

# Microsoft Turning Off Do-Not-Track in its Next Generation Browser

April 3, 2015 – For the past two years, Microsoft has enabled “do-not-track” (DNT) by default in Internet Explorer (IE). The company received a lot of positive publicity when it made the announcement. So it caught our eye when the company announced that “do-not-track” would no longer be default-enabled when it releases its next browser. As it turns out, the company appears to have little choice in the matter.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

The change is due to a policy shift by the World Wide Web Consortium (W3C). W3C sets the standards for do-not-track and has just released draft language for the new DNT standard. That draft contains the following line of text: “In the absence of user choice, there is no tracking preference expressed.”

The language means that if Microsoft enables DNT in its browsers, companies would be able to ignore the setting without breaking W3C policy. Apache ignited a fire storm of criticism when it announced that it would ignore Microsoft’s security settings in its web servers specifically because Microsoft had DNT turned on by default.

To be clear, the W3C standard is voluntary. Companies can ignore without running afoul of the law but most comply for publicity reasons.

The announcement does make things a little less convenient for IE users. But Microsoft has said that it will make the ability to turn on DNT as easy as the company possibly can, and will provide detailed instructions to users.

At ACCESS we like the concept of DNT however, because compliance is voluntary, we also know that anyone using a browser with DNT enabled could be lulled into a false sense of security. Using a browser with DNT embedded in it is no substitute for vigilance.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here.

Registration is easy and free.

Follow me on Twitter:

Follow ACCESS