Comments regarding the FTC Town Hall Meeting on Behavioral Advertising,
Ehavioral Advertising: Tracking, Targeting, and Technology
by
Center for Digital Democracy, Center for Democracy and Technology, Consumer Action, Consumer Federation of America, Privacy Rights Clearinghouse, Privacy Times, Public Information Research, World Privacy Forum
to:

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

Via email

October 19, 2007

The Center for Digital Democracy, Center for Democracy and Technology, Consumer Action, Consumer Federation of America, Privacy Rights Clearinghouse, Privacy Times, Public Information Research and the World Privacy Forum are pleased to submit comments to the Federal Trade Commission (FTC) regarding its Nov. 1-2 Town Hall Meeting on behavioral advertising.[1] Our comments take the form of questions that we have regarding behavioral targeting and other aspects of the digital advertising sector. We understand that the FTC has been looking at the behavioral targeting marketplace in detail, so it is our expectation that the November Town Hall meeting will provide the answers to these questions.

I. General Questions Surrounding Behavioral Targeting and Profiling

- Modern definitions of personal information or personally identifiable information (PII) recognize that identifiability is no longer dependent upon traditional data such as the Social Security Number, date of birth, and name. Is the Network Advertising Initiative (NAI)[2] definition of personally identifiable information

[1] *See* FTC Ehavioral Advertising Town Hall Meeting, <http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml>. (Last visited October 18, 2007).

[2] The NAI is a self-regulatory group whose members have agreed to abide by the NAI Self-Regulatory Principles for online preference marketing by network advertisers. See <http://www.networkadvertising.org/pdfs/NAI_principles.pdf> and <http://www.networkadvertising.org/>.

tenable today, in light of the fact that individuals can be effectively identified through non-personally identifiable information?[3]

- How will industry ensure that new competitors, or existing competitors using a new type of tracking method or business model, be accountable under a self-regulatory regime?

- What health or other sensitive information is collected as part of behavioral targeting, and what are the objective criteria for determining what constitutes sensitive data in any area? How are the criteria applied across the industry?

- What do industry patent applications indicate about the future of profiling in this field?

- How long must information be retained in identifiable form for effective behavioral targeting?

- What metrics will be applied to evaluate the success of a self-regulatory initiative, and what actions will be taken if the initiative is unsuccessful?

II. Questions Regarding Collection of Information

- What information is collected?
    - Unique identifier(s)
    - Contact information
    - Demographic information
    - Behavioral (as in previously viewed sites, interests, and preferences)
    - Behavioral (as in how one interacts with a page, how far an individual scrolls down, etc.)
    - Behavioral (as in lifestyle, purchasing habits, purchasing frequency)
    - Location information
    - Other

- Is the collection of information so broad now that it does not matter what specific PII is being collected? That is, are the advertisers' pictures of consumers so detailed that they in effect have what amounts to PII, even if they are not collecting PII as defined by the NAI?

    - For instance, in the 2006 AOL data breach, individuals were identified within the company by a unique number, which was then disclosed online along with some of the individuals' search history. Newspaper reporters and others were able to identify some of the individuals by name, even

[3] *See* NAI definition of PII: "Personally Identifiable Information (PII) is data used to identify, contact or locate a person, including name, address, telephone number, or email address." <http://www.networkadvertising.org/managing/faqs.asp>. (Last visited October 18, 2007).

though these individuals were initially identified only by a number.[4] Given that individuals were rendered personally identifiable by a limited collection of their search terms, how does the sheer scope and amount of information collected by behavioral targeting advertising companies impact the definition of PII?

  - What happens when an advertiser incorrectly identifies an individual's preferences, lifestyle, or other factors in a predictive or other targeting profile because the collection of data accrued from multiple individuals using one or more shared devices (such as a computer or mobile phone) or because of other shortcomings or errors in the collection process?

  - How does the information collected about individuals impact those individuals? For example, do individuals with different web browsing patterns also have different opportunities offered to them, opportunities that may have the potential to impact their quality of life, such as differing offers of credit, and so forth? What studies has the FTC done on the impact of behavioral targeting on individuals with varying behavioral profiles?

- How long is consumer data retained?

- What technologies are employed in this collection?
  - Cookies
    - What about cookies stored in the browser cache?
  - Web bugs
  - Javascript
  - Flash cookies
  - Browser history and bookmarks
  - RSS
  - Non-browser-based information collection
    - Such as tracking in Digital Rights Management (DRM) systems
  - Or variations on the standard use of the above technologies?
  - Other persistent identifying elements?

- Are there special considerations for data that might be sensitive?
  - Health web sites
  - Other health-related web browsing activities
  - Sensitive financial information
  - Pornographic web sites
  - Sensitive identifiers, such as the Social Security Number or other government issued-identification

[4] Michael Barbaro and Tom Zeller Jr., "A Face Is Exposed for AOL Searcher No. 4417749," New York Times, August 9, 2006.

- How can NAI's standards accommodate new technologies?
    - The NAI principles have not changed in seven years, but the entire digital advertising landscape has changed dramatically. Where are the incentives for NAI's members to address new problems, and in a timely manner?[5]

III. Questions Regarding Linkage

- Is there multi-channel linkage of information? For example, will the day come when a keyword search on a search engine will trigger a customized ad within a video game that consumers are playing on a game console?

- Is there multi-platform linkage? For example, if a consumer uses personal and work computers to access the same web sites or other content, can the consumer's personal and work activities be linked?

- Is online data enhanced with information from third parties?
    - Is information collected offline ever combined with online data (whether from third parties or otherwise)?
    - Are consumers ever informed about the use of third party information?

- Some companies quietly track a user with the ultimate purpose of presenting the user with an opportunity to divulge personal information, for example, in a quiz or survey, perhaps without disclosing to the user how the new information might be linked with other data. What begins as anonymous tracking is intended to result in a rich behavioral profile that is identifiable. Is it possible to reject this practice and divorce identifiable systems from tracking?

- Commercial databrokers, for example, Acxiom, have announced behavioral targeting programs that rely on detailed profiles of consumers linked with targeted advertising on web sites.[6] Acxiom is apparently not a member of NAI and does not apparently offer an NAI opt-out cookie. Since the online-offline linkage is occurring within one company, how can consumers be told about and protected from both the linkage and the targeting? Where is the recourse for consumers in this business model?

- What recourse do consumers have when desiring to opt out of linked information from companies who are not members of the NAI?

---

[5] *See*: "Advocacy: As online marketing continues to grow and new marketing technologies evolve, the NAI will remain a vigorous advocate for consumer privacy and responsible online marketing standards and practices and will remain committed to consumer education," available at <http://www.networkadvertising.org/managing/>. (Last visited Oct. 3, 2007).

[6] *See*: *Acxiom Brings Better Predictive Insight to Interactive Ad Targeting with Relevance-X Solutions,* Press Release Oct. 16, 2007. < http://www.acxiom.com/default.aspx?ID=3160 >. (Last visited October 18, 2007).

IV. Questions About Decision Making

- How are the data being used?
    - Ad delivery
    - Site optimization
    - Product recommendations
    - Price discrimination/customization
    - Content customization/personalization
    - Sale of data/profiles to data brokers, other companies
    - Predictive decision making about who should receive offers of credit, insurance, or other offers or products?
    - Redlining
    - Other?

- What new business models can we expect to emerge?

- What kinds of segments or demographic groups are being created and/or used by the behavioral targeting advertising companies? Are these segments demographic, behavioral, or a combination? It is well established that companies such as Claritas and Acxiom have products that segment consumers or households into highly defined demographic groups such as *Young Digerati*, *Upper Crust*, or *Gray Power*.[7] What kinds of categories are being used across the behavioral advertising sector? Are these categorizations made available to consumers for their perusal, and are consumers informed of which category they are placed in? What impacts do these categorizations and segmentations have on consumers?

- Inferences from segmentation and other behavioral profiling may not be defined as PII by the current NAI, even though the inferences may directly affect what consumers see and what opportunities are presented to them. What rights do individuals have to limit the use of these inferences, access them, and correct them?

- Is there any oversight by any public or private organization of potentially discriminatory uses of behavioral preference marketing?

V. Questions About User Control/Welfare

- How do behavioral advertisers' practices fit in with Chairman Majoras' idea (in the spyware context) that third parties are not free to help themselves to the resources of individuals' computers? Are there techniques for behavioral

---

[7] *Ibid.* Acxiom states that it places "each U.S. household into one of 70 unique clusters and 21 different lifestages based on that households' specific consumer and demographic characteristics, including shopping, media, lifestyle, and attitudinal information." Claritas also creates profiles, including behavioral profiles. See Claritas MarketPlace NET- Behavioral Profiles <http://www.claritas.com/claritas/Default.jsp?ci=3&si=2&pn=mybestprofiles>.

marketing practices that rely on the user's computer facilities? What are these techniques or practices?

- Is notice given?
  - When?
  - How often?
  - Are users aware of the sophistication of these systems?
    - How can the nuances of behavioral profiling be presented so that individuals can understand these systems?
  - The terms *clear* and *conspicuous* are used many times in the NAI in the context of notice. How does the NAI define these terms?
  - What opportunities are there for notice in real time, to expose the presence of web bugs/beacons/pixel tagging? That is, how do consumers get additional notice, outside the privacy policy? How can NAI promote visible notice?
  - Should companies expressly disclose each technical measure used to track users, along with instructions on how to avoid the measures?

- What choices are available to consumers?
  - Opt in/opt out
    - How do we make opt-in fair and effective, for example, by not denying access to a website unless a user opts-in?
    - How can choice be dealt with across platforms? Solutions should work on all major platforms.
    - Can the behavioral targeting community work with web browser developers to build a robust consumer choice mechanism into their browsers? Will all companies making browsers, including large companies, be willing to support robust consumer choices?
    - Will opt-outs and privacy notices as well as other robust notices be accessible to those with disabilities?
  - Can consumers control the types of ads they see, for example, block all pornographic ads, or ask for more car ads?
  - Currently, a number of tools allow advanced users to avoid advertising (Adblock, Privoxy, Noscript). Some of these tools already disable features with content (i.e., blocking Javascript breaks many sites). Will users still be able to get content in the future if they block cookies, scripts, etc?

- Can consumers access and correct their profiles? How does this work in a meaningful way?

- Is overpersonalization occurring? Is there a limit to user desire for or tolerance of personalization, just as there was a limit to banner advertising?

- In what manner are profiles stored?
  - Anonymously

- Identifiably
- Pseudonymously

- Is information being collected for no immediate purpose or use, but simply kept for some future, unforeseen use?

- Law enforcement implications of data release
  - Have behavioral advertising companies received subpoenas or other requests from law enforcement agencies to obtain consumers' profile data?

VI. Education

- The NAI (§5) says that covered companies will perform both business and consumer outreach to educate the public about online profiling. What have NAI companies done to promote education in this area, including neutral, unbiased information?

- Are there efforts to determine how effective such outreach has been?

VII. Enforcement/Oversight Questions

- How should we deal with the ephemeral nature of self-regulatory groups, such as the NAI, the Online Privacy Alliance, and the Individual Reference Services Group?[8] How do we ensure that any future self-regulatory structure is sound and functioning robustly after the FTC has finished its inquiry into the issues?

- How should we deal with the changing nature of practices and technologies? How frequently should the FTC revisit consent agreements?

- The Do-Not-Call list[9] did not work as a self-regulatory initiative, so the FTC took its operation over. Should there be a similar approach here?

- Are NAI audits currently conducted by an independent, neutral third party? Are the NAI audits published in granular detail for perusal by consumers? Are audits that are highly redacted and generalized a useful oversight mechanism? Is TRUSTe an independent, neutral third party auditor for a self-regulatory body?[10]

---

[8] For Online Privacy Alliance see <http://www.privacyalliance.org/>. To view the IRSG web site (www.irsg.org) when it was operated by the IRSG self-regulatory group, see <http://web.archive.org/web/*/http://www.irsg.org>.

[9] *See* National Do Not Call Registry page at the FTC, <http://www.ftc.gov/donotcall>.

[10] *See* <http://www.truste.org/>.

- Where are the detailed public reports about the NAI? Are the TRUSTe "watchdog reports" the only reports on the NAI available to the public?[11] What has the NAI done to educate the public about the availability of its audits?

- Should complaints about the NAI go to the FTC Consumer Sentinel Database?[12]

VIII. Conclusion

Thank you for the opportunity to submit comments on these issues, which are of great interest and importance to consumers. We look forward to learning the answers to these and other questions at the November Town Hall meeting.

Respectfully submitted,

Center for Digital Democracy
Center for Democracy and Technology
Consumer Action
Consumer Federation of America
Privacy Rights Clearinghouse
Privacy Times
Public Information Research
World Privacy Forum

[11] *See* < http://www.truste.org/consumers/watchdog_reports.php>.
[12] *See* <http://www.ftc.gov/sentinel/index.shtm>.