Consumer Federation of America

April 11, 2008

Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue NW
Washington, DC 20580

RE: Behavioral Marketing Principles

Dear Mr. Clark:

The Consumer Federation of America (CFA), an association of more than 300 nonprofit consumer organizations, has since 1968 sought to advance the consumer interest through research, education, and advocacy. Consumers Union (CU) is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance. Consumers Union's income is solely derived from the sale of *Consumer Reports*, its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* with approximately 5.8 million paid circulation, regularly carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions that affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

CFA and CU offer the following comments to the Federal Trade Commission (FTC) concerning the Proposed Online Behavioral Advertising Self-Regulatory Principles issued by the FTC on December 20, 2007.

Principles are not enough

We believe that the proposed principles are useful to articulate the consumer concerns that were raised during the Town Hall meeting on behavioral advertising that the FTC held on November 1 and 2, 2007 and promote further discussion about how to address those concerns. Later in this submission we will make specific recommendations about how best to approach the issues that are raised by these principles. However, as a general matter, we would like to state at the onset that consumers cannot be adequately protected by self-regulatory principles and general FTC enforcement powers.

The evidence presented at the Town Hall meeting not only demonstrates the failure of the current voluntary approach but the inevitable inability of poorly defined

principles to protect the public. There is a deep-seeded failure in the online advertising/marketing space that cannot be addressed by half measures.

Simply put, there is a fundamental mismatch between the technologies of tracking and targeting and consumers' ability to exercise informed judgment and control over their personal data. The result is that consumers suffer a persistent and substantial disadvantage vis-à-vis marketers.

It is clear 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.

The industry focuses its efforts on providing a sliver of the population that has the necessary characteristics to exercise choice enough of an option to be placated and silent, while the vast majority of consumers are exploited. In the technological battle with online advertisers, the consumer is outgunned. We need policy to ensure the consumer is protected and can effectively exercise choice.

We reach this conclusion by combining key facts that were brought out at the Town Hall meeting. 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), but we know that each click dissuades a significant percentage of consumers from taking action. 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 at the Town Hall meeting 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.

Furthermore, many consumers who see privacy policies simply assume that this means that their information is not shared with others and that it is not combined with information about them obtained from other sources. When online behavioral tracking and targeting is explained to them in simple terms, a significant number reject it if their

only choices are to agree in order to get content from the site or to pay for the site and not have their information collected.[1]

We find multiple and diverse advertisers and partners with different privacy, data gathering and marketing policies on individual pages and within individual sessions, each of which requires a separate action by consumers to protect themselves and for which there is no immediate and clear notice of the information that is being tracked or how it will be used.

We saw survey evidence of a huge gap between what consumers want and what marketers think they deserve.[2] 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.

As a result, the gathering of the data is not subject to meaningfully informed consent and the use of the data is surreptitious. It circumvents consumer defenses to the detriment of the consumer.

Privacy is a right to be protected, not a harm to be avoided

Much of the discussion at the Town Hall meeting about what privacy protection should and should not do in the online advertising market was based on a mischaracterization of the moral basis of privacy. Consumer privacy is a right to be protected, not a harm to be avoided. The notion that privacy is a human right goes back centuries. In modern times, it is found in the 1948 United Nations Declaration of Human Rights [3] and in many international conventions and treaties.

Of course, privacy is not just a moral issue. 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 they distort consumption. The inherently deceptive practices that pervade the behavioral marketing space include suggestions of relationships that do not exist and use of

---

[1] Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace, Joseph Turow, Deirdre K. Mulligan, Chris Jay Hoofnagle, University of Pennsylvania Annenberg School for Communications and UC Berkeley Law's Samuelson Law, Technology & Public Policy Clinic, October 2007, http://www.law.berkeley.edu/clinics/samuelson/annenberg_samuelson_advertisiing-11.pdf

[2] FTC Presentation on Cookies & Consumer Permissions, Dr. Larry Ponemon, Ponemon Institute LLC, http://www.ftc.gov/bcp/workshops/ehavioral/presentations/3lponemon.pdf

[3] "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." http://www.un.org/Overview/rights.html

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," a hot topic at the Town Hall meeting, 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 reacting to major data breaches, the FTC has little capacity to monitor or detect the extent of these harms.

Choice is good for consumers and advertisers

We also heard a series of dubious claims at the Town Hall meeting 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, but a well-crafted consumer privacy protection scheme will support competition and efficiency in an expanding advertising market. Advertising will continue and improve within the parameters that public policy sets.

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 socially responsible direction. Judging from what happened in response to creating the national "Do Not Call" registry, the market will split between those who want and need a simple, single consumer-friendly way to block behavioral tracking and those who will be more selective choosing privacy protection.

The FTC must take a stronger approach to the problem

Behavioral tracking for the purposes of targeting online advertising and marketing is an invasion of privacy and an inherently deceptive practice that must be closely regulated under the FTC's authority. The voluntary principles that the FTC has proposed are wholly inadequate to protect the public's right to privacy and prevent consumer detriment.

The FTC should adopt and enforce a mandatory program of consumer privacy protection that adheres to a stronger set of principles.[4] This must include:

(1) A simple consumer-friendly interface that facilitates the choice not to be tracked across all platforms to be implemented.

(2) 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 definitions that consumers can understand.

(4) Enforcement that has "teeth" to ensure compliance, 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.

Self-regulatory programs can be useful to encourage industry members to meet and even exceed their obligations, but they should not be substituted for a strong legal consumer protection framework.

Definitions are needed

Definitions are essential to provide clear rules of the road for industry members. These definitions should include:

[4] See Joint comments by the Center for Democracy and Technology, Consumer Action, Consumer Federation of America, Electronic Frontier Foundation, Privacy Activism, Public Information Research, Privacy Journal, Privacy Rights Clearinghouse, and the World Privacy Forum, October 2007, http://www.worldprivacyforum.org/pdf/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf

a. Personally Identifiable Information. Personally identifiable information (PII) consists of any information that can, directly or indirectly:

(1) identify an individual, including but not limited to name, address, IP address, SSN and/or other assigned identifier, or a combination of unique or non-unique identifying elements associated with a particular individual or that can be reasonably associated with particular individual, or

(2) permit a set of behaviors or actions to be consistently associated with a particular individual or computer user, even if the individual or computer user is never identified by name or other individual identifier. Any set of actions and behaviors of an individual, if those actions create a uniquely identified being, is considered PII because the associated behavioral record can have tracking and/or targeting consequences.

b. Non-Personally Identifiable Information. Non-Personally Identifiable information (Non-PII) is:

(1) aggregated data not associated with any individual or any individual identifier, or

(2) any individual level data that is not PII.

c. Behavioral Tracking. Collecting and compiling a record of individual consumers' activities, interests, preferences, and/or communications over time.

d. Behavioral Targeting. Using behavioral tracking to serve advertisements and/or otherwise market to a consumer based on his or her behavioral record.

e. Sensitive Data. Any PII about health, financial activities and account numbers, political activities, sexual behavior or sexual orientation, social security and other government-issued ID numbers, and children under age 18.

f. Internet Access Provider. Any service providing network connectivity, including but not limited to an Internet service provider (ISP).

Transparency

The proposed principle for disclosing that consumer data is being collected on a Web site for behavioral advertising purposes does not provide adequate assurance that consumers will receive that information in a meaningful and contextual manner. Since consumers do not realize that behavioral tracking may be occurring, it is not sufficient to simply put a link at the bottom of the home page to a statement that provides that disclosure. The average consumer would be unlikely to look for or click on such a link. Yet nothing in the principle proposed by the FTC suggests that this important disclosure should be made in a way that is any different than the manner in which privacy policies are typically presented – policies that are acknowledged to be largely unread.

Providing the disclosure in a "clear, concise, consumer-friendly, and prominent statement," as the FTC proposes, is not enough, because it is unclear what "prominent"

means here. Would simply highlighting this information within a privacy policy be adequate? Should there be a separate statement about behavioral targeting? At what point(s) should this important disclosure appear? Our view is that this information will be most useful to consumers at the time that they first take an action that triggers the possibility of their data being collected and that the notice must be pushed out to them, rather than expecting them to look for it. Of course, the information should also be included in the privacy policy. The FTC should specifically require the disclosures to be *clear, concise, consumer-friendly, timely, contextual, and robust.*

It is also important to require disclosures to be more specific than the vague statements that are usually provided in privacy policies (i.e. we will share your information with our family of companies and others whose products or services might interest you).

For consumers to make informed choices based on these disclosures, they need to know:

- What kinds of data are being colleted;
- What factors are likely to be used;
- What types of ads are likely to be delivered to them;
- What the impact of collecting the data might be in terms of actions such as price differentiation;
- How long the data will be retained;
- How the data will be safeguarded;
- What access they have to the data; and
- Who else has access to the data, including the fact that it may be accessible to civil litigants or law enforcement agencies.

Furthermore, the FTC should require the disclosures to explain exactly what options consumers have for allowing their behavioral data to be collected and used, deleting data that they no longer want to be used, and stopping their data from being collected later if they choose.

Details could be provided in a layered manner as long as essential information – that behavioral tracking is taking place, for what purpose, and what options consumers have for control – are clearly spelled out upfront. Finally, there should be a direct link from the disclosure to the mechanism for exercising consumers' options.

Consumer control

The proposed principle falls far short of giving consumers meaningful, effective control of their privacy because it would require them to opt-out at each Web site they visit at which such tracking is taking place. CFA, CU and other consumer and privacy groups believe that it is essential to provide consumers with more control and easy-to-use

tools. Among them should be a national "Do Not Track" registry similar to the national "Do Not Call" registry.[5]

Any advertising entity that sets a persistent identifier on a user device would be required to provide to the FTC the domain names of the servers or other devices used to place the identifier. Companies providing Web, video, and other forms of browser applications would provide functionality (i.e., a browser feature, plug-in, or extension) that allows users to import or otherwise use the "Do Not Track" registry of domain names, keep the registry up-to-date, and block domains on the registry from tracking their Internet activity.

Advertisements from servers or other technologies that do not employ persistent identifiers would still be displayed on consumers' computers. Thus, consumers who sign up for the "Do Not Track" registry would still receive advertising.

The "Do Not Track" registry would be available on the FTC Web site for download by consumers who wish to use the list to limit tracking. We would expect the FTC to undertake broad educational efforts aimed at both consumers and industry members about the "Do Not Track" registry and how to use it. It would also be important for the FTC to actively encourage all creators of browsing and other relevant technology to incorporate facilities that would enable consumers to use the registry.

As with the "Do Not Call" registry, not all consumers would choose to use the "Do Not Track" registry. Consumers should also have the right to decide on a case by case basis to allow their information to be used for behavioral tracking, but in no case should collection of "sensitive data" be permitted. At the Town Hall meeting, industry members and consumer advocates all agreed that consumer control was paramount to acceptance of behavioral advertising. We believe that giving consumers real control means that consumers get to make the decision. Consumers' comments to the FTC in response to the proposed principles indicate that the favored approach may be opt-in.[6]

Whatever the method is for exercising consumer control, we agree that it should be easy-to-use and accessible. It might be helpful to expand on what is meant by accessibility. We believe that accessibility means that the method to exercise control is free, one-click away, and can be used by consumers regardless of their physical abilities and the types of computers and Internet access they have.

Another issue that was highlighted during the Town Hall meeting was that sometimes consumers' preferences do not persist over time because systems are not

---

[5] See comment by Mike Wall, http://www.ftc.gov/os/comments/behavioraladprinciples/071220wall.pdf

[6] See comments from Charles Cooper, Mark Harper, and Ben Madden, http://www.ftc.gov/os/comments/behavioraladprinciples/080320cooper.pdf, http://www.ftc.gov/os/comments/behavioraladprinciples/071222hammond.pdf, http://www.ftc.gov/os/comments/behavioraladprinciples/080225madden.pdf

always designed to ensure that they do. There should be a requirement that consumers' choices will be honored and will persist until and unless they change them.

Reasonable security, and limited data retention, for consumer data

All PII should be required to be reasonably secured. Consumers' data should not be retained any longer than is needed for the purpose that was disclosed to them or that may be legally required. Indeed, there should be no reason to retain the information for long periods of time, since one can reasonably assume that consumers will return to the Web sites frequently and that relatively fresh information is more useful than old data.

It is also important to require that if the data is shared with others, they should be under the same obligations to limit use for the stated purpose, provide reasonable security for it, and follow the same retention policy. Furthermore, if sensitive data is allowed to be collected, there should be a requirement to notify affected consumers if a breach occurs. This is important because consumers may have no direct relationship with the data user and would not be able to learn about the problem in a timely fashion otherwise.

Sensitive Data

We believe that sensitive data should *not* be allowed to be collected because the risk of harm is too great when lapses in security or misuse, which are inevitable, occur. While errant companies may be subject to legal action, it is difficult to put the genie back in the bottle once sensitive information is exposed.

If there is no prohibition against collecting sensitive data for behavioral tracking and targeting, consent *must* be on an opt-in basis and the information *must* be encrypted.

Affirmative express consent for material changes to existing privacy promises

We would support a requirement that consumers be given advance notice and asked to opt-in to continue to allow their data to be used if the way that it will be handled or protected is slated to change.

Access to data

Those collecting behavioral data should be required to provide consumers with access to PII and other information that is associated with PII retained by the advertiser for behavioral tracking and targeting uses.

Using data for purposes other than for online advertising

At the Town Hall meeting, questions about whether and how behavioral tracking data was used for purposes other than for online advertising went unanswered. This is a very important issue, because disclosures to consumers and the choices they make based on them are meaningless if they do not have all of the information they need about what

is happening with their data. Is information about consumers collected offline being combined with consumer data collected online, and vice versa? For what purposes?

These questions must be answered so that the FTC can address the consumer protection issues related to behavioral tracking and targeting comprehensively. The FTC may wish to convene another workshop or initiate a proceeding on just this subject to gather more information on this issue.

Adverse action against consumers should be prohibited

Another concern that must be addressed is the potential for consumers to be prevented from accessing a Web site or subject to some other adverse action – for instance, being charged more for goods or services – if they decline to allow their data to be tracked for behavioral targeting.[7] This should be expressly prohibited. Advertising that is more relevant to consumers should bring them additional benefits, but benefits that consumers would normally expect to receive should not be withheld for failure to participate in behavioral tracking and targeting.

Transparent reporting of industry compliance is needed

To monitor whether the requirements that are placed on industry in regard to behavioral tracking and targeting are being met, the FTC will not be able to rely on consumer complaints, since consumers may be unaware that their information is being tracked when they have not consented to that or is being used in ways other than what they were led to believe. Any organization engaged in behavioral tracking activities must be required to have independent auditing of its compliance with privacy standards.

Audit results must be public, except for bona fide trade secrets and PII about consumers. All audits of a self-regulatory entity or the advertising industry at large should be conducted by a neutral third party, and should be made public in their entirety, not in a condensed form. Consumer complaints to the self-regulatory entity or industry body with company identification should be public, redacted of consumers' PII. Alternatively, consumer complaints may be added to the FTC Consumer Sentinel database provided that the company information remains subject to public disclosure.

Advertisers should make full annual compliance reports to the FTC. The FTC should produce an aggregated report (i.e., an Annual Consumer Advertising Protection Report) on the effectiveness of any self-regulatory scheme. The FTC should report annually on the number of companies that are in self-regulatory safe harbors as well as the total number of companies in the industry doing any type of behavioral tracking or targeting.

Enforcement

[7] See comment by Pastor Andy Logan, http://www.ftc.gov/os/comments/behavioraladprinciples/071220logan.pdf

Relying solely on a self-regulatory approach would make it difficult for the FTC, state attorneys general, and consumers themselves to take effective enforcement action against errant companies. Some companies engaged in behavioral tracking and targeting will decide not to voluntarily adopt the FTC's proposed principles, some may implement policies and procedures that are not consistent with those principles, some may not disclose what their policies and procedures are, and some may do little or nothing to address the concerns that have been raised.

Furthermore, not all companies will join a self-regulatory program, and even for those that do, the action such programs can take if members violate their commitments is limited to asserting peer pressure, revoking their membership, and asking the FTC to investigate. There are no penalties for not participating in a self-regulatory program or for leaving one, voluntarily or involuntarily. As the FTC correctly stated in its 2000 report to Congress about online profiling, "Self-regulation cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program."[8]

Moreover, it is difficult to know what actions self-regulatory organizations have taken and assess their effectiveness. According to the recent report by the World Privacy Forum about the National Advertising Initiative, it is difficult even to find basic information about how many complaints that program received and exactly what happened with them.[9] There is no evidence of any action against member companies.

Without a requirement that companies that engage in behavioral tracking and targeting must have policies that meet or exceed certain standards and publicly disclose them, meaningful enforcement is difficult. Each company must be responsible for its own policies and be held legally liable for adhering to them.

The FTC should establish a national "Online Consumer Protection Advisory Committee"

The FTC should establish a consumer protection advisory committee that would include representatives from offices of state attorneys general, state and local consumer privacy and consumer protection officials, and consumer and privacy-focused nonprofit organizations. The advisory committee would hold regular meetings to evaluate changes in the advertising and consumer marketing sector, including but not limited to new technologies and other changes impacting consumers. The committee would review detailed audit reports from advertisers and industry, and would report problems and suggest solutions to the FTC. The committee should have the ability to hold hearings, and to report its findings to Congress, the FTC, and the public.

[8] Online Profiling: A Report to Congress Part 2 Recommendations, July 2000, page 10, http://www.ftc.gov/os/2000/07/onlineprofiling.pdf

[9] The National Advertising Initiative: Failing at Consumer Protection and at Self-Regulation, November 2007, http://www.worldprivacyforum.org/pdf.WPF_NAI_report_Nov2_2007fs.pdf

Conclusion

The existing marketplace creates a race to the bottom where the most invasive companies will succeed and consumers will not have effective options – assuming that they are even aware of the fact that they are being tracked. Companies engaged in behavioral tracking and targeting have no real incentive to adopt the FTC's principles, since their activities are invisible, so only the best are likely to do so.

On the other hand, as we noted previously, a well-crafted consumer privacy protection scheme can spur competition and efficiency, and improve advertising to better serve the needs of consumers who want to receive it.

We hope that the FTC will take stronger steps to protect consumer privacy and is committed to working with the agency and others to achieve that aim.

Sincerely,

Mark Cooper
Research Director
Consumer Federation of America

Susan Grant
Director of Consumer Protection
Consumer Federation of America

Chris Murray, Senior Counsel
Consumers Union