



Consumer Federation of America

**PRESS RELEASE
FOR IMMEDIATE RELEASE**

CONTACT:
Jack Gillis, (202) 737-0766

CFA CALLS FOR A “DO-NOT-TRACK” TOOL TO PROTECT CONSUMER PRIVACY ONLINE

House Testimony (Dec. 2, 2010) Outlines Dangers if Consumer Can't Control Access to Their Online Activities

Washington, D.C. - At a December 2, 2010 hearing before the House Committee on Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection, Susan Grant, CFA's Director of Consumer Protection, answered the question that the subcommittee posed, "Do-Not-Track Legislation: Is Now the Right Time?," with a resounding "Yes." Consumers are being tracked on the Internet wherever they go, whatever they do, without their knowledge and consent. The information gleaned from their online advertising, called "behavioral tracking," is used to tailor ads to show them based on their profiles. However, as Grant pointed out, this information can also be used to make assumptions about people for other purposes, such as employment, housing, insurance, and financial services. It can also be used for lawsuits and 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," Grant testified.

Grant noted that assumptions made about people based on their online activities or who their "friends" are in social networking sites may not be accurate. "I may be searching online for information about cancer or HIV because a friend or relative is ill; I certainly would not want my insurance company to know about my searches or to make any determinations about me on the assumption that I have a condition," Grant said. Furthermore, she said that surveys have shown that many consumers simply do not want to be followed around on the Internet, even if that would result in seeing ads that are more relevant to their interests.

To give consumers effective control over information about their online activities, CFA and other consumer and privacy groups are calling for a "Do-Not-Track" mechanism. This would be similar to the immensely popular national "Do-Not-Call" registry, which is overseen by the Federal Trade Commission and enables consumers to opt out of all telemarketing calls if they wish. It would not require consumers to sign up or to provide any personal information, however. Instead, what CFA and others envision is a browser-based tool that would automatically tell the Web sites that consumers visit not to track them. Under this proposal, all browsers would be required to include a "Do-Not-Track" mechanism as a standard feature, and no extra cost to consumers, and all trackers would be required to honor the consumers' preferences. Consumers would be able to adjust the settings to accept tracking by certain entities if they wished.

Self-regulation is not adequate, according to Grant. “There is no requirement that companies participate in them, there is no oversight or transparency, and there is no enforcement,” Grant explained. Furthermore, the opt-out mechanisms that industry-led programs use are based on cookies, which do not work for some tracking methods and fail to provide persistent protection from unwanted tracking since cookies can be deleted for a variety of reasons. CFA has created a new fact sheet, *Why We Need a “Do-Not-Track” Mechanism to Protect Consumers’ Online Privacy*. The fact sheet and Grant’s testimony are in the privacy section of CFA’s Web site, <http://www.consumerfed.org/consumer-privacy/privacy>.

The Consumer Federation of America is an association of nearly 300 nonprofit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.