

# Regulators, ad companies huddle over 'Do Not Track' features

April 12 2012, By Mike Swift

---

The momentum of a growing multibillion-dollar industry is colliding with online privacy worries this week, as regulators and privacy advocates face off against the Internet advertising industry to hash out how proposed "Do Not Track" features in Web browsers will actually work.

Federal regulators and many politicians want to give [consumers](#) the option of clicking a button in their browser to provide some privacy from the extensive industry that has grown up around the collection and sale of information about people's online interests.

But a pivotal question remains unanswered: Does "Do Not Track" mean consumers could only block advertising targeted to their interests, while Internet companies continue to monitor and share data about them? Or should "Do Not Track" give consumers the ability to block most data collection by companies that sell the information about their online habits?

The [World Wide Web Consortium](#) (or W3C) Tracking Protection Group, a standard-setting group that includes big Internet [advertising companies](#) like Google and Facebook as well as privacy advocates and regulatory agencies from the U.S. and Europe, on Tuesday began three days of meetings in Washington. After a series of meetings in recent months from [Silicon Valley](#) to Belgium, the group hopes this week's sessions will help settle a universal "Do Not Track" standard for major Web browsers such as Microsoft's [Internet Explorer](#), Mozilla's Firefox,

Google's Chrome and Apple's Safari.

"It's something that I think most people don't even realize is going on, but those negotiations could have huge ramifications about whether [future generations](#) of [Internet users](#) can browse the web without being tracked everywhere they go," said Rainey Reitman of the San Francisco-based [Electronic Frontier Foundation](#), which is participating in the talks.

Meanwhile, digital advertisers are concerned the talks could supersede their own self-regulatory efforts, and undermine an industry that is the financial backbone of the Internet and that has generated billions of dollars for Google, Yahoo and Facebook and many other companies.

"We don't want to fragment the successful self-regulatory efforts that have taken place over the last four years by industry," said Mike Zaneis, general counsel for the Interactive Advertising Bureau, an industry group participating in W3C.

While consumer concerns about online privacy are real, Zaneis said, consumers do not want to sacrifice the many free products - such as email, online news, digital music and social networks - paid for by online advertising. "I don't think that most privacy advocates speak for the general public. Most of these groups don't have broader insight into consumer expectations," he said.

The Federal Trade Commission, the federal agency most directly charged with consumer privacy, recommended March 26 that Do Not Track features be added to the major browsers. In recent statements, FTC officials have said Do Not Track must do more than just block targeted advertising.

"Most consumers care less about the ads," Christopher Olsen, who heads the FTC's Division of Privacy and Identity Protection, said at a recent

legal conference in Washington. "They care more about the fact that they are being followed or tracked. So we do look at it more as 'Do Not Collect' versus 'Do Not Target.' "

A "Do Not Collect" standard that limits the gathering of data about online behavior would have a significant financial impact on the industry, Zaneis said. A recent industry study found that advertising targeted according to a person's interests and online history is worth more than twice as much to advertisers than ads that are not targeted.

Still, it's unclear how many consumers would actually use Do Not Track technology if it became standardized across all major browsers.

Firefox was the first browser to offer a built-in Do Not Track feature more than a year ago, but only about 7 percent of desktop Firefox users, and 18 percent of mobile Firefox users, have turned it on, according to Mountain View, Calif.-based Mozilla.

One key issue the W3C group is tackling this week is "third party" data collection.

An example of that is when a visit by a consumer to a website results in tracking technology such as software "cookies" being attached to the consumer's browser, generally without the consumer's knowledge, by a third party that the website has a business relationship with, but that the consumer does not.

"That's really the crux of what Do Not Track is about - it's about managing tracking by those people who you don't have a relationship with," said Peter Eckersley, technology project director of the Electronic Frontier Foundation.

Many [privacy advocates](#) say the strong statements made by the FTC and

European regulators that consumers need to a tool to block data collection and not just ads give them more leverage in this week's talks.

"They created the business - [Google](#), Yahoo and others - they created the online model without thinking about the privacy implications, and it's been hugely successful for them," said Jeff Chester, executive director of the Center for Digital Democracy, a privacy rights group.

"Now, what we're saying is, 'You've got to put the consumer-data-collection genie back in the bottle. You've got to give consumers control about how their data is used.' And they are balking."

(c)2012 the San Jose Mercury News (San Jose, Calif.)  
Distributed by MCT Information Services

Citation: Regulators, ad companies huddle over 'Do Not Track' features (2012, April 12)  
retrieved 10 May 2024 from <https://phys.org/news/2012-04-ad-companies-huddle-track-features.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--