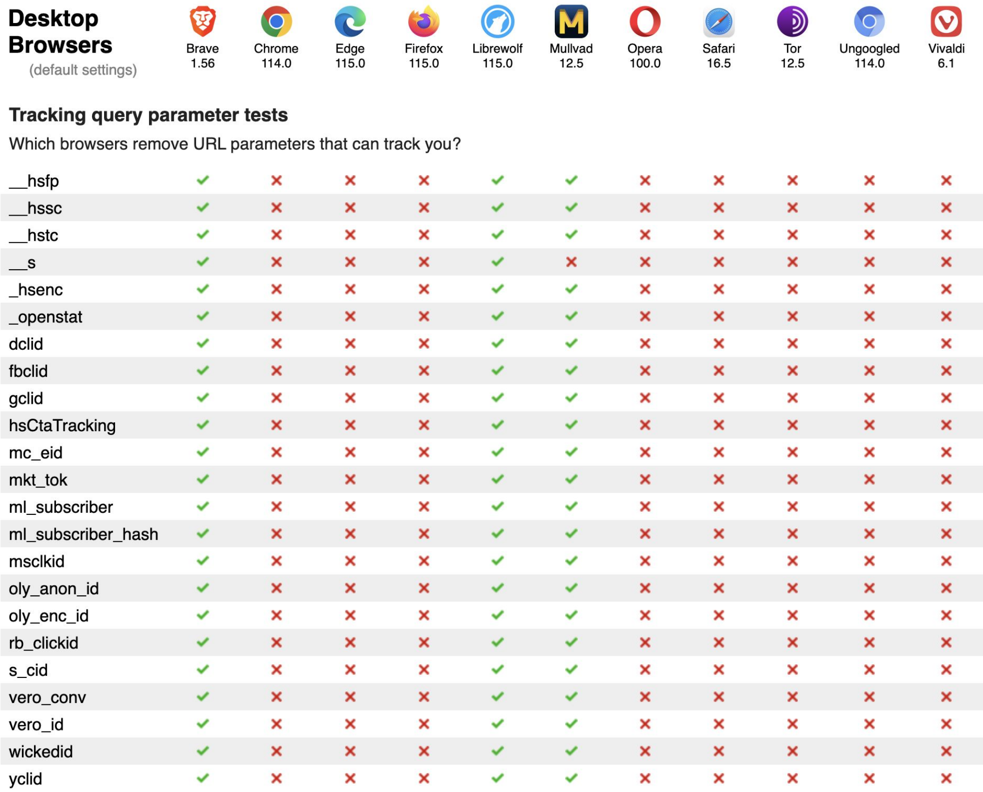
	Brave 1.56	Chrome 114.0	Edge 115.0	Firefox 115.0	Librewolf 115.0	Mullvad 12.5	Opera 100.0	Safari 16.5	Tor 12.5	Ungoogled 114.0	Vivaldi 6.1
Media query screen height	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
Media query screen width	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
outerHeight	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
screen.height	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
screen.width	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
screenX	✓	✗	✗	✓	✓	✓	✗	✗	✓	✗	✗
screenY	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
System font detection	✓	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗

Tracker query parameters (1)

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

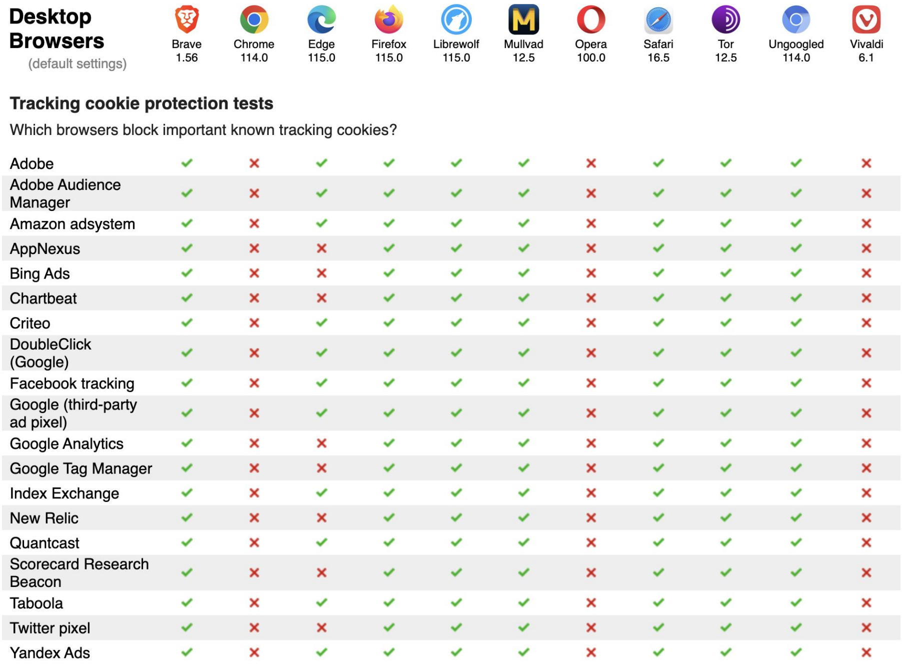
Google “DoubleClick” ID

Tracker query parameters (2)

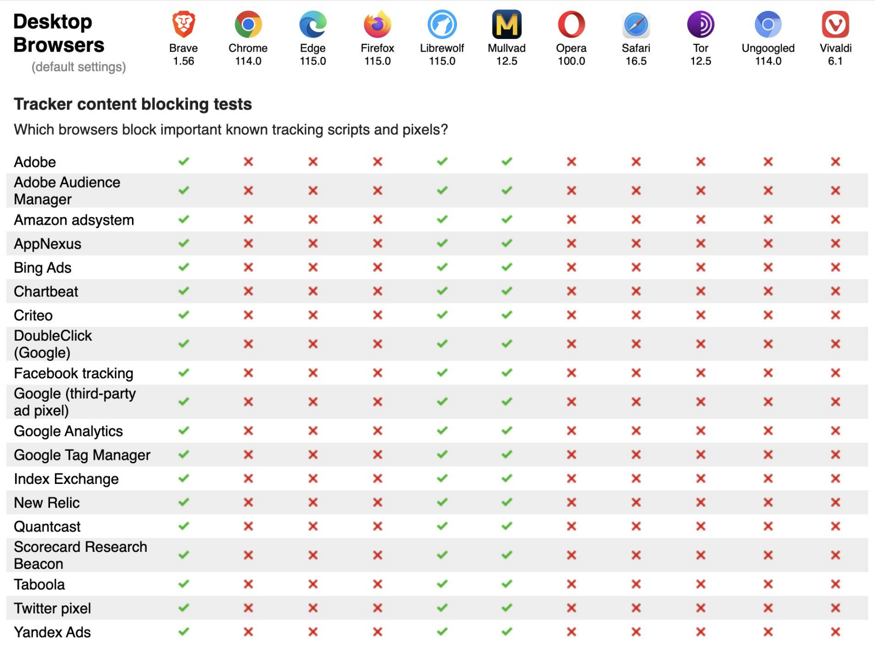


Desktop Browsers (default settings)	Brave 1.56	Chrome 114.0	Edge 115.0	Firefox 115.0	Librewolf 115.0	Mullvad 12.5	Opera 100.0	Safari 16.5	Tor 12.5	Ungoogled 114.0	Vivaldi 6.1
Tracking query parameter tests Which browsers remove URL parameters that can track you?											
__hsfp	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
__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	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗

Tracking cookies and tracking content

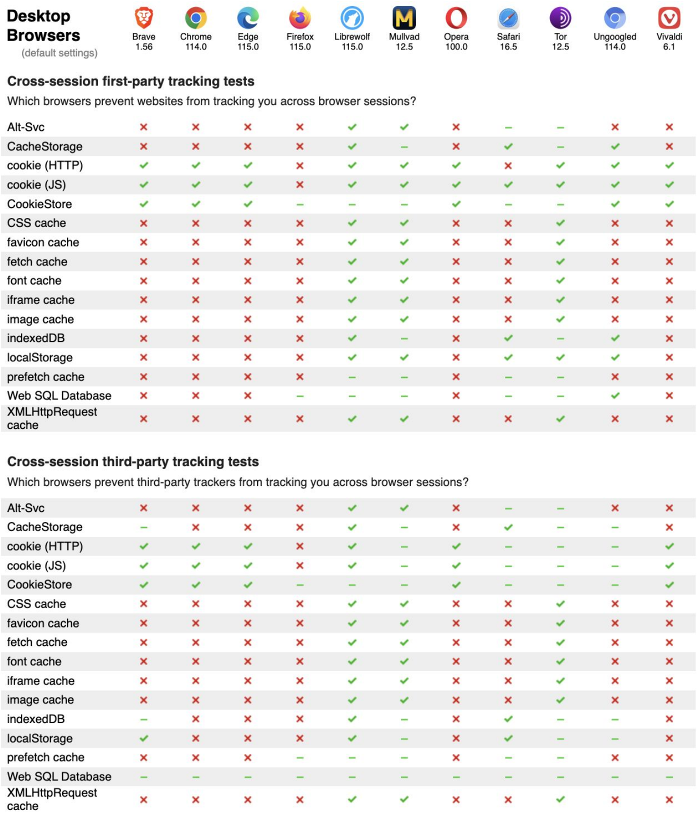


Desktop Browsers (default settings)	Brave 1.56	Chrome 114.0	Edge 115.0	Firefox 115.0	Librewolf 115.0	Mullvad 12.5	Opera 100.0	Safari 16.5	Tor 12.5	Ungoogled 114.0	Vivaldi 6.1
Tracking cookie protection tests Which browsers block important known tracking cookies?											
Adobe	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗
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	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✗



Desktop Browsers (default settings)	Brave 1.56	Chrome 114.0	Edge 115.0	Firefox 115.0	Librewolf 115.0	Mullvad 12.5	Opera 100.0	Safari 16.5	Tor 12.5	Ungoogled 114.0	Vivaldi 6.1
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	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗

Cross-session tracking



Desktop Browsers
(default settings)

Cross-session first-party tracking tests

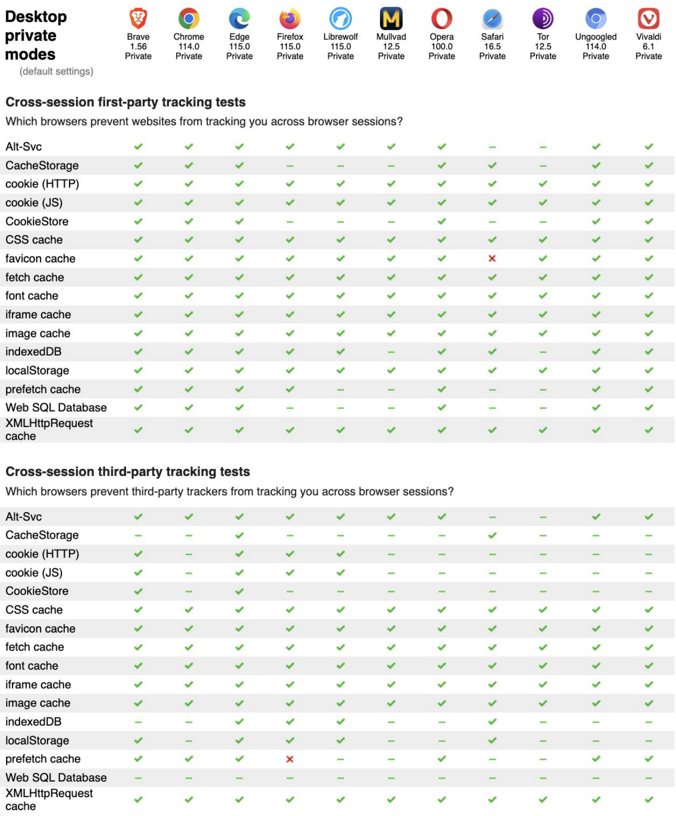
Which browsers prevent websites from tracking you across browser sessions?

	Brave 1.56	Chrome 114.0	Edge 115.0	Firefox 115.0	Librewolf 115.0	Mullvad 12.5	Opera 100.0	Safari 16.5	Tor 12.5	Ungoogled 114.0	Vivaldi 6.1
Alt-Svc	✗	✗	✗	✗	✓	✓	✗	–	–	✗	✗
CacheStorage	✗	✗	✗	✗	✓	–	✗	✓	–	✓	✗
cookie (HTTP)	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓
cookie (JS)	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
CookieStore	✓	✓	✓	–	–	–	✓	–	–	✓	✓
CSS cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
favicon cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
fetch cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
font cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
iframe cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
image cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
indexedDB	✗	✗	✗	✗	✓	–	✗	✓	–	✓	✗
localStorage	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✗
prefetch cache	✗	✗	✗	✗	–	–	✗	–	–	✗	✗
Web SQL Database	✗	✗	✗	–	–	–	✗	–	–	✓	✗
XMLHttpRequest cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗

Cross-session third-party tracking tests

Which browsers prevent third-party trackers from tracking you across browser sessions?

	Brave 1.56	Chrome 114.0	Edge 115.0	Firefox 115.0	Librewolf 115.0	Mullvad 12.5	Opera 100.0	Safari 16.5	Tor 12.5	Ungoogled 114.0	Vivaldi 6.1
Alt-Svc	✗	✗	✗	✗	✓	✓	✗	–	–	✗	✗
CacheStorage	–	✗	✗	✗	✓	–	✗	✓	–	–	✗
cookie (HTTP)	✓	✓	✓	✗	✓	–	✓	–	–	–	✓
cookie (JS)	✓	✓	✓	✗	✓	–	✓	–	–	–	✓
CookieStore	✓	✓	✓	–	–	–	✓	–	–	–	✓
CSS cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
favicon cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
fetch cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
font cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
iframe cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
image cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
indexedDB	–	✗	✗	✗	✓	–	✗	✓	–	–	✗
localStorage	✓	✗	✗	✗	✓	–	✗	✓	–	–	✗
prefetch cache	✗	✗	✗	–	–	–	✗	–	–	✗	✗
Web SQL Database	–	–	–	–	–	–	–	–	–	–	–
XMLHttpRequest cache	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗



Desktop private modes
(default settings)

Cross-session first-party tracking tests

Which browsers prevent websites from tracking you across browser sessions?

	Brave 1.56 Private	Chrome 114.0 Private	Edge 115.0 Private	Firefox 115.0 Private	Librewolf 115.0 Private	Mullvad 12.5 Private	Opera 100.0 Private	Safari 16.5 Private	Tor 12.5 Private	Ungoogled 114.0 Private	Vivaldi 6.1 Private
Alt-Svc	✓	✓	✓	✓	✓	✓	✓	–	–	✓	✓
CacheStorage	✓	✓	✓	–	–	–	✓	✓	–	✓	✓
cookie (HTTP)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
cookie (JS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CookieStore	✓	✓	✓	–	–	–	✓	–	–	✓	✓
CSS cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
favicon cache	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
fetch cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
font cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
iframe cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
image cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
indexedDB	✓	✓	✓	✓	✓	–	✓	✓	–	✓	✓
localStorage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
prefetch cache	✓	✓	✓	✓	–	–	✓	–	–	✓	✓
Web SQL Database	✓	✓	✓	–	–	–	✓	–	–	✓	✓
XMLHttpRequest cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Cross-session third-party tracking tests

Which browsers prevent third-party trackers from tracking you across browser sessions?

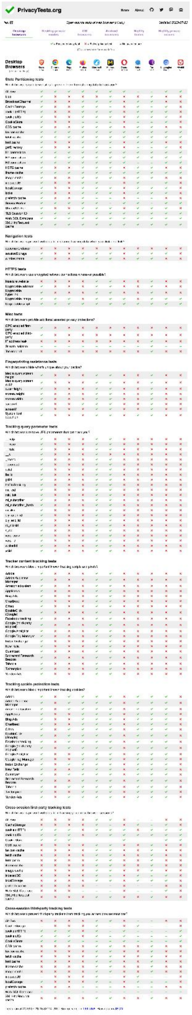
	Brave 1.56 Private	Chrome 114.0 Private	Edge 115.0 Private	Firefox 115.0 Private	Librewolf 115.0 Private	Mullvad 12.5 Private	Opera 100.0 Private	Safari 16.5 Private	Tor 12.5 Private	Ungoogled 114.0 Private	Vivaldi 6.1 Private
Alt-Svc	✓	✓	✓	✓	✓	✓	✓	–	–	✓	✓
CacheStorage	–	–	✓	–	–	–	–	✓	–	–	–
cookie (HTTP)	✓	–	✓	✓	✓	–	–	–	–	–	–
cookie (JS)	✓	–	✓	✓	✓	–	–	–	–	–	–
CookieStore	✓	–	✓	–	–	–	–	–	–	–	–
CSS cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
favicon cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
fetch cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
font cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
iframe cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
image cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
indexedDB	–	–	✓	✓	✓	–	–	✓	–	–	–
localStorage	✓	–	✓	✓	✓	–	–	✓	–	–	–
prefetch cache	✓	✓	✓	✗	–	–	✓	–	–	✓	✓
Web SQL Database	–	–	–	–	–	–	–	–	–	–	–
XMLHttpRequest cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Notable browser updates since October 2021

December 2021	Brave partitions network state
June 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

What have I learned so far?

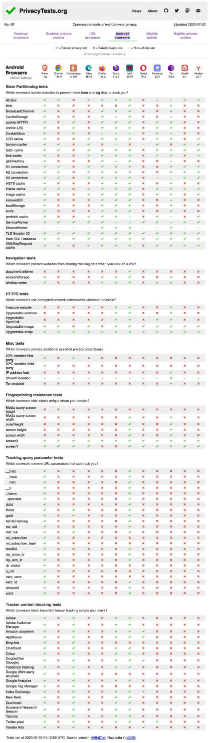
- All 3 browser engines (Chromium, WebKit, Gecko) have already been hardened for privacy in some browsers: no excuses!
- Nearly all browser engineering teams are interested in the results and want to fix privacy leaks
- Lots of users are very interested in browser privacy!



PrivacyTests.org

Desktop Browsers

State Partitioning tests



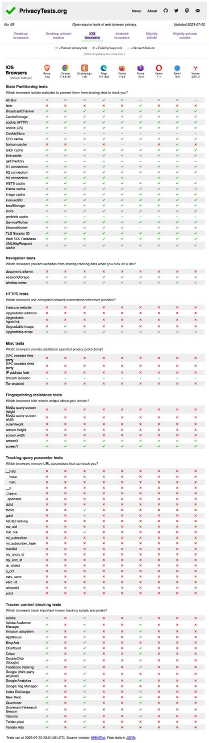
PrivacyTests.org

No. 65 Open-source tests of web browser privacy. Updated 2023-07-22

Android Browsers (default settings)

State Partitioning tests

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

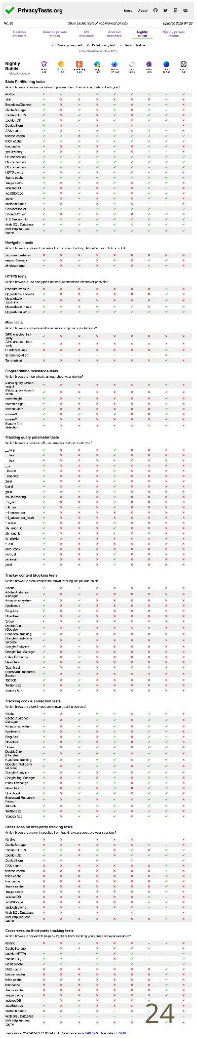


PrivacyTests.org

No. 65 Open-source tests of web browser privacy. Updated 2023-07-22

iOS Browsers (default settings)

State Partitioning tests



PrivacyTests.org

Nightly Builds

State Partitioning tests

Future work ideas

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

Acknowledgments

Shivan Kaul Sahib

Steven Englehardt

Aleksey Khoroshilov

Simon Mainey

Jasper Rebane

Sukhbir Singh

Peter Snyder

John Wilander

Many people on github and twitter

Thank you!

Reach me at:
contact@privacytests.org

@privacytests (Twitter)

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