SUMMARY COMPARISON OF UNIVERSAL OPT-OUT MECHANISMS FOR WEB TRACKING

Alissa Cooper / March 25, 2011

This table summarizes and builds upon "Overview of Universal Opt-Out Mechanisms for Web Tracking," an Internet draft recently submitted to the IETF, available at http://tools.ietf.org/html/draft-cooper-web-tracking-opt-outs-00. Consult the draft for a fuller discussion and comparison of web tracking opt-out mechanisms.

	Domain/request blocking	Do Not Track HTTP header	Do Not Track DOM property
Universality *Does it work across domains/apps/entities?*	Relies on extent to which domains/resources that conduct tracking are included on block lists	Can be sent with every HTTP request	Can be made accessible to all sites that access the DOM
Effectiveness *How well does it prevent tracking?*	Prevents tracking altogether from domains/resources on block lists	Relies on how tracking is defined and extent to which tracking entities honor the header May require enforcement or intervention from governmental privacy authorities	Relies on how tracking is defined and extent to which tracking entities honor the property May require enforcement or intervention from governmental privacy authorities
Comprehensiveness *Does it work for different tracking technologies?*	Applies to tracking via any mechanism that originates with a web server request (cookies, other HTTP headers, script-based techniques, etc.)	Can be defined to apply to tracking via any mechanism employed by HTTP servers	Can be defined to apply to tracking via any mechanism employed by client-side documents
Simplicity *How easy is it to use?*	Requires block list to be installed and kept up-to-date	Can be offered via simple binary choice with possibilities for more granular choices	Can be offered via simple binary choice Offering granular choices is more complicated because DOM is shared across domains
Continuity with web functionality *How does it impact existing web sites and applications?*	Prevents content delivery from domains used for both tracking and content serving Domain operators could seek to avoid being blocked by switching domains or requiring users to disable block lists to access content	Does not directly interfere with existing functionality Sites that detect the header may prevent users from accessing content or may request that users turn it off before access is granted	Does not directly interfere with existing functionality Scripts that detect the property may prevent users from accessing content or may request that users turn it off before access is granted
Standardization *What components could or should be standardized?*	Block list format and processing rules	Syntax, semantics and usage	Syntax, semantics and usage