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

Online Behavioral Advertising: Tracking Your Every Click

What is online behavioral advertising?

It is targeting advertisements to consumers based on profiles that are created by tracking their activities online over time. Those activities can include:

- The searches they make
- The Web pages they visit
- The content they view
- The videos they watch and other interactions on social networking sites
- The content of emails they send and receive.
- How they spend money online.

Other data derived offline can be combined to create even more detailed profiles of consumers. This is different than contextual advertising, in which ads are generated by a search that a consumer is conducting or a page the consumer is viewing at that moment.

What are the risks of online behavioral advertising to consumers?

- **Tracking people's every move online is an invasion of privacy.** It's like being followed by an invisible stalker – consumers aren't aware that it's happening, who is tracking them, and how the information will be used. They're not asked for their consent and have no meaningful control over the collection and use of their information, often by third-parties with which they have no relationships.

- **Online behavioral advertising can be used to take advantage of vulnerable consumers.** Information about someone's health, financial condition, age, sexual orientation, and other personal attributes can be inferred from online tracking and used to target the person for payday loans, sub-prime mortgages, bogus health cures and other dubious products and services. Children are an especially vulnerable target audience since they lack the capacity to evaluate ads.

- **Online behavioral advertising can be used to unfairly discriminate against consumers.** Profiles of consumers, whether accurate or not, can result in "online redlining" in which some people are offered certain consumers products or services at higher costs or with less favorable terms than others.

- **Online behavioral profiles may be used for purposes beyond advertising.** For instance, law enforcement agencies may be interested in using these profiles to attempt to identify terrorists or other criminals. Employers, divorce attorneys, private investigators

and identity thieves may also find the information attractive. Consumers have no control over who has access to it, how it is secured, and under what circumstances it may be obtained.

What needs to be done to protect consumers from these risks?

Consumers are entitled to respect for their privacy when they browse the Internet and communicate with others online. The growth of ecommerce and the ability to use the online medium for social interaction and civic discourse is endangered if they must worry that their every move is being tracked.

- **No online behavioral tracking without express consent.** The Federal Trade Commission should devise a standard disclosure and opt-in form. Consumers who opt-in should be able to change their minds anytime and have their profiles deleted.
- **No tracking of sensitive personal information.** Information about a consumer's health, sexual orientation, and financial condition should not be allowed to be tracked because the risks that could result from abuse and security lapses are too severe.
- **Do-Not-Track Registry.** Similar to the popular Do-Not-Call Registry, this would enable consumers to avoid all behavioral tracking easily.

Wouldn't these restrictions kill free content on the Web?

No, free content on the Web will still be available from commercial and non-commercial sources. Contextual advertising, which does not raise the same concerns, would not be impacted. Behavioral tracking and targeting would still be allowed, but consumers would be in control. It's up to advertisers to make the case for why consumers should exchange their personal information for the benefits of behavioral advertising. If it's a fair exchange, consumers will agree to the deal.

Aren't companies' privacy policies enough?

No. Studies have shown that when consumers see privacy policies on Web sites, they incorrectly assume that means that their personal information is not shared with others. Privacy policies are written in legalese that most consumers can't understand. Furthermore, behavioral tracking is usually done by third-party ad networks, not the owners of the Web sites themselves, so the privacy policies on the sites do not apply.

Why not let self-regulation and guidance from the FTC solve the problem?

Self-regulatory programs have been totally ineffective to protect consumers from this invisible stalking. They rely on "opt-out" mechanisms that most consumers don't know about and that don't work well. The FTC's principles for behavioral advertising don't require companies to do anything and don't provide a basis for action to stop abuses.

Written by: Susan Grant, Director of Consumer Protection, Consumer Federation of America (202-387-6121). Endorsed (in formation) by Center for Digital Democracy, Consumer Watchdog, Privacy Rights Clearinghouse