Eliot Spitzer
Governor

STATE OF NEW YORK
EXECUTIVE DEPARTMENT
CONSUMER PROTECTION BOARD

Mindy A. Bockstein
Chairperson and Executive Director

February 14, 2008

BY E-MAIL AND OVERNIGHT MAIL
Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: Proposed Online Behavioral Advertising Self-Regulatory Principles

Dear Commissioners:

As New York State's top consumer watchdog, the New York State Consumer Protection Board ("CPB") is involved in a wide array of consumer issues. The CPB conducts consumer investigations, research and analysis; develops legislation, consumer education programs and materials; responds to individual complaints by working to settle disputes through voluntary agreements and represents the interests of consumers before the Public Service Commission and other State and federal agencies. In 2007, we handled an average of approximately 600 Internet-related complaints. Under Governor Spitzer, information privacy, the protection of consumers who communicate and conduct transactions online, and the maintenance of consumer trust in the online forum have become critical issues for the CPB. As behavioral advertising impacts all of these issues and, significantly, the preservation of consumer trust in the Internet, we write today to offer comment on the Proposed Online Behavioral Advertising Self-Regulatory Principles issued on December 20, 2007, by the Federal Trade Commission ("FTC").

Disclosure

In drafting the guidelines, the FTC broadly articulated the issues of concern in the behavioral targeting area, stating that "[t]he staff intentionally drafted the principles in general terms to encourage comment and discussion by all interested parties and further development of the principles based on the comments." We understand and agree with this approach. However, we urge the FTC to incorporate specificity in the final guidelines. For example, we support the comments submitted to the FTC on November 12, 2007, by the Center for Democracy and Technology ("CDT") and other privacy advocates urging the FTC to incorporate specific definitions of important terms, including but not limited to, "behavioral targeting," "sensitive data," and other key terms. Defined terms will promote consistent usage throughout and allow for better consumer protection through clear communication. Definitions will also result in clear

direction to industry and enhance compliance. Further, definitions will facilitate government and consumer oversight and enable more focused enforcement.

The need for clarity in this area is discussed and supported by survey data in the research report titled, *Consumers Fundamentally Misunderstand the Online Advertising Marketplace*, written by Joseph Turow, Deidre K. Mulligan and Chris Jay Hoofnagle (October 2007). The report, submitted to the FTC as public comment prior to the behavioral advertising conference, demonstrates that "[c]onsumers do not understand the nature and legality of information-collection techniques that form the core of online advertising business models." The report cites survey data indicating "that when consumers see the term 'privacy policy,' they assume the website cannot engage in many practices that, in reality, are common in ecommerce."

We further urge the FTC to issue guidance requiring uniformity in the communication of privacy promises across websites. We echo the sentiments of Professor Carlos Jensen of Oregon State University, who states, in comments submitted to the FTC on November 16, 2007:

> Requiring policies to address certain minimum sets of information would make them much more meaningful, and make consumers more likely to consult them. Such an online "nutrition label" should include, in a standard layout and [in] language clear and unambiguous[,] information on opt-in/opt-out mechanisms, what information sites collect, how it is collected, how it is processed and combined, how it is used, shared, or sold, and to whom. [Vague] [t]erms such as "trusted partners" and "general statistics" should be strongly discouraged.

All information privacy disclosures should be clear and conspicuous. With respect to standards for "clear and conspicuous" language, the financial privacy requirements of the Gramm-Leach-Bliley Act ("GLB") should be used as a guidepost. Under GLB, consumers are entitled to receive various financial privacy notices, including a "clear and conspicuous" opt-out notice prior to the sharing of any nonpublic personal information with certain third parties. Under the law, "clear and conspicuous" means that the notice must be "reasonably understandable" and "designed to call attention to the nature and significance of the information in the notice." Further, under GLB "reasonably understandable" means:

- Clear and concise sentences;
- Plain language and
- Using the active voice.

"Designed to call attention" means using:

- Headings;

- Easily read typeface and margins and
- Wide margins.

If the notice is posted on a website:

- Text or visual cues should be used to encourage scrolling down the page to view the entire notice;
- The notice should be placed on a frequently accessed page or via a clearly labeled link and
- There should be no distracting graphics or sound.

GLB Act, Public Law 106-102, 15 U.S.C. Sec. 6801 et seq., Title V, Subtitle A.

All of these concepts are translatable to the online advertising context. Accordingly, we urge the FTC to adopt the same approach to privacy policy and practices language in the final guidelines.

Once given full and robust disclosure of all privacy practices, including behavioral targeting practices, the consumer will be in a position to make an informed decision about his or her Internet usage, especially whether to consent to being a subject of behavioral targeting. The FTC should require a specific, uniform mechanism that is clear, easy-to-use and accessible, pursuant to which an informed consumer can exercise his or her choice. Further, a means should be in place to permit a consumer who subsequently changes his or her mind to opt-out after initially opting in.

Additionally, with respect to the practice of behavioral targeting, mere disclosure to a consumer visiting a site that this activity or practice will occur is not sufficient. Consumers need to be apprised of what behavioral targeting seeks to accomplish and the fact that, if they choose to consent to being targeted, profiles will be created with their tracked personal information. Further, there must be specific disclosure on exactly who will have access to this information, how it will be stored and for how long, whether or not the consumer will have access to it, for example, to modify or correct any entry, and what security precautions will be in place to safeguard the data.

Disclosure must also include the following:

- Specific information on the types of ads that could be served (for example, food, health-related or financial ads);

- How the choice to serve an ad will be made (for example, based upon location, or demographic information the consumer previously provided such as gender, age, income range or profession) and

- How behavioral targeting engaged in by the site could impact the terms of an offer made, such as cost (for example, through cost customization: offering an item at varying prices by monitoring a person's use of price-comparison sites to determine how much a consumer is willing to pay, and allowing a merchant to reconfigure costs accordingly).

To the extent consumers' tracked data will be used for purposes other than behavioral targeting, notice must specify for what purposes the data will be used. Further, consumers should be given the ability to choose whether or not to have their data used for other purposes, and to exercise this choice on an opt-in basis.

Further, a site engaging in behavioral targeting should be required to disclose to consumers its data retention period(s). If there are other entities involved in behavioral targeting in connection with any site, such as an advertiser or advertising network, the fact that these organizations may have different and possibly longer retention periods should be disclosed in a conspicuous manner.

With respect to requiring "reasonable security" for "collect[ed] and/or store[d] data," the guidelines are fairly specific, requiring that "[c]onsistent with the data security laws and the FTC's data security enforcement actions, such precautions should be based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable precautions available to a company" [citation to FTC's data security program and data security enforcement actions omitted].

We urge the FTC to require further that companies engaging in behavioral targeting disclose whether encryption will be used and for what types of data it will be used. Moreover, the FTC should consider making the use of encryption mandatory for certain types of data, such as sensitive or financial data, if these types are collected. There should also be required disclosure that, as in any situation involving the existence of a database, the possibility of a security breach exists.

Such conspicuous disclosure should be required not only in a site's privacy policy but also specifically flagged on the website itself, with a link to the appropriate provision in the site's privacy policy which would contain more detail. Vague terms should not be permitted. In addition, Internet access providers and search engines should make specific disclosure in this manner as well.

In the event a site materially changes privacy promises made with respect to a specific practice, a site should disclose this "clearly and conspicuously" on its website, linking to more detail. Consideration should be given to requiring sites to provide tailored notice to a consumer when visiting the site, if material changes have occurred since the consumer's last visit to the site. As stated by Professor Jensen, requiring a consumer constantly to check a privacy policy document to see if privacy policies have changed puts an undue burden on the consumer.

Further, data collected prior to a privacy practice change should be given special treatment. If this data will be subject to the changed practice, such disclosure must be made to the consumer before implementation. The consumer must be afforded the opportunity to give consent to the new manner in which his or her previously collected data will be treated through an opt-in procedure.

Sensitive Information

With respect to sensitive information (a term which we urge the FTC to define), we call upon the FTC to disallow or limit the tracking and collection of health information. To do otherwise would be inconsistent with the intent of the United States Congress, as demonstrated by the enactment of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA established, *inter alia*, *Standards for Privacy of Individually Identifiable Health Information* (the "Privacy Rule"). The Privacy Rule standards address the use and disclosure of individuals' health information, called "protected health information," by organizations subject to the Privacy Rule (health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form in connection with certain prescribed transactions). The Privacy Rule also sets standards to promote individuals' understanding of their privacy rights and to allow individuals to control how their health information is used.

A goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. It protects all "individually identifiable health information" (as defined), held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral ("Protected Health Information" or "PHI"). A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires, or (2) as the individual who is the subject of the information (or the individual's person representative) authorizes in writing. In defining the term "sensitive" information and in setting online advertising guidelines surrounding the tracking and collection of such data, we call upon the FTC to be guided by these protections extended by HIPAA's Privacy Rule.

Audits and Compliance Reports

We also support the call by the CDT and other privacy advocates for independent auditing and advertiser compliance reports. The FTC should require any organization engaged in behavioral tracking activities to provide independent auditing of its compliance with privacy standards. These results should be made public. Advertisers should be required to make annual compliance reports to the FTC. The FTC could then compile an aggregated report which could be used to assess the effectiveness of the self-regulatory scheme. Further, the FTC should issue annual reports to the public in this area.

Enforceability

Online behavioral targeting is powerful in ways beyond marketing. It shapes choices we make as a society and as individuals. "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," see comments of Dr. Mark Cooper, Director of Research, Consumer Federation of America, submitted to the FTC on November 16, 2007. Behavioral targeting has been attributed to the promotion of obesity in children, see *Interactive Food & Beverage Marketing: Targeting Children and Youth in the Digital Age,* Jeff Chester and Kathryn Montgomery, Berkeley Media Studies Group, 2007, and to the perpetuation of gender stereotypes, see comments of Jean Brownell submitted to the FTC, 10/19/07.

This powerful marketing technique must be regulated. While the guidelines when finalized will not be enforceable per se, it is our hope that the FTC will utilize them in the same manner it utilizes the *Dot Com Disclosures* (issued by the FTC in May 2000) (the "Dot Com disclosures"). The Dot Com disclosures provide guidance to businesses about how FTC law applies to online activities with a particular focus on the clarity and conspicuousness of disclosures in Internet ads. The final online advertising guidelines should be used by the FTC to determine when behaviorally targeted marketing does and does not violate Federal Trade Commission Act Section 5, for purposes of bringing enforcement actions. To do otherwise would result in the unequal application of consumer protection, as websites and advertisers that behaviorally target would be permitted to engage in practices that are inherently deceptive, secret and distort consumption. Further, this would flaunt FTC policy as articulated by the FTC in a staff working paper titled, *Dot Com Disclosures: Information about Online Advertising*:

> The same consumer protection laws that apply to commercial activities in other media apply online. The FTC Act's prohibition on "unfair or deceptive acts or practices" encompasses Internet

advertising, marketing and sales. In addition, many Commission rules and guides are not limited to any particular medium used to disseminate claims or advertising, and therefore, apply to online activities.

Conclusion

Technology is advancing at a pace never before seen in our history, and although there are many benefits, government should act to ensure that the public's fundamental right to privacy is not abridged. Failure to act may result in a chilling effect.

Thank you for your consideration of these comments.

Sincerely,

Mindy A. Bockstein

Mindy A. Bockstein
Chairperson and Executive Director

5 Empire State Plaza, Suite 2101, Albany, New York 12223
Tel: 518-474-3514 ▪ Fax: 518-474-2474

1740 Broadway, 15th Floor, New York, New York 10019
Tel: 212-459-8850 ▪ Fax: 212-459-8855

Consumer Hotline 800-697-1220

www.nysconsumer.gov