mozilla

Position Paper: Do Not Track
W3C Workshop on Web Tracking and User Privacy, April 28-29, 2011
Prepared by Mozilla and Submitted on March 25, 2011

Mozilla supports a full range of innovations and industry practices that enhance consumer choice and control with regard to online behavioral advertising. This includes the creation of a uniform and comprehensive choice mechanism through a new Do Not Track (DNT) HTTP header as another step in a series of many privacy improvements. Continued leadership is required to develop consensus on the scope of DNT as it relates to online behavioral advertising and implementation across the online advertising industry. We are interested in participating in the upcoming W3C workshop to share our recent experience in implementing the DNT header in Firefox 4, how industry continues to rise to the occasion in crafting a response, as well as how we think the W3C efforts fit with our parallel submission to the IETF.

Do Not Track Mechanisms for Online Behavioral Advertising

Unlike blocking lists or opt-out cookies, which place the burden on the consumer and, more importantly, do not respond to all forms of OBA-related tracking and targeting, a DNT header has the potential for consumers to broadcast preferences for advertisers and publishers to honor while not undermining or blocking more widely-accepted and privacy-preserving forms of advertising. Success of the header approach will require support and collaboration from stakeholders across the web technology and display ad ecosystem.

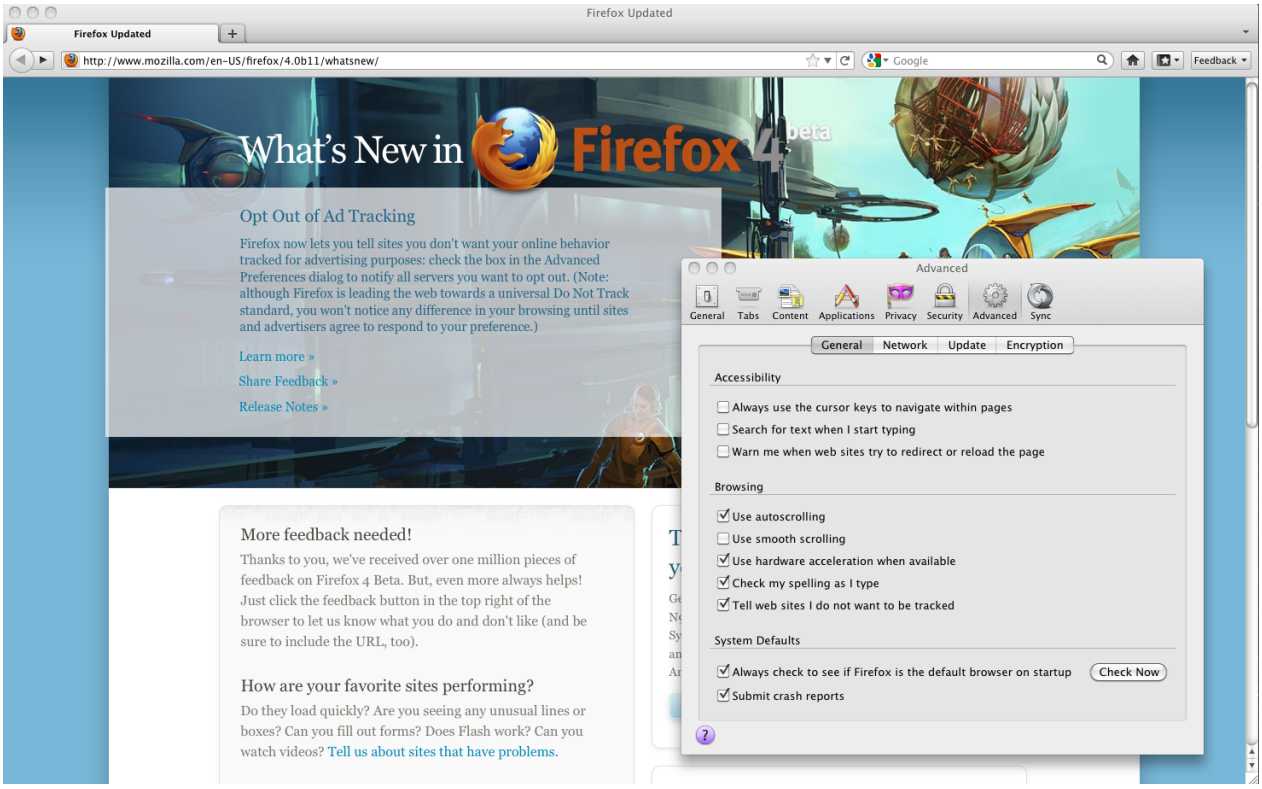
Since the release of the FTC's proposed framework, there has been considerable public and media attention given to the topic of online behavioral advertising (OBA) and the FTC's recommendation for the creation of a Do Not Track (DNT) mechanism. Mozilla recently added the new HTTP DNT header that Firefox users can use to state a preference to not be tracked across websites for advertising. This feature easily co-exists with other browser-based privacy and cookie-based tools already available to Firefox users today.[1,2,3]

The DNT header builds on the work of the advertising networks by re-framing the cookie-based systems they make available to people online. There are many advantages of the header technique over the cookie-based technique; it is less complex and simple to locate and use, it is more persistent than cookie-based solutions, it addresses all forms of OBA-based tracking that may not all be cookie-based, and it does not rely on consumers finding, loading and managing lists of ad networks and advertisers to work.

However, it is important to point out that browser implementation of the DNT header does not represent a complete solution, as industry participation is required to create the technical mechanisms to respond to DNT browser requests broadcast by consumers via their browsers.

[1] "More Choice and Control Over Online Tracking," Alexander Fowler; https://firstpersoncookie.wordpress.com/2011/01/23/more-choice-and-control-over-online-tracking/
[2] "Opting-out of Behavioral Ads;" Sid Stamm; http://blog.sidstamm.com/2011/01/opting-out-of-behavioral-ads.html
[3] "Thoughts on Do-Not-Track," Michael Hanson; http://www.open-mike.org/entry/thoughts-on-do-not-track

Screenshot: Firefox Welcome Page with Configuration Panel Open to Show DNT Header



Ad networks, advertisers and publishers are very supportive of the DNT header and see it as preferable to cookie-based or list blocking approaches. Consensus is emerging that a simple first step for responding to a consumer's intent could be: if the DNT header is present and the site or third-party advertiser has a tracking opt-out mechanism, then the mechanism should be activated. If the site or third-party advertiser does not have an explicit opt-out mechanism, the consumer should experience only content from a first-party relationship with the page being viewed. For behavioral advertising servers and data brokers, the intent of a DNT header is quite clear: it should be interpreted as though the consumer visited the opt-out registry and clicked the checkbox and that the consumer's activity or data is not collected or logged. We expect announcements to be forthcoming shortly on how first party and third party entities will be responding to the DNT header.

There are a number of steps ahead that will require continued leadership and support to see companies implement responses to consumers with the DNT header enabled, including:

- Fostering consensus on what the DNT header means to all stakeholders. We have proposed an initial definition focused on the display advertising market, and we seek a focused definition all stakeholders can agree upon.
- Helping to educate the public on DNT and what reasonable expectations of privacy people should have when using the DNT header or other mechanisms in a browser.
- Working with sites, advertisers and data brokers to establish best practices in implementing meaningful responses to a DNT header that are transparent to the public.
- Evaluating enforcement mechanisms to combat entities that systematically ignore the DNT header and jeopardize those efforts made by responsible companies.

Perspective on Working on DNT at the IETF and Tracking Protection Lists

On March 7, 2011 we jointly submitted a draft proposal with Jonathan Mayer and Arvind Narayanan of Stanford's Center for Internet and Society to the IETF. The proposal, entitled "Do Not Track: A Universal Third-Party Web Tracking Opt Out," is a first attempt to define the syntax and semantics of a HTTP header-based mechanism for DNT and it also provides a recommendation for how web services should respond to such a mechanism.

At roughly the same time, Microsoft submitted a Tracking Protection proposal to the W3C containing three parts: Tracking Protection Lists (TPLs), the DNT header, and a doNotTrack DOM element. While TPLs provide a meaningful consumer protection for privacy, we do not think they necessarily fit well with the DNT header or DOM element; the goals and effects of the technologies seem to be quite different. For instance, TPLs affect how clients interpret and access content, while DNT header and the DOM element ultimately affect what servers do to preserve privacy. Additionally, there is no reason to limit deployment of the DNT header to web browsers; all HTTP-based communication could potentially benefit from this signal whether from a browser, application, or embedded device. We are in favor of moving the DNT header to a separate working group, preferably with the IETF, and then create a subcommittee of the W3C working group on TPLs to tackle standardization of the DNT DOM solution.

We recognize that he W3C has considerable experience working on privacy-related standards; however, HTTP is generally seen as the domain of the IETF. We also understand that the IETF may be a more open venue for stakeholders impacted by DNT headers who may not be members of the W3C, so that may be another factor to consider in selecting the appropriate venue.

About Mozilla and Privacy

Mozilla is a global community of people working together since 1998 to build a better Internet. As a non-profit organization, we are dedicated to promoting openness, innovation, and opportunity online. Mozilla and its contributors make technologies for consumers and developers, including the Firefox web browser used by more than 400 million people worldwide. As a core principle, we believe that the Internet, as the most significant social and technological development of our time, is a precious public resource that must be improved and protected.

Privacy and security are important considerations for Mozilla. They are embraced in the products and services we create, and derive from a core belief that consumers should have the ability to maintain control over their entire web experience, including how their information is collected, used and shared with other parties. We strive to ensure privacy and security innovations support consumers in their everyday activities whether they are sharing information, conducting commercial transactions, engaging in social activities, or browsing the web.