

Jan. 5, 2015

## Online Behavioral Advertising: Industry Guides Require Real Time Notice When Data Are Collected or Used for Personalized Ads

### WHAT'S COVERED?

Online behavioral advertising (OBA) has become a very common tool for commercial websites. OBA can be defined as follows:

*the collection of data online from a particular computer or device regarding web viewing behaviors over time and across Web sites for the purpose of using such data to predict preferences or interests and to deliver advertising to that computer or device presumed to be of interest to the user of the computer/device based on observed Web viewing behaviors.*

OBA might be implemented by use of cookies directly on a company's website by the company itself. Or it might occur through technology embedded in ads from other parties displayed on the company's site. Either way, the operators of commercial websites need to be aware when OBA is occurring on their sites and should be taking steps to provide greater transparency about OBA occurring on their sites.

### WHAT'S THE CONCERN?

While the use of OBA is largely unregulated by law in the U.S. at this time, its spread has generated concern among privacy advocates. Of particular concern is the gathering of data about consumers without their knowledge where such information is supposed to be anonymous but advances in technology make it more and more possible to link that information to individuals (not just devices) through combination with other information. Examples can include information about health conditions and other sensitive information gleaned by watching the sites a user visits, the searches he/she conducts, etc. Key characteristics of OBA include that it is: (a) invisible to the user; (b) hard to detect; and (c) resilient to being blocked or removed.

In an effort to stave off government regulation of OBA in the United States, the Digital Advertising Alliance (DAA), a consortium of the leading advertising trade associations, has instituted a leading set of guidelines. Based on standards proposed by the Federal Trade Commission, the DAA Self-Regulatory Program is designed to give consumers enhanced control over the collection and use of data regarding their Internet viewing for OBA purposes.

### WHAT'S REQUIRED?

The key principles of the DAA's guides are to provide greater transparency to consumers to allow them to know when OBA is occurring and to provide the ability to opt out. For commercial website operators that allow OBA on their sites, the compliance implications are as follows:

1. First Party OBA. First Parties are website operators/publishers. If a company simply gathers information for its own purposes on its own site, it is generally not covered by the guidelines. However, as soon as the First Party allows others to engage in OBA via the site, it has a duty to monitor and make sure that proper disclosures are being made and even to make the disclosures itself if the others do not do so, including assuring that “enhanced notice” (usually the icon discussed below or a similar statement) appears on every page of the First Party’s site where OBA is occurring.
2. Third-Party OBA. Third parties are ad networks, data companies/brokers, and sometimes advertisers themselves, who engage in OBA through ads placed on other parties’ sites. These Third Parties should provide consumers with the ability to exercise choice with respect to the collection and use of data for OBA purposes. (See below on how to provide recommended disclosures.)
3. Service Providers. These are providers of Internet access, search capability, browsers, apps or other tools that collect data about sites a user visits Service Providers generally are expected to provide clear disclosure of OBA practices which may occur via their services, obtain consumer consent for such practices, and provide an easy-to-use opt-out mechanism.

## HOW TO COMPLY

Generally, Third Parties and Service Providers should give clear, meaningful, and prominent notice on their own websites that describes their OBA data collection and use practices. Such notice should include clear descriptions that include:

- > The types of data collected online, including any PII for OBA purposes;
- > The uses of such data, including whether the data will be transferred to a nonaffiliate for OBA purposes;
- > An easy to use mechanism for exercising choice with respect to the collection and use of the data for OBA purposes or to the transfer of such data to a nonaffiliate for such purpose; and
- > The fact that the entity adheres to OBA principles.

In addition, “enhanced notice” should appear on each and every ad (or page) where OBA is occurring. The “enhanced notice” means more than just traditional disclosure in a privacy policy. It means placement of a notice on the page/ad where OBA is occurring. The notice typically is given in the form of the following icon (in blue color) which should link to a DAA page describing OBA practices and providing an easy-to-use opt-out mechanism:



The icon/link should appear in or around each ad where data are collected. Alternatively, it can appear on each page of a website on which any OBA ads are being served. It is normally the duty of the advertisers (Third Parties) to deploy the icon. However, if they fail to do so, then the operator of the site where the OBA ads appear has the duty to make appropriate real-time disclosures about OBA on each page where OBA activity is occurring, including links to the DAA page describing OBA practices and providing an easy-to-use opt-out mechanism.

## ENFORCEMENT

The DAA is taking its OBA guidelines seriously. It has issued sets of “compliance warnings” to many major U.S. companies. While DAA has no direct authority to impose fines or penalties, its issuance of a ruling finding a violation of its guidelines could create a tempting target for the FTC or plaintiffs’ class action lawyers to bring separate actions against a company not following the DAA guidelines. For all these reasons, operators of websites employing OBA (either first party or third party) should pay heed to the [DAA Guidelines](#).

This *GT Alert* was written by **Ed Chansky** and **David A. Wheeler**. Questions about this information can be directed to:

- > [Ed Chansky](mailto:chansky@gtlaw.com) | +1 702.599.8016 | [chansky@gtlaw.com](mailto:chansky@gtlaw.com)
- > [David A. Wheeler](mailto:wheelerd@gtlaw.com) | +1 312.456.8450 | [wheelerd@gtlaw.com](mailto:wheelerd@gtlaw.com)
- > Or your [Greenberg Traurig](#) attorney

<b>Albany</b> +1 518.689.1400	<b>Denver</b> +1 303.572.6500	<b>New York</b> +1 212.801.9200	<b>Shanghai</b> +86 (21) 6391.6633
<b>Amsterdam</b> +31 (0) 20 301 7300	<b>Fort Lauderdale</b> +1 954.765.0500	<b>Northern Virginia</b> +1 703.749.1300	<b>Silicon Valley</b> +1 650.328.8500
<b>Atlanta</b> +1 678.553.2100	<b>Houston</b> +1 713.374.3500	<b>Orange County</b> +1 949.732.6500	<b>Tallahassee</b> +1 850.222.6891
<b>Austin</b> +1 512.320.7200	<b>Las Vegas</b> +1 702.792.3773	<b>Orlando</b> +1 407.420.1000	<b>Tampa</b> +1 813.318.5700
<b>Boca Raton</b> +1 561.955.7600	<b>London*</b> +44 (0) 203 349 8700	<b>Philadelphia</b> +1 215.988.7800	<b>Tel Aviv^</b> +972 (0) 3 636 6000
<b>Boston</b> +1 617.310.6000	<b>Los Angeles</b> +1 310.586.7700	<b>Phoenix</b> +1 602.445.8000	<b>Tokyo<sup>‡</sup></b> +81 (0)3 3216 7211
<b>Chicago</b> +1 312.456.8400	<b>Mexico City+</b> +52 (1) 55 5029 0000	<b>Sacramento</b> +1 916.442.1111	<b>Warsaw~</b> +48 22 690 6100
<b>Dallas</b> +1 214.665.3600	<b>Miami</b> +1 305.579.0500	<b>San Francisco</b> +1 415.655.1300	<b>Washington, D.C.</b> +1 202.331.3100
<b>Delaware</b> +1 302.661.7000	<b>New Jersey</b> +1 973.360.7900	<b>Seoul<sup>∞</sup></b> +82 (0) 2 369 1000	<b>Westchester County</b> +1 914.286.2900
			<b>West Palm Beach</b> +1 561.650.7900

*This Greenberg Traurig Client Advisory is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. \*Operates as Greenberg Traurig Maher LLP. \*\*Greenberg Traurig is not responsible for any legal or other services rendered by attorneys employed by the strategic alliance firms. †Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ‡Greenberg Traurig Tokyo Law Offices are operated by Greenberg Traurig Horitsu Jimusho, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2015 Greenberg Traurig, LLP. All rights reserved.*