Concurring Statement
of Commissioner Jon Leibowitz
FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising
(February 2009)

Behavioral marketing is complicated, and determining its appropriate regulatory framework is complicated, too. The FTC staff's commendable Report continues to examine emerging practices, consider public comments and consumer expectations, and fashion an appropriate and flexible approach for industry self-regulation. As the Report points out, targeted advertising can benefit consumers, subsidize free content, and promote a robust online market. But the concomitant online tracking and data collection, coupled with inadequate notice to consumers about what information is collected and how it is used, raise critical privacy concerns. How companies collect, combine, disclose and dispose of this data has serious ramifications for consumers.

I write separately to ensure that the Report's endorsement of self-regulation is viewed neither as a regulatory retreat by the Agency nor an imprimatur for current business practice. Indeed, despite a spotlight on e-commerce and online behavioral marketing for more than a decade, to date data security has been too lax,[1] privacy policies too incomprehensible,[2] and consumer tools for opting out of targeted advertising too confounding.[3]

Industry needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite legislation by Congress and a more regulatory approach by our Commission.[4] Put simply, this could be the last clear chance to show that self-regulation can – and will – effectively protect consumers' privacy in a dynamic online marketplace. Commissioner Harbour's thoughtful statement underscores this point.

To their credit, many companies and organizations recently have reinvigorated efforts to address privacy issues and have made noteworthy attempts to empower consumers. For example, leading search engines such as Yahoo! are reducing the amount of time they retain consumers' personal data.[5] Microsoft and other developers of Internet browsers are designing better tools for consumers to control the amount of information they share online.[6] Such "competition" to protect consumer privacy is a welcome development. Other industry groups are coming together and attempting to formulate (and reformulate) better practices.[7] In addition to these industry efforts, a coalition of consumer and privacy groups proposed a national "Do Not Track List," which deserves serious consideration.[8] But it is uncertain whether these fledgling efforts will fulfill their promise. More work needs to be done.

The Report's revised principles provide a sound baseline for further self-regulatory efforts. Notably, the Report clarifies that the self-regulatory principles should stretch beyond traditional concepts of personally identifiable information to cover practices involving information that "could reasonably be associated with a particular consumer or computer or other device" (e.g., IP addresses, cookie data). The Report further clarifies that the principles should apply to information collected outside the traditional website context, such as through mobile devices and Internet Service Providers' "deep packet inspection" to mine data from consumers' Internet traffic streams for targeted advertising.[9] These are significant and necessary steps for enhancing consumer privacy.

Beyond the principles, I offer a few observations regarding privacy, transparency, and consumer control both within and outside the behavioral advertising context:

To begin, as the Report should make clear, there is no free pass for those who engage in "first-party" or "contextual" online advertising outside the scope of the principles. That is, *all* companies must implement reasonable security for and limit their retention of sensitive consumer data. *All* companies must keep their promises about how they will use consumers' information. If they fail to do so – whether first party or third party, online or offline – we will go after them.

Moreover, I continue to be troubled about some companies' unfettered collection and use of consumers' "sensitive data" – especially information about children and adolescents. Some data is so sensitive and some populations so vulnerable that extra protection may be warranted.[10] Perhaps more companies (even those outside the scope of the behavioral advertising principles) should allow consumers to "opt in" when it comes to collecting their personal information – particularly when the information is "sensitive," or disclosed to third parties, or collected or shared across various web-based or offline services. Perhaps more companies should simply say "hands off" when it comes to targeting ads to children based on their online activities, as even the Network Advertising Initiative proposed (although it has not mustered the industry support to adopt this principle).[11]

Finally, we need to better understand if and how companies combine online and offline data to build detailed consumer profiles and uses of online tracking data for purposes unrelated to behavioral advertising. The possibility that companies could be selling personally identifiable behavioral data, linking click stream data to personally identifiable information from other sources, or using behavioral data to engage in price discrimination or make credit or insurance decisions are not only unanticipated by most consumers, but also potentially illegal under the FTC Act. Industry's silence in response to FTC staff's request for information about the secondary uses of tracking data is deafening. As a result, the Commission may have to consider using its subpoena authority under Section 6(b) of the FTC Act to compel companies to produce it.

In sum, almost all of us want to see self-regulation succeed in the online arena, but the jury is still out about whether it alone will effectively balance companies' marketing and data collection practices with consumers' privacy interests. A day of reckoning may be fast approaching.

Endnotes

[1.] *See* Report at n.8 and accompanying text (citing numerous FTC enforcement actions challenging online and offline companies' failure to provide reasonable security for consumers' sensitive information); *see also* Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times (Aug. 9, 2006), *available at* http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63 (describing incident in which AOL released purportedly "anonymous" user search data, but some users were identified based on their queries).

[2.] A study of the privacy policies of Fortune 500 companies found that they were essentially incomprehensible for the majority of Internet users. Only one percent of the privacy policies were understandable for those with a high school education or less (like most teens and many consumers). Thirty percent of the privacy policies required a post-graduate education to be fully understood. Felicia Williams, *Internet Privacy Policies: A Composite Index for Measuring Compliance to the Fair Information Principles* at 17 & Table 2 (Sept. 2006), *available at* http://www.ftc.gov/os/comments/behavioraladvertising/071010feliciawilliams.pdf.

[3.] For example, the NAI opt-out tool can be difficult for consumers to find and use and the cookie-based methodology is problematic. Privacy conscious consumers who routinely delete all their cookies or use anti-spyware programs may unintentionally delete the opt-out cookies. *E.g.*, Prof. Peter P. Swire & Prof. Annie I. Anton, *Comments on the FTC Staff Statement, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles"* (Apr. 10, 2008), *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080410swireandanton.pdf.

[4.] *See, e.g.,* Saul Hansell, *Senators Weigh Possible Rules for Advertising and Online Privacy*, http://bits.blogs.nytimes.com/2008/07/09/senators-weigh-possible-rules-for-advertising-and-online-privacy/ (July 9, 2008, 4:15 PM); John Eggerton, *Senate Commerce Committee holds hearing on 'Privacy Implications of Online Advertising,'* Broad. & Cable (July 9, 2008), *available at* http://www.broadcastingcable.com/article/114482-Senate_Commerce_Committee_Examines_Online_Privacy.php; John Eggerton, *Markey Pushes for Online-Privacy Legislation,* Broad. & Cable (July 9, 2008), *available at* http://www.broadcastingcable.com/article/114606-Markey_Pushes_for_Online_Privacy_Legislation.php.

[5.] Miguel Helft, *Yahoo Limits Retention of Search Data,* N.Y. Times, Dec. 18, 2008, at B3*, available at* http://www.nytimes.com/2008/12/18/technology/internet/18yahoo.html?_r=1&fta=y&pagewanted=print.

[6.] *See, e.g.,* Ctr. for Democracy & Tech., *Browser Privacy Features: A Work in Progress,* CDT Report (Oct. 2008), *available at* http://www.cdt.org/privacy/20081022_browser_priv.pdf (comparing the privacy features of Mozilla Firefox 3, Microsoft Internet Explorer 8 Beta 2, Google Chrome, and Apple Safari 3).

[7.] For example, in January, 2009, the American Association of Advertising Agencies, the Association of National Advertisers, the Direct Marketing Association, the Interactive Advertising Bureau, and the Council of Better Business Bureaus announced that they formed a coalition to develop self-regulatory guidelines for behavioral targeting. Mike Shields, *Online to Obama: We Can Police Ourselves; Concern about new regulation prods speedy digital ad industry reaction*, Adweek (Jan.19, 2009), http://www.adweek.com/aw/content_display/news/digital/e3iecbc44179b8d6b3130e3a2b509fa0f52.

[8.] Ctr. for Democracy & Tech., Consumer Action, Consumer Fed'n of Am., The CryptoRights Found., Elec. Frontier Found., Privacy Activism, Public Info. Research, Privacy Journal, Privacy Rights Clearinghouse & World Privacy Forum, *Consumer Rights and Protections in the Behavioral Advertising Sector* at 4 (Oct. 31, 2007), *available at* http://www.ftc.gov/os/comments/behavioraladvertising/071115jointconsensus.pdf.

[9.] Even if deep packet inspection might conceivably be used for pro-consumer network management, protection for consumers in this area is essential. ISPs can in principle use deep packet inspection ("DPI") to scrutinize everything that consumers do on the Internet using the ISP's network. In addition, consumers typically only use one ISP for their broadband access (i.e., the broadband provider has a "terminating access" monopoly to that consumer in telecom terms), and would only be able to avoid deep packet inspection by that ISP by switching to another ISP entirely. Under some frameworks, DPI was

conducted so that information from consumers who had opted out was still sent to third parties who were engaged in behavioral targeting. Consumers concerned about this sharing could not avoid it except by switching ISPs.

[10] *See, e.g.*, Am. Acad. of Child & Adolescent Psychiatry, Am. Acad. of Pediatrics, Am. Psychological Ass'n, Benton Found., Campaign for a Commercial Free Childhood, Ctr. for Digital Democracy, Children Now, and Office of Commc'n, United Church of Christ, Comment at 13 (Apr. 11, 2008), *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080411childadvocacy.pdf (recommending voluntary industry guidelines that define "sensitive data" to include the online activities of all persons under the age of eighteen and prohibit the collection of sensitive information for behavioral advertising purposes); Consumer Fed'n of Am. & Consumers Union, Comment at 4 (Apr. 11, 2008), *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080411cfacu.pdf.

[11] *Compare* NAI, *2008 NAI Principles, Draft: For Public Comment* at 8 (Apr. 10, 2008), *available at* http://www.networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf (prohibiting use of information about children under 13 for behavioral advertising) *with* NAI, *2008 NAI Principles, The Network Advertising Initiative's Self-Regulatory Code of Conduct* at 9 (Dec. 16, 2008), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf (permitting use of information about children under 13 for behavioral targeting with parental consent).