

**Private Browsers:
ask us anything, then help us** 

The Tor Project

Tor&Mullvad Browser

- Firefox forks
- Shared patchset + specific patches
 - <https://gitlab.torproject.org/tpo/applications/tor-browser/-/commits/tor-browser-152.0a1-16.0-2>
- Privacy&security focused



Our guide: the design document

- <https://gitlab.torproject.org/tpo/applications/wiki/-/wikis/Design-Documents/Tor-Browser-Design-Doc>
- Requirements
- Philosophy
- Adversary model
- **No implementation details**



Always-on PBM

- Cross-session linkability
- Disk leaks
- Huge impact on usability
 - Okay for Tor Browser
 - Less for Mullvad Browser
- Permissions are also memory-only

Strict first-party isolation

- Everything is partitioned on eTLD + 1 whenever possible
- Even tor circuits are partitioned
- This breaks some sites
- Third-party cookies are disabled

Fingerprinting resistance

- We enable Firefox's resist fingerprinting mode
- Continuous collaboration for improving it

RFP: core ideas

- Prefer uniformity and actual behavior changes
- Randomize when uniformity is hard (e.g., canvases)
- Disabling is the last resort

RFP controls

- <https://searchfox.org/firefox-main/source/toolkit/components/resistfingerprinting/RFPTargets.inc>



Additions to RFP

- Bundled fonts
- Strictly controlled localization
- No translations
- No WebGL 2
- No WebGPU
- No HEVC

Data collection

- Data collection and remote services are disabled
 - No data, no responsibilities, no leaks
- Data-driven decision is almost impossible for us
 - Only opt-in surveys

Some pain points

- Keep up with upstream and the web platform
- Users need to do their part, but this needs education and documentation
- Balance between gate-keeping and user freedom
- Accessibility and fingerprinting protection?

Help us!

- Keep privacy into account when creating new standards
- Define baseline profiles for features
- Moonshot: standardize RFP?

Thanks for your attention!

Questions?