

Web Tracking Protection

W3C Workshop on Web Tracking and User Privacy

28/29 April 2011, Princeton, NJ, USA

[Adrian Bateman](#), Internet Explorer Program Manager, Microsoft Corporation

At Microsoft, we believe that it is critical for the industry to build innovative solutions founded on the principles of transparency, control and security. We are very proud that Internet Explorer 9 was the [first major browser to respond](#) to the recent call from the Federal Trade Commission in the United States for a “Do Not Track” mechanism.

In February, we made a [Member Submission](#) to the W3C proposing a [Web Tracking Protection](#) standard. This specification is designed to help users have better control over their online information and has two parts:

- Filter lists, which can enforce user privacy preferences by preventing the user agent from making unwanted requests to specific third party web servers that could be used to track users as they visit first party web sites.
- A “Do Not Track” user preference, which is an HTTP header and a DOM property.

Together these technologies can be used to provide privacy protections for users by helping them to control which third party web sites their user agent communicates with and to allow their user agent to signal their intention with respect to tracking.

A filter list contains parts of third-party URIs that a browser may access automatically when referenced within a web page that a user deliberately visits. Rules in a filter list may change the way the user agent handles third-party content. By limiting the calls to these third party web sites the filter list limits the information other sites can collect about a user.

The “Do Not Track” user preference is maintained by the user agent and is exposed as both a HTTP header, which can be read by a web server, and as a DOM property, which can be accessed by client-side JavaScript. The DOM property is particularly important in environments where the site developer may not have access to the raw HTTP request headers. Both the header and property convey the same user preference.

Web sites that choose to respect the “Do Not Track” user preference will read this value and will not “track” the user when this setting is enabled. This depends on what the definition of “tracking” is and what it means not to track a user. This is a complex topic as “tracking” could cover a wide variety of activities including online behavioural advertising, analytics, etc. Microsoft has submitted a separate paper about defining the meaning of “track” and appropriate web site responses to the “Do Not Track” user preference.

The final version of Internet Explorer 9 [released on March 14](#) implements full support for the features described in our Web Tracking Protection submission. With IE9, anyone on the Web can create and publish a Tracking Protection filter list. These simple files are uploaded to a web site and

made available to others via a link. Users can create or subscribe to more than one list if they wish and, because the Web evolves over time, IE9 will automatically check for updates to the user's lists on a regular basis. We invite workshop participants and the wider community to review the details of the submission.

References

Web Tracking Protection

W3C Member Submission 24 February 2011

<http://www.w3.org/Submission/2011/SUBM-web-tracking-protection-20110224/>