



**TRUSTe Comments**  
**FTC Staff Proposed Principles for Behavioral Advertising**  
**March 2008**

TRUSTe recognizes that online advertising is fuelling the development of rich new consumer experiences. While data collected to target ads can be very useful to enhance consumer experience and support services, important privacy considerations are posed by the collection, use and storage of this data. Consumers have the right to know how their data is being used and control its use.

TRUSTe believes that behavioral advertising can be performed in a responsible and beneficial manner, but only if the businesses involved take full stock of the privacy implications of the practice, and build a transparent and protective consumer experience.

We are pleased that industry has begun to explore self-regulatory actions to address consumers' behavioral advertising concerns. We welcome the work done by the FTC staff to develop principles as a way to drive these efforts, and we are pleased to provide the following commentary.

TRUSTe's founding mission was to provide notice and choice to consumers on the internet regarding the collection and use of their personal information. A decade later, new models continue to emerge that test the Fair Information Principles and our own self-regulatory principles. The evolution of our program requirements and development of new certification and enforcement models to meet emerging practices and business models, such as the Trusted Download program, inform our viewpoint on behavioral advertising.

In line with our mission, TRUSTe has begun to initiate a discussion among industry leaders to coordinate an online consumer education effort which would include developing instructional materials, and leverage TRUSTe sealholders to guide concerned consumers to an educational program.

In general we will apply three main themes in our comments regarding behavioral advertising:

1. **Education:** the need for consumer education on behavioral advertising;
2. **Accountability:** that all commercial beneficiaries, where appropriate, should be accountable in providing education, notice and choice to consumers
3. **Proactive Notice:** that notice for targeting should be pushed to the consumer wherever feasible and that a sliding scale approach should

be used depending on the practices and potential harm to consumer privacy.

## **I. Proposed Principle: Transparency and Consumer Control**

*Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option.*

TRUSTe strongly agrees that there is a need for greater transparency and consumer control related to behavioral advertising. In behavioral advertising, pseudonymous information<sup>1</sup> is collected and combined with other pseudonymous and anonymous<sup>2</sup> information, including web sites visited, specific pages viewed, search terms, and other elements, to create a profile, often linked by an individual identifier, such as a unique ID stored in a cookie. These profiles are used to approximate an individual's interests, or more accurately, an aggregation of interests corresponding to the user(s) of a specific computer, for the purposes of ad targeting.

TRUSTe's survey of more than 1,000 consumers, conducted in February of 2008<sup>3</sup> shows that more than 70% of consumers are aware that their online activities may be tracked by third parties for the purposes of targeting advertising. When asked if they are comfortable with advertisers using their browsing history to target advertising 57% say they are not comfortable even when it is not tied to their name or any other personal information.

When developing the requirements for certification of downloadable software in our Trusted Download Program (TDP) we concluded that participants, including those whose software is used for behavioral advertising, must provide consumers clear notice and the ability to opt out of collection and use of pseudonymous or anonymous data for marketing purposes.<sup>4</sup> Behavioral advertising raises privacy issues generally similar to those raised by

---

1. The term "Pseudonymous Information" means information that may correspond to a person, account or profile but is not sufficient, either on its own, or through combination with other easily accessible public information, to identify, contact, or locate the person to whom such information pertains. Examples include, but are not limited to, a User's IP address, machine ID, and the web pages a user views.

2. "Anonymous Information" means information that does not fall within the definition of either Personally Identifiable Information or Pseudonymous Information. "Anonymous information" includes but is not limited to aggregate information.

3. 2008 Study: Consumer Attitudes About Behavioral Targeting  
[http://www.truste.org/about/press\\_release/03\\_26\\_08.php](http://www.truste.org/about/press_release/03_26_08.php)

4. The Trusted Download Program Requirements are available at  
<http://truste.org/trusteddownload.php>.

downloadable software, and we assert that consumers should be provided with similar levels of notice and control over their data.

We do not believe that notice and choice obligations should be designed in a manner that would stop all mainstream behavioral advertising and the services that rely on them, in their tracks. Notice and choice obligations should be tiered in a sliding scale manner, with sensitivity of the data collected and perceived privacy impact of the use to the consumer being the controlling variables. Both of these attributes are captured in the potential harm equation discussed below. At a minimum, notice should be provided in the privacy statement. Since we know consumers' primary purpose on websites is not to read legal notices but to browse, engage, and transact, we suggest that there are a variety of additional ways for websites to provide notice.

The level of transparency and control required should be directly related to the possible harm. It is a well established position in law that the burden to mitigate a risk be in relation to the amount of potential harm. Where the sensitivity of the data and the likelihood of harm to the consumer are low, the notice and choice burden may be lower than where the likelihood of harm (either due to probability or due to size) is greater. For example, where only pseudonymous data is collected, notice may be appropriate in a privacy policy and the choice mechanism may be an opt-out.

The burden of education on targeting and tracking has thus far fallen on the advertising networks that have promoted behavioral advertising techniques to advertisers, publishers and their agents. Unfortunately, the education and transparency discussion has taken place largely within industry and not with the subjects of data collection and use - consumers. By and large the ad networks do not have direct relationships with consumers, so reliance upon them to provide education has failed. TRUSTe promotes that advertisers and publishers are also accountable for the privacy of internet users needs. In many cases, the most appropriate source for notice to consumers is the owner of the website where the collection is initiated or takes place.

We believe that companies should not collect data from or about individuals for behavioral advertising without offering them, at a minimum, an opportunity to opt-out of the collection, or use; even if that choice means that the individuals may not use the service offered on the Web site where the data is collected. In surveys, nearly half of consumers indicate a willingness to click on banner ads or buttons to reduce unwanted advertising, and 64% would like to only see ads from brands and stores they know and trust. Companies should embed contextual educational information wherever feasible, even in cases of first party collection and use, to promote awareness of such use, including limitations, discuss consumer benefits as applicable, and empower consumers with tools for control. Proactive notice systems are essential and necessary at this stage of market development,

given the current level of awareness and discomfort that our survey revealed.

For third party collection and use, TRUSTe is considering standards for minimum reference and proactive notices, and the proper implementation of choice. Clearly these mechanisms need to exist. The diversity of relationship models and interfaces has created challenges that the market is addressing at this stage with experimentation. Every corporate beneficiary of the targeting chain, including first parties with consumer relationships that merely facilitate the tracking performed by third parties, are equally responsible for ensuring that affected consumers have been given accurate and full reference notice, a viable choice mechanism, and that the parties involved have embarked on a reasonable proactive notice campaign.

We also believe that appropriate consent should be required where (1) companies seek to merge Personally Identifiable Information with previously collected Pseudonymous Information and (2) where companies seek to collect sensitive data for behavioral advertising. In the first example, affirmative express consent prior to the merger of information would be appropriate. Such consent could be gathered by creating a barrier page for content areas that, when browsed, would lead to sensitive information collection, or other just-in-time methods. In the second example, an obvious and unavoidable opt-in may be appropriate.

## **II. Proposed Principles: Reasonable Security, and Limited Data Retention, for Consumer Data**

*Any company that collects and/ or stores consumer data for behavioral advertising should provide reasonable security for that data. . . such protections 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 protections available to a company.*

*Companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.*

TRUSTe agrees that companies must provide reasonable data security. We require our own licensees to adopt commercially reasonable security measures, and we recognize that the FTC has developed a well established body of knowledge as to what constitutes "commercially reasonable security". Data collected for behavioral advertising, including personally identifiable information, pseudonymous, or anonymous information tied to personally identifiable information, should be stored securely, commiserate

with the sensitivity, accessibility, and use of such data. The relevant systems must also be monitored and updated to maintain that security.

Companies should have sound data retention and destruction policies as a part of their security program which limits how long they hold data. Data should not be retained forever, but we are concerned that the language stating that companies should “retain data only as long as is necessary to fulfill a legitimate business or law enforcement need” provides insufficient guidance to companies on the parameters of the term “legitimate business need.” We suggest that the data retention principle would benefit from the addition of a discussion of the Commission staff’s views on what they consider to be legitimate business needs.<sup>5</sup>

### **III. Proposed Principle: Affirmative Express Consent for Material Changes in Existing Privacy Promises**

*[B]efore a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers.*

Any time there is a change in collection, use or disclosure policies, notice and consent is needed. Where such change is applied to data collected after notice, the consent may appropriately be opt-out. TRUSTe agrees that such notice and consent may use the same methods as the original notice and consent.

However, in the circumstance that the change in use will be applied to previously collected data, TRUSTe agrees that affirmative express consent should be required. Such consent is often obtained by suspending service for existing users once a material change in data use has been implemented, delivering notice of the change in data use through a barrier page or interstitial, and reactivating existing users only if they consent to the change.

### **IV. Proposed Principle: Affirmative Consent to (or prohibition against) using Sensitive Data for Behavioral Advertising**

---

5. While we acknowledge the Commission’s important work in providing business guidance on this issue in its handbook entitled “*Protecting Personal Information: A Guide for Business*,” we would respectfully point out that that resource uses several different terms, including “legitimate” business needs or reasons, “essential business need” and “business reasons” to describe alternative bases for retaining data. In our experience, there remains confusion about the application of these terms, which detracts to some extent from the very useful information provided elsewhere in the *Guide*.

*Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising.*

TRUSTe agrees that affirmative express consent should be required prior to the collection and use of sensitive data. In the discussion of Principle One we suggested a sliding scale for providing notice and choice, and a prohibition against the collection of sensitive data unless a short, just-in-time notice is provided and consumers opt in to the use of that data for marketing purposes.

#### Definition and Acceptable Uses of "Sensitive Data"

Defining sensitive data has always been challenging. Anonymous information can include sensitive information, including health conditions, sexual orientation, personal interests, political or other affiliations, etc. The boundary between sensitive and non-sensitive information varies with the individual. TRUSTe defines "sensitive information" to include social security numbers, financial account and transaction information, and health information that is connected to Personally Identifiable Information. While the definition of sensitive data is still evolving and requires further market testing, we believe that one of the criteria must be whether or not open transfers of the data to certain third parties might do the consumer material harm. This criteria moves beyond the 'spook' factor, to consider specific cases where, for example, certain medical information, if it were to be shared with health care providers, might increase insurance rates or reduce coverage. Any category of information with a similar potential for harm should be collected with higher consent standards and corresponding strict security and sharing standards.

At a minimum, companies that are collecting and using for marketing, sensitive data should be required to provide additional concise, just-in-time notice and consumer control in the form of an opt-in.

TRUSTe does not recommend excluding the collection of sensitive data. Excluding broad categories of data is bound to have unintentional consequences, especially at this early stage where the definition of sensitive information remains unclear. In addition, we are already seeing inventive business models emerging in the consumer finance market for example, that leverage sensitive information for ad targeting purposes with full consent. These models, which may have significant consumer benefit, would not be allowable in a market with a blanket prohibition on sensitive data collection and use.

## **Conclusion**

Behavioral Advertising presents both opportunities for creativity and innovation and challenges to consumer privacy. We applaud the Commission staff's efforts to generate dialogue on best practices in this area. Behavioral advertising is still in a nascent stage. As such, it is the appropriate moment for the broader community to begin educating consumers regarding current and emerging practices to ensure that they are empowered to make appropriate choices in building their online experiences. Companies engaging in behavioral advertising, aided by rapidly evolving tools and technologies, are experimenting with delivering notice and choice in a variety of innovative and powerful ways outside the privacy statement. New methods for delivering choice are emerging. The FTC call for guidelines has helped spur experimentation and collaboration for self-regulation, but additional regulation, or enforcement would be premature at this stage. In the on-going development of our own privacy program requirements we will be considering the range of business models, and balance consumer empowerment with the practices and available tools.

## **About TRUSTe**

TRUSTe helps consumers and businesses identify trustworthy online organizations through its Web Privacy Seal, Children's Privacy Seal, EU Safe Harbor Seal, Email Privacy Seal and Trusted Download Programs. ; TRUSTe certifies more than 2,400 Web sites, including the major internet portals and leading brands such as Microsoft, IBM, Oracle, Nestle, Intuit and eBay. TRUSTe resolves thousands of individual privacy disputes every year. TRUSTe celebrated its 10th anniversary in 2007, a complete description of all of our programs may be found on our Web site at [www.truste.org](http://www.truste.org).

In May 2001, the Federal Trade Commission approved TRUSTe's Children's Privacy Seal Program as a safe harbor under the Children's Online Privacy Protection Act. We are proud to have received that designation TRUSTe also serves as a safe harbor program under the Safe Harbor Framework administered by the U.S. Department of Commerce for U.S. companies wishing to receive personal data from countries in the European Union ("EU"). Our EU Safe Harbor Seal Program gives companies assurance that they are in compliance with the Framework and, therefore, with national data protection laws in all EU member states.