



## **Online Behavioral Advertising Possible Self-Regulatory Principles**

### **Comments Submitted to the Federal Trade Commission by TrueEffect April 11, 2008**

#### **Introduction**

TrueEffect is an ad serving company founded in 2002 and based in Denver, CO. The TrueEffect founders were able to bring with them experts and intellectual property from their previous start-up effort: MatchLogic, a seminal internet advertising technology company started in the mid-nineties and acquired by Excite@Home. The majority of the TrueEffect staff has worked in the fields of advertising, database marketing and technology for over 20 years with well-known global companies such as General Motors, Apple, InterPublic Group, EDS, Bronner and Fair Isaac.

TrueEffect Chief Operating Officer, Scott Nelson, spoke at the FTC E-haviorial Advertising Town Hall meeting held in Washington, D.C. on November 1 and 2, 2007. TrueEffect has also been participating in ongoing discussions between cross-industry representatives and privacy advocates through the Internet Privacy Working Group led by the Center for Democracy and Technology.

TrueEffect was founded largely on the perspective that advances in technology and business models can support smart advertising while also providing a higher degree of consumer privacy. We have gotten involved in the policy process around this issues to provide both our technical expertise and our point of view that things can be done differently – and better.

#### **Background**

Before addressing the specific principles proposed in the FTC staff paper issued in December 2007, it seems appropriate to provide some relevant information and definitions that will add context to our input about self-regulatory principles.

As a basic definition, ad servers are companies that deliver ad campaigns across the Internet and measure their performance for online advertisers and publishers. Advertisers are the companies that pay to have ads about their products or services delivered to consumers. Publishers are companies that present content on their website to attract consumers, and sell advertising in that content.

As the growth of the Internet and advent of clickable Web ads accelerated from the early to mid-nineties, many large, brand-name companies interested in building an online advertising capability lacked the in-house technical expertise. This lent itself to the formation of an entire industry of third party companies who jumped at the chance to fill this market need. In doing so, ad servers developed several different methods to target ads. We define targeting as the opportunity to select which of two or more potential ad messages to deliver. The basis for choosing between those two or more messages can be categorized in several ways:

- Contextual targeting infers the best selection of an ad based on the information contained on the Web page. For example, placing travel oriented ads on travel related sites.
- Demographic targeting infers the best selection of an ad based on known characteristics of a user such as gender, education or presence of children. For example, serving an ad for a family vacation destination to a user known to have children in the household.
- Geographic targeting infers the best placement for an ad based on a user's likely geographic location. For example, placing an ad for a restaurant chain on web sites for performing arts centers in the same cities where the restaurant has locations.
- Technographic targeting uses information about the connection speed, browser version or other data about the consumer's technical configuration to determine what ads to serve. For example, sending graphic rich ads only to high-speed, broadband connections and not to dial-up users.
- Behavioral targeting uses information gathered at the time a consumer undertakes a specific and measurable action representing a particular behavior. For example, delivering an ad for mortgage services based on the consumer entering mortgage-related terms into a search engine. Behavioral targeting, given it is based on the measurable behavior of a consumer and not personally identifiable information, is usually achieved using anonymous data.

While much attention has been paid recently to the online aspects of behavioral targeting, the basic concept has been used in the offline world for years and is an informative example of how it can work. We all value our individual privacy, but we also appreciate not being bombarded with irrelevant ads. As an example, when a coupon or postcard is delivered in the mail from a pet supply store to a home that does not have a pet, it is likely to be considered junk mail and quickly thrown into the recycling bin. In contrast, when a marathon runner receives a 20% discount coupon in the mail to a sporting goods store it is likely to be viewed as something valuable, even if it is not a store the person has shopped at previously. Similarly, at the grocery store check-out coupons are often given along with the receipt. A coupon for a new brand of juice is more likely to be useful if juice was purchased than a coupon for diapers if no baby products were purchased.

Ultimately, advertisers only want to pay to deliver messages to consumers that are likely to be interested, and consumers are only interested in receiving information about the things they need and want. The Internet as an ad delivery mechanism offers considerable opportunity to address these desires. At the same time, the convergence of data collected online and offline, the ever decreasing cost of data storage, as well as mergers and acquisitions between media,

Internet and telecom companies raise questions about how we can meet the consumer's expectation for protecting their privacy. Technology will help us to address those expectations to a point, but we cannot depend on technology alone for a solution. Representatives from industry, government regulatory bodies and consumer advocates will need to agree how best to ensure that consumers' interests are represented and protected, including protecting consumer access to the highly-valued, ad-supported content that so many have made part of their everyday lives.

## **1. Transparency and Consumer Control**

### FTC Proposed Principle:

*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 interest and 2) consumers can choose whether or not to have their information collected for such purpose. The web site should also provide consumers with a clear, easy-to-use and accessible method for exercising this option.*

### TruEffect Comments:

We agree that transparency and consumer control should be fundamental elements of online advertising programs. Generally, the privacy expectations a consumer has will depend on the situation, the type of data and the entity requesting the data. Consumers often make choices in a range of situations about how much information to provide depending on the relationship and trust that exists with a particular company or organization. For example, with a vendor that the consumer has an ongoing relationship, the company is known and trusted by the consumer, the consumer may share a great deal of information. Whereas with an unknown company that the consumer does not trust there may not be any information the consumer is willing to share.

Providing consumers with information they can use to make informed decisions and exercise control over the ways their information is used presents challenges, as currently Web site privacy statements as well as advertising notice and consent regimes take various forms. The lack of consistency puts a greater burden on consumers.

The FTC or industry groups may need to be more directive about the types of information that consumers should receive in various circumstances, and the mechanisms available for consumers to make choices about whether or not their information is collected.

## **2. Reasonable Security, and Limited Data Retention, for Consumer Data**

### FTC Proposed Principle:

*Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with the data security laws and the FTC's data security enforcement actions, 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.*

### TruEffect Comments:

We strongly agree with this principle. Companies should certainly be held accountable to protect consumer data. Too often companies upstream from the delivery of ads cede any role in data stewardship to the companies delivering ads and/or collecting data. Ad servers, third party data aggregators and companies that pay for advertising all need to take their role as responsible data stewards seriously. Greater transparency in the process serves as an incentive for companies to take care with the data they hold. Particularly, when companies with valuable consumer brands are part of the process, they have a stake in data stewardship to protect their reputations.

FTC Proposed Principle:

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

*Question: Can or should companies reduce their retention periods further?*

TruEffect Comments and Response:

We agree companies should retain data only as long as necessary to fulfill a legitimate business or law enforcement reason. Companies should have the shortest retention period practical, however the appropriate retention period will vary depending on the type of data and type of business holding the data. A primary business reason to retain data would be for legal compliance, and legal requirements vary by industry, country and situation. Maintaining customer relationships is another key reason companies retain data. Sales cycles vary from industry to industry and so too will the time periods that companies retain sales related data. For example, a Web site that provides online movie rentals may retain rental history and a list of movies a former customer was interested in, so that if the customer later returns to renew their membership they will not need to start over building their interest list. A car dealership may retain information about those who requested a test drive even if they do not result in a sale, as the likely purchaser will probably not be in the market for a car again in several years. While retention periods are important, transparency around the collection of data and solid data stewardship principles about how to responsibly retain and secure data minimize concerns about retention periods per se.

### **3. Affirmative Express Consent for Material Changes to Existing Privacy Promises**

FTC Proposed Principle:

*A company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Before 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. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way a company collects, uses and shares data.*

TruEffect Comments:

We agree with this principle when dealing with personally identifiable data. It would be worthwhile for industry groups to further investigate and identify the most effective ways to notify consumers about changes in policies given that it would be easy to envision such notices being ignored or lost to spam filters. In the end, companies may determine it will be easier to uphold

the initial terms of use. In the case of data that is aggregated, there may not be a way to disaggregate the information to identify which consumers it came from initially, in which case future notices would not be possible.

#### **4. Affirmative Express Consent to (or prohibition against) Using Sensitive Data for Behavioral Advertising**

##### FTC Proposed Principle:

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

*Questions: What classes of information should be considered sensitive? Should using sensitive data for behavioral advertising be prohibited? Or should it be subject to consumer choice?*

##### TruEffect Comments and Response:

Different individuals will have different definitions about what they consider to be sensitive data. Their relationship and level of trust with the entity collecting the data will influence their feelings and expectations about sharing sensitive data as well. It is important to focus on providing a higher level of consumer choice in saying how any potentially sensitive information may be used.

There are some technical solutions that could help provide greater granularity about consumer preferences. It would be possible to establish a convention for preference cookies, similar to opt-out cookies. However, there is an inherent weakness in using cookies to control cookies, particularly as more and more users delete cookies regularly, and anti-spyware and similar software programs also may be set by users to delete all cookies regularly. There are also other technical solutions that exist, such as P3P, that may help to address these issues.

Central to this principle is acknowledgement that these challenges are increasingly surfacing outside a browser-based context. The rise in mobile device use, beyond laptops into phones and other new multi-purpose devices, requires that this issue be looked at in a broader context to consider how any principles issues will function across technical platforms. There is opportunity here for greater technological innovation to further empower consumers in ways that are easy to understand and use.

It is important that the FTC avoid giving technical directives that attempt to direct engineers how to build products, more prescriptive guidelines about the functions various technologies must be able to fulfill may need to be investigated and proposed. Most important is devising principles that can be applied to sensitive data consistently in different circumstances, both online and offline, both browser-based and non-browser based.

#### **5. Using Tracking Data for Purposes Other Than Behavioral Advertising**

##### FTC Call for Additional Information:

*Which secondary concerns raise concerns?*

*Are companies using data for these secondary purposes?*

*Are concerns about secondary uses limited to the use of personally identifiable data or do they also extend to non-personally identifiable data?*

*Do secondary uses merit some form of heightened protection?*

TruEffect Response:

TruEffect primarily deals with click stream data collected in the course of Internet users browsing Web sites, so we are most familiar with transaction level data and our comments in this section apply to transaction records. Our company provides the information collected to the advertisers that are our customers. There are also companies that will take transactional data and collect it in an anonymous profile repository. Secondary uses for this type of data that we understand to be in practice by some companies include:

- Identifying patterns of purchasing behavior to drive segments for banner targeting
- Planning and managing production and inventory of products based on anticipated demand
- In-house testing of enhancements or fixes to existing products
- Developing trend data about media consumption
- Statistical analyses of Internet industry such as number of various browser types, etc.
- Appending it to personally identifiable information volunteered by consumers to gain new insights underlying buying behaviors
- Deriving customer analytics based on attributes that customers have volunteered

Some kinds of secondary uses raise definite privacy concerns. Most concerning is when companies link click stream data they have collected with other data sources that include personally identifiable information. As companies with offline and online business operations merge data, and as mergers and acquisitions of companies in the media, Internet and telecom industries continue, the potential for linkage between click stream data and PII increases, heightening secondary use concerns.

In each of these cases, the difference between “good” data uses and those that most people would view as concerning are business practices rather than technology. Government set guidelines about the use of consumer data are an important component to effectively regulating the market and ensuring that consumers interests are not subjugated to profit motivations.

With a range of players in the market, and data often passing through several companies, it is important to clearly establish which companies are the stewards of the data and what requirements rest on them to protect and control use of the data. Along these lines, a consistent method of clearly disclosing data uses/stewards/associations to consumers needs to be developed.

Conclusion:

While the people at TruEffect are very familiar with the ad serving models used to date, in fact some of us helped to create them, we believe it is time for a change. We strongly support greater transparency in the online advertising system. This enables consumers to make conscientious choices to interact, shop and buy from reputable businesses, and to share information based on their level of knowledge and trust with the entity collecting the information.

With the patent-pending technologies we've developed, we can remove the ad server from the data equation by placing the advertiser and consumer into a direct relationship, or in certain cases, eliminating the collection of consumer data from the model altogether. By empowering companies to more directly control their online advertising campaigns it creates a clear one-to-one relationship between advertisers and their customers or likely customers. This simplified model makes it very clear who is collecting the data and thus, makes setting, monitoring and enforcing clear standards for data handling a more focused effort. This is particularly important as technology continues marching forward.

The Internet is no longer defined by servers and browsers exchanging information across copper and fiber. Going forward, data about consumer behavior will not be mediated by the cookie facility embedded in browser software. With the explosive growth of digitally addressable media (including digital cable, satellite TV and mobile), consumer data privacy guidelines must apply across all these data gathering channels.

As technologies continue to evolve, advertising guidelines need to support and promote consumers' ability to match their expectations for varying levels of privacy depending on the circumstance with the data collection and retention approaches used.