

# Data and Identity Security

## **Be On Your Best Behavior: Principles For Online Behavioral Advertising**

---

*by*  
*Mark P. Kessler, Esq.*  
*and*  
*Matthew Savare, Esq.*

*Lowenstein Sandler PC*  
*Roseland, New Jersey*

**A commentary article  
reprinted from the  
April 2010 issue of  
Mealey's Litigation Report:  
Data and Identity Security**



# Commentary

---

## Be On Your Best Behavior: Principles For Online Behavioral Advertising

By  
**Mark Kessler**  
and  
**Matthew Savare**

*[Editor's Note: Mark P. Kessler is chair of Lowenstein Sandler PC's Intellectual Property section of the firm's Tech Group and co-chair of the IP Litigation Group. He provides strategic guidance to technology-based businesses. His e-mail is mkessler@lowenstein.com. Matthew Savare practices intellectual property, media, and entertainment law with Lowenstein Sandler PC. His e-mail is msavare@lowenstein.com. Copyright 2010 by Mark P. Kessler and Matthew Savare. Responses are welcome.]*

As the Internet has expanded and evolved, consumers have enjoyed unprecedented access to free content, communication, and information. Generally, this free content is supported by advertising, which has become more textured and interactive. Companies with a web presence are increasingly employing targeted advertising based on a user's online behavior in order to deliver relevant ads to a more defined audience. By targeting their customers with greater precision, companies employing such "behavioral advertising" seek to pay for fewer impressions of their ads and enjoy higher click-through and conversion rates.

Although such an arrangement seems beneficial for all parties — consumers continue to receive free content and services in exchange for ads that they may actually find useful, and advertisers are able to concentrate their resources on viable prospects — behavioral advertising has come under increased scrutiny, as the aggregation, combination, and use of consumers' online viewing habits have raised privacy concerns.

Wary of potential government regulation, the advertising industry — like the entertainment industry had done years prior with respect to rating its content — responded by adopting its own self-regulatory measures. These guidelines, which have recently gone into effect, require companies to comply with a series of best practices modeled on principles espoused by the Federal Trade Commission ("FTC"). Implementing, monitoring, and enforcing these principles are paramount to industry staving off any formal action by the government.

### Regulatory Background

Over the last decade, in the wake of highly-publicized electronic data breaches and privacy violations, greater attention has been placed on consumer privacy in the digital age. In November 2007, the Federal Trade Commission ("FTC"), spurred by organizations such as the Electronic Frontier Foundation, the Center for Digital Democracy, Privacy Rights Clearinghouse, and Consumers Union, held a town hall meeting to discuss online behavioral advertising. A month after these meetings, the FTC released for public comment a set of proposed principles intended to serve as the basis for industry self-regulation.

In February 2009, the FTC issued a report titled, "Self-Regulatory Principles for Online Behavioral Advertising" (the "FTC Report"), which addressed the more than sixty public comments it received in response to its originally-proposed principles. The FTC Report set forth the following four principles

for industry to follow: (1) transparency and consumer control, (2) reasonable security and limited retention of consumer data, (3) affirmative express consent for material changes to existing privacy promises, and (4) affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising (collectively, the "Principles").

In crafting the scope of the Principles, the FTC issued three significant findings. First, the FTC concluded that in the context of behavioral advertising, the conventional notion of what constitutes personally identifiable information ("PII") and non-PII is becoming less meaningful and strict definitions should not be used to determine the protections afforded to consumer data. Rather, the FTC found that the best approach is for the Principles to govern "any data collected for online behavioral advertising that reasonably could be associated with a particular consumer or with a particular device."

Second, the FTC concluded that so-called "first party advertising" (*i.e.*, advertising in which a website collects consumer information to deliver targeted ads at its site, but does not share any of this data with third parties) does not fall within the scope of the Principles. However, the FTC cautioned that if the company later sells or shares the data with a third party for purposes of behavioral advertising or participates in a network for behavioral advertising, such practices would fall within the Principle's scope.

Finally, the FTC determined that "contextual advertising" (*i.e.*, the delivery of ads based upon a consumer's single search query or visit to a single website) is not covered by the Principles.

### Industry Responds

In July 2009, a group of the largest media and marketing trade associations responded to the FTC Report with its own report of the same name ("Industry Report"). The consortium, which includes the Association of National Advertisers, the Direct Marketing Association, and the Council of Better Business Bureaus, adopted the Principles set forth by the FTC and included two additional ones: public education and industry accountability.

Here is a brief overview of the principles described in the Industry Report, which defines "Online Be-

havioral Advertising" as "the collection of data from a particular computer or device regarding Web viewing behaviors over time and across non-Affiliate Web sites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors."

1. Transparency — Third parties and service providers are to provide "clear, meaningful, and prominent notice on their own websites that describe their Online Behavioral Advertising data collection and use practices." This is a significant change for many companies, which tend to bury any such disclosures in their privacy policies. In addition, operators of websites employing behavioral advertising should include a "clear, meaningful, and prominent" link on the web page where consumer data is collected or used for such purpose that either links to an industry-developed website that lists such Third Parties or individually discloses such Third Parties.

In January 2010, in an effort to simplify and standardize the disclosure process, the advertising industry agreed on a standard icon — a white "i" surrounded by a circle on a blue background — that companies using Online Behavioral Advertising will add to their online ads to inform consumers how their data is being collected and used. The icon, which major companies plan on adding to their online advertisements by mid-summer, is to be accompanied by a phrase such as "Why did I get this ad?" When consumers click on the icon or the phrase, they will be redirected to a page that explains how the advertiser used their online history and demographic information to send them such targeted ads.

2. Consumer Control — Third Parties should allow consumers to choose whether their data is collected and used for Online Behavioral Advertising. Service Providers should not collect and use data for such purposes without first obtaining the consumer's consent, which, once granted, should be made easy to withdraw.

3. Data Security — Entities are to employ “appropriate” physical, electronic, and administrative safeguards to protect consumer data. In addition, such data should be retained only as long as necessary to fulfill a legitimate business need or as required by law. In addition, Service Providers, among other things, are to anonymize, alter, or randomize any consumer PII or unique identifiers to prevent such data from being reconstructed.
  4. Material Changes to Existing Online Behavioral Advertising Policies and Practices — Before applying any material change to their data collection and use policies with respect to Online Behavioral Advertising, entities are to obtain a consumer’s consent.
  5. Sensitive Data — Entities should not engage in Online Behavioral Advertising directed to children they have actual knowledge are under thirteen, except as permitted by the Children’s Online Privacy Protection Act. In addition, entities should not collect personal information from children they know to be under thirteen or from sites directed to children. With respect to other forms of “sensitive data,” entities should not collect and use Social Security Numbers, financial account numbers, drug prescriptions, or medical records for Online Behavioral Advertising without the consumer’s consent.
  6. Accountability — The Industry Report notes that its principles are self-regulatory in nature, and apply to the more than 5,000 companies that belong to any of the sponsoring organizations. It also stipulates that monitoring, reporting, and compliance programs need to be put into place to process complaints, ensure transparency, and promote compliance.
  7. Education — The Industry Report encourages entities to participate in educational and outreach programs to instruct individuals and businesses about Online Behavioral Advertising.
- Conclusion**
- A dynamic online marketplace supported by targeted ads served based upon consumers’ online behaviors and the protection of those consumers’ privacy do not have to be mutually exclusive. With the adoption of the Industry Report, industry has taken a meaningful step toward self-regulation. Should companies fail to rigorously comply with and enforce these principles, it will likely invite legislation by Congress and regulation from the FTC. Accordingly, companies employing Online Behavioral Advertising are well-advised to follow these guidelines. ■

**MEALEY'S LITIGATION REPORT DATA AND INDENTITY SECURITY**

*edited by Bajeerah LaCava*

**The Report** is produced monthly by



1018 West Ninth Avenue, 3rd Floor, King of Prussia Pa 19406, USA

Telephone: (610) 768-7800 1-800-MEALEYS (1-800-632-5397)

Fax: (610) 962-4991

Email: [mealeyinfo@lexisnexis.com](mailto:mealeyinfo@lexisnexis.com) Web site: <http://www.lexisnexis/mealeys>

ISSN 1942-7387