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

Five Myths about Online Behavioral Advertising

Myth #1. Free content on the Internet will disappear if advertisers can only engage in online behavioral tracking and targeting with affirmative consumer consent (opt-in).
False. While industry-funded studies show some economic value of online advertising, they provide NO proof that advertising will be greatly diminished or free content on the Web would cease to be available if online behavioral tracking and targeting is subject to consumer consent. Contextual advertising, in which ads are delivered based on what consumers are doing online at that moment, would not be impacted at all. Behavioral tracking and targeting would still be allowed, but consumers will be in control. Advertisers would have to make the case why consumers should allow their online behavior to be tracked and used for tailored advertising. If it's a fair exchange, consumers will agree. Furthermore, limits on the collection and use of information about consumers' online behavior would spur advertisers to innovate and develop new, more privacy-oriented techniques to deliver tailored ads. One group of professors has already developed a program that enables a computer user's browser to choose ads based on the user's interests, without the advertiser having any information about the person.[1]

Myth #2. There is no reason to be concerned because there is no harm in behavioral advertising.
False. Tracking people's every move online is a fundamental invasion of their privacy. It's like being followed by someone who compiles and sells information showing everywhere you drive, where and when you stop, and what you do at that location. It violates basic human dignity, which the Federal Trade Commission recognizes as an important interest that must be protected.[2] There are also other concerns. For instance, the FTC's counterpart in the UK, the Office of Fair Trading, is looking into how online behavioral tracking is being used for "customized pricing" (redlining) as part of an investigation of advertising practices.[3] Information about someone's health, finances, age, sexual orientation, and other personal attributes inferred from online behavioral tracking could be 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. Furthermore, government agencies, employers, insurers, divorce attorneys, private investigators and identity thieves may find information from behavioral tracking useful for purposes that have nothing to do with advertising.

---

[1] See blogpost and link to paper at http://www.freedom-to-tinker.com/blog/felten/privads-behavioral-advertising-without-tracking
[2] "Fresh Views at Agency Overseeing Online Ads," New York Times, August 4, 2009, http://www.nytimes.com/2009/08/05/business/media/05ftc.html
[3] "Office of Fair Trading to probe use of personal data by online retailers," Guardian, October 15, 2009, http://www.guardian.co.uk/business/2009/oct/15/retail-pricing-tactics-oft-investigation

Myth #3. It's just "privacy elitists" who are concerned about online behavioral advertising – consumers, especially young people, want tailored ads and are not troubled by tracking.
False. Surveys show that most consumers are concerned about their online privacy. A new study[4] by researchers at the University of Pennsylvania and the University of California-Berkeley found that two-thirds of adults in the U.S. don't want Web sites to show them ads that are tailored to their interests. When the common methods of behavioral advertising are explained the rejection rate is even higher, (75 percent don't want ads based on Web sites they are visiting; 87 percent don't want ads based on Web sites they have visited; and 89 percent don't want ads based on their offline activities, such as in stores). Responses from the 18-24 age group are similar (67 percent don't want ads based on Web sites they are visiting, 86 percent don't want ads based on other Web sites they have visited, and 90 percent don't want ads based on their offline activities). Even the prospect of discounts or more relevant news from Web sites does not appreciably change people's attitudes. Many (63%) believe that advertisers should be required by law to immediately delete information about Internet activity.

Myth # 4. Notice and ability to opt-out is enough.
False. The University of Pennsylvania and University of California-Berkeley study [5] shows that privacy policies and misunderstood and inadequate. Many adults (63%) incorrectly believe that if a Web site has a privacy policy, it means that the site cannot share information about them with other companies without their permission. Other surveys have produced similar results. One reason for this misunderstanding may be that privacy policies are written in legalese that most consumers can't understand. If marketers must get consumers' affirmative consent to track their behavior for advertising purposes, the marketers will have to clearly explain the benefits to persuade people to sign up. This is how the marketplace should work if the goal is to give meaningful choice to consumers.

Myth #5. Self-regulation will solve the problem.
False. Self-regulation for privacy has failed repeatedly in the past. Self-regulation has been totally ineffective to protect consumers from the invisible stalking of behavioral tracking. It relies on "opt-out" mechanisms that most consumers don't know about and that don't work well.[6] The "Self-Regulatory Principles for Online Behavioral Advertising"[7] recently released by industry groups don't provide real privacy protection. For instance, they allow companies to track visitors' behavior on their Web sites for their own use and their affiliates' invisibly; notice is only required if the information is shared with third-parties. Consent is only required to collect certain narrowly-defined types of sensitive information such as Social Security numbers, financial account numbers, prescriptions, or medical records – no consent is needed to track the health or financial Web sites consumers go to or other sensitive online activities. Behavioral data can be kept indefinitely. While self-regulatory programs can help provide guidance to companies, participation in them should not create "safe harbors" that presume that privacy protections for consumers are adequate.

---

[4] *Americans Reject Tailored Advertising and Three Activities that Enable It*, Turow, King, Hoofnagle, Bleakly, Hennessy, September 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214
[5] Id
[6] See for example *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*, World Privacy Forum, Fall 2007, http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf
[7] See http://www.iab.net/insights_research/public_policy/behavioral-advertisingprinciples