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

COMMENTS OF DR. MARK COOPER,
DIRECTOR OF RESEARCH,
CONSUMER FEDERATION OF AMERICA
TO THE
FEDERAL TRADE COMMISSION TOWN HALL MEETING ON
"EHAVIORAL ADVERTISING: TRACKING, TARGETING AND TECHNOLOGY"

November 16, 2007

At the Town Hall meeting on "Ehavioral Advertising: Tracking, Targeting and Technology" a group of privacy, technology and consumer organizations proposed a "Do Not Track" list, modeled on the "Do Not Call list," to protect consumer privacy in the online marketplace. After listening to two days of presentation and discussion of the current state of privacy protection in the online market, the Consumer Federation of America, one of the groups supporting the proposal, is more convinced than ever that such a mechanism in necessary.

The Problem

The conference made it abundantly clear to us that after seven years of industry self regulation, neither the voluntary organizations nor the individual companies' approaches to privacy protection are working. Somewhat less than 5 percent of consumers are effectively able to protect their privacy.

- Only if consumers are strongly interested, extremely literate, well informed and highly skilled can they negotiate the opaque, inconsistent morass of opt-out procedures, and even then there are numerous data collection and tracking mechanisms that go undisclosed.

- Unfortunately, the vast majority of consumers lack one or more of these characteristics and therefore are not protected.

We reach this conclusion by combining key facts that were brought out at the Town Hall. The industry claims things are good in the privacy space of the online market because there are some sites that would let the consumer opt-out with as few as three clicks (but the average seems closer to five). We have been at too many meetings with e-companies who insist that each click costs them ten percent market share (and therefore they have got to be the default) to accept the claim that three or five clicks is good enough. Consumer privacy is not getting a fair shake in the online market.

We heard that 85% of the companies have privacy statements, but that 99% of them are incomprehensible. As a result, less than one percent of consumers read privacy statements. There was not one advertising company in the room that would dare walk into a client with language looking like the current crop of privacy statements and say, "here, use this to sell your product." They would be kicked out of the office and be out of business in no time flat. Consume privacy is not getting a fair sake in the online market.

We saw survey evidence of a huge cap between what consumers want and what marketers think they deserve. This is not an uniformed public, as suggested by the presenter; it is a public that is very concerned about its privacy. The desire of over three quarters of the respondents for strong privacy protection is not being met in the marketplace.

The Approach to the problem

We heard a series of bogus claims about what privacy protection should and should not do in the online advertising market that stem primarily from a mischaracterization of the moral basis of privacy. Consumer privacy is a right to be protected, not a harm to be avoided.

The issue is not about democratic speech or antitrust merger enforcement, or even competition and efficiency. It is about the consumer's right to privacy.

- Democratic discourse on the internet is vigorous and likely to remains so -- consumer privacy protection is not.

- While there may be threats to an open, democratic Internet (like a lack of network neutrality), they are not grounded in advertising.

- Antitrust merger enforcement is weak in America (some would say dormant), but even if it were vigorous, it would not achieve the level of privacy protection the public wants, expects or deserves. Shoe horning privacy into merger proceedings requires the acceptance of the harm-based frame and the economic efficiency analytic as supreme, weakening the moral claim to privacy protection and narrowing the range of solutions.

Moreover, even if the FTC insists on a harm-based approach, we heard more than enough evidence of the threat to the public welfare to justify dramatic changes in public policy designed to improve consumer privacy protection.

Because behavioral targeting involves practices that are inherently deceptive and distort consumption, especially among vulnerable populations like youth and the elderly. The inherently deceptive practices that pervade the behavioral marketing space include suggestions of relationships that do not exist and use of information about the consumer that the consumer has not willingly divulged to the seller.

Behavioral targeting may be particularly harmful to vulnerable populations, including youth and the elderly. Although the survey data showed that few consumers of any age comprehend the trade-offs involved with behavioral targeting, youth and the elderly are at special risk of not understanding the consequences of being tracked online. These populations in particular deserve better than an opt-out description buried five clicks away in a privacy policy.

So-called "sensitive information" was a hot topic at the workshop, and gets to the heart of another harm stemming from behavioral targeting. Industry practices concerning the collection of health, sexual, religious, political, and other forms of sensitive data are not uniform and mostly unregulated, leaving open the potential for highly personal information to be exposed. We can all recognize the danger of a situation where an employee's health condition is at risk of being revealed to his or her employer – and yet the controls around this kind of data collection and use in the behavioral targeting area are slim.

Behavioral targeting also opens the door to undue price discrimination and red lining. While these practices may not be yet be widespread in the marketplace, there is little standing in the way of employing behavioral data for these purposes, while consumers remain ignorant to such developments.

Behavioral data is also open to civil subpoenas, court orders, and unauthorized or warrantless government access. Civil litigants and government authorities will no doubt soon realize the treasure trove of behavioral profile information held by online behavioral targeting firms.

Finally, because behavioral targeting involves the collection of large quantities of data about individuals, security breaches – both internal and external – are a constant threat and may expose consumers to the risks of identity theft. Aside from major data breaches, the FTC has little capacity to monitor or detect the extent of these harms.

We also heard a series of bogus claims about what privacy protection would and would not do to the online advertising market. This issue is not about "killing free content" on the Internet. Not only is there a vast array of noncommercial content that will remain (part of the reason we reject the claim that advertising will kill democracy on the Internet), but a well-crafted consumer privacy protection scheme will support competition and efficiency in an expanding advertising market. Advertising will continue and continue to improve, within the parameters that public policy sets. Representative of several e-companies affirmed that behavioral tracking is not necessary to build successful online advertising models.

If behavioral targeting is constrained by consumer privacy protections, innovation will focus on the legitimate mechanisms that can improve the quality of advertising. The innovative juices of the industry just need to be channeled in the social responsible direction. Judging from the "do not call list" the market will split between those who want and need a simply, single consumer-friendly way to opt out of tracking and those who will be more selective choosing privacy protection.

Principles for a solution

Given the failure of the current approach to privacy protection in the past seven years, a new approach must be adopted based on six principles, outlined in the " do not track" proposal.

(1) A simple consumer-friendly interface to the desire not to be tracked across all platforms must be implemented.

(2) There must be robust notification about how to make that declaration and continuous contextual notification of the status of tracking

(3) A consistent set of basic privacy protections and definition that consumers can understand.

(4) Enforcement to ensure compliance must have teeth, so consumers can trust the system to protect their privacy.

(5) An effective right to correct information about and categorization of the consumer that is used for marketing online.

(6) An organized process for overseeing and updating the protection of consumer privacy protection. Seven years is too long to wait to keep consumer protection on a pace with innovation in online markets.