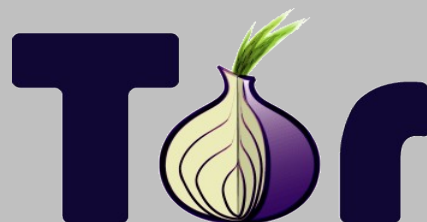


Do Not Beg: Moving Beyond Do Not Track with Privacy By Design

Mike Perry
W3C DNT
Nov 28, 2012



Do Not Track as Privacy By Design

The meat of the initial IETF DNT Draft:

“A server acting in a third-party capacity **MUST NOT** track a user or user agent...”

“Tracking includes collection, retention, and use of all data related to the request and response.”

Can be met through three areas of technical change:

- First Party Identifier Unlinkability
- First Party IP Address Unlinkability
- First Party Fingerprinting Unlinkability

Goal: First Party Top-Level Privacy UI



Identifier Unlinkability in Tor Browser

- Jail/silo identifier sources to first party domain
 - Cache is siloed similar to Stanford SafeCache
 - HTTP Auth is restricted to first party
 - Window.name is cleared on origin change
- Disable/Limit features we haven't yet siloed
 - Third Party Cookies currently disabled
 - DOM Storage, AppCache, IndexedDB, SPDY
 - SSL Session IDs and Tickets
 - HTTP-Keepalive limited to 20 seconds

Identifier Unlinkability: Remaining Work

- Silo disabled identifier sources to first party
 - “Double-key” (or hold-until-click) 3rd Party Cookies
 - DOM Storage, AppCache, IndexedDB
 - HTTP-Keepalive and SPDY connection usage
 - Disable HSTS for third parties in non-HSTS domains
- Prompt before automated cross-domain redirects
 - Obtain user consent to avoid covert 3rd party->first party promotion
- Utilize Tor path isolation for IP unlinkability
 - Set SOCKS username to first party domain
 - ISPs could provide such proxies too

Fingerprinting Defenses in Tor Browser

- Disable plugins
- Limit number of font probes per first party origin
- Report a fixed map of “System Colors” to CSS
- Report content window size for desktop and outer window resolutions
 - Limited set of initial window sizes
- Limit WebGL to click-to-play
- Prompt on read access of HTML5 Canvas data
- Report timezone as GMT
- Report OS as Windows

Fingerprinting Defenses: Remaining Work

- Improve resolution defenses
 - Maximization, toolbars cause problems
 - Prompt? Zoom?
- Reduce Javascript timing resolution
 - Keystroke, CPU fingerprinting
- Protocol handler enumeration
- Likely possible to infer OS several ways..
 - Fonts (provide font pack?), button shape?
- New HTML5 features need evaluation
 - May need to rely on simulations or intuition

Common Concerns

Link Sharing/Like Buttons?

- Web-send.org
 - Privacy preserving link sharing + federated login
 - Disappeared from Google Chrome?
- Safari/Priv3-style hold-until-click cookie policy

Federated Login?

- OAuth and OpenID still work per each first party
- Persona/BrowserID

Supporting the Long Tail

- Behavioral Targeting may support small publishers
- “Targeted, Not Tracked” discusses three client-side mechanisms to serve privacy-preserving targeted ads
 - Auditable and Universal
- More work is needed before Tor would deploy something like this...
 - Must be Open Source or will be perceived as spyware
 - But privacy doesn't mean the end of the free web

W3C Q&A Highlights

- Third Party Analytics Services?
 - Dual-Keyed cookies will allow this
- Click-Fraud/Abuse?
 - Link-click driven conversion is still trackable
 - Also, see “Nymble” and related research literature
 - Blinded tokens using scarce resource (Computation, SMS)
 - Tor currently lacks engineering resources to deploy
- How much will websites break?
 - Depends on engineering effort invested client-side
 - Per-site login for like buttons, but alternatives exist
(See Priv3 Firefox extn; or web-send.org)