Consumer Federation of America
1620 I Street, N.W., Suite 200 * Washington, DC 20006

Why We Need a "Do-Not-Track" Mechanism to Protect Consumers' Online Privacy

What is Online Behavioral Tracking and Targeting?

Consumers are being tracked on the Internet wherever they go, whatever they do, without their knowledge and consent. Information about their online activities – what they search for, what they click on, what they purchase, what they share with others – is compiled, analyzed, and used to profile them. Sometimes information that is gathered about them offline is added to create even richer profiles. This "behavioral tracking" is primarily used for marketing purposes at this point, but it can also be used to make assumptions about people in connection with employment, housing, insurance, and financial services; for purposes of lawsuits against individuals; and for government surveillance. There are no limits to what types of information can be collected, how long it can be retained, with whom it can be shared, or how it can be used. As the Wall Street Journal characterized it, "one of the fastest- growing businesses on the Internet is the business of spying on consumers."[1]

What do consumers think about online behavioral tracking and targeting?

Surveys clearly show that many consumers are uncomfortable with online behavioral tracking and targeting. For example, a 2009 survey by researchers at the University of Pennsylvania and the University of California found that 66 percent of respondents did not want the Web sites they visit to show them ads tailored to their interest, and when the common tracking methods were explained, an even higher number rejected tailored advertising. More recently, a poll commissioned by the nonprofit organization Consumer Watchdog in July 2010 revealed that 90 percent of Americans wanted more laws to protect privacy, 86 percent favored the creation of an "anonymous button" that allows individuals to stop anyone from tracking their online searches or purchases, and 80 percent wanted a "do-not-track-me" list for online companies that would be administered by the FTC.

Why are consumers concerned?

Some of the information that is tracked is sensitive, such as that related to people's health conditions or sexual preferences. Another concern is that behavioral profiles created by online tracking can be used for purposes beyond simply deciding whether to display an ad for a pick-up truck or a sedan to a consumer – they can also be used to make assumptions about people for employment, insurance, housing or financial services. Decisions are even being made about consumers' creditworthiness based on who their friends are on social networking sites! These assumptions may not be accurate – for instance, a person researching cancer online because of a friend's illness might be wrongly assumed to have the disease. There are also concerns about access to online profiles by law enforcement agencies, lawyers in divorce proceedings and others who might use the information in ways that consumers would never expect. And some consumers may feel that it is simply unfair to follow them around the Internet when they are engaged in their own personal activities.

---

[1] See Wall Street Journal, *What They Know*, series of articles from July 31-August 10, 2010, http://online.wsj.com/public/page/what-they-know-digital-privacy.html

Don't consumers already have protection from unwanted tracking?

No, there are no laws that require consumers to be given the choice of whether or not to be tracked, and voluntary programs offered by industry are not adequate. Not all companies that engage in behavioral tracking and targeting participate in those programs, and there are no real penalties for failing to comply with them. There are also many loopholes in industry programs; for example, they may not apply to tracking by or sharing profiles with a company's many affiliates – other companies that are under the same corporate ownership but with which the consumer may not be familiar or have any relationship. Plus industry programs that enable consumers to choose not to be tracked are based on placing "cookies" on their computers. These electronic files are not always effective in stopping tracking depending on the methods that are used to do it, and they can be deleted.

How would a "Do-Not-Track" mechanism work?

A "Do-Not-Track" mechanism would not work the same way as the national "Do-Not-Call" registry with which many consumers are familiar. There would be no need to sign up anywhere or provide any personal information. It would be a setting in Web browsers (such as Internet Explorer) that consumers could use to indicate that they do not wish to be tracked. The browsers would express the consumers' preferences to the Web sites they visit. It would be easy to implement and simple for both consumers and trackers to use. And just as consumers whose numbers are on the national "do-not-call" registry can opt-in to receiving calls from telemarketers on a company-by-company basis, so could consumers give permission for tracking by certain entities, in this case through their browser settings. All browsers would be required to include a "do-not- track" mechanism as a standard feature, at no extra cost to consumers. And just as important, all trackers would be required to honor the consumers' preferences.

Who would enforce a "Do-Not-Track' requirement?

The Federal Trade Commission, which is responsible for making sure that marketers do not engage in unfair or deceptive practices and created the "Do-Not-Call" registry, is the logical federal agency to enforce "Do-Not-Track" requirements. The FTC would not dictate the design of the technology but would set the overall goals that it should accomplish: providing consumers with a simple, easy-to-use mechanism that effectively and persistently enables them to exert control over online tracking. If a "Do-Not-Track" requirement implemented, the FTC should be tasked with performing audits and "mystery browsing" to ensure that trackers are complying, since it is very difficult for consumers themselves to know if their information is being tracked and how it is being used. Consumers should also be able to bring their own legal actions to enforce their privacy rights.

Where can consumers get more information?

For more information about the issues related to online behavioral tracking and targeting go to www.consumerfed.org/consumer-privacy/privacy and read the fact sheets, testimony and comments there. At http://donottrack.us, there are helpful explanations of how a "Do-Not-Track" mechanism would work.