

## **Be On Your Best e-havior**

### **The Fine Line Between Tracking User Information and Consumer Privacy**

by Jill Fishbein and Heidi Walas

Most on-line users have had the experience of searching the Web and being inundated with unsolicited banner ads that flash messages such as car sales or the latest celebrity diet. More recently, you might have noticed that these advertisements are becoming particularly relevant to your interests or needs - a sports enthusiast might see advertisements for the upcoming soccer championships, while a new parent might see advertisements for baby clothes. While this form of targeted advertising has its appeal to advertisers and some consumers, others have heightened concerns about disclosure of their “behavioral profiles” and other sensitive, personal information. The on-line advertising industry has responded by creating voluntary *best practices*, although some privacy advocates would prefer to codify these practices into law.

#### **What is e-havioral Marketing?**

Advertising, as a backbone to the web, provides real and hoped-for income to new and seasoned on-line businesses, who, in turn, provide free information and services to Web users. E-havioral marketing helps make advertisements more relevant and, therefore, more valuable. By incorporating on-line behavioral activity, contextual advertising and other targeted marketing devices, e-havioral marketing can lead to customized advertisements for specific online viewers. Advertising networks apply information collected from users’ web-browsing history while continuing to use other more conventional data, such as geography and demographics to serve up pertinent, targeted ads.

When a user views a web page, the user will receive the content displayed by the web page’s creator or publisher and will receive additional content from multiple sources of advertising, often served in the form of banner ads. The banner ads may appear as a result of the web page requesting such advertisements from one or more ad network servers before loading it on the user’s computer screen.

The ad network will not only send the image for the advertisement, but will also send to the user’s computer a common tracking mechanism embedded in the ad called a “cookie”. A cookie is a unique identification assigned to each of a web-site’s visitors and is temporarily

stored on the visitor's computer. The cookie allows for the tracking of a user's browsing history, permitting an ad network or an advertising analytics enterprise to watch the user reappear on other web sites. In addition to cookies, other tracking mechanisms include "web beacons" or "pixels." These work in conjunction with cookies to deliver to ad networks information gathered from users. Another tracking tool is called a "web beacon", which is an invisible image on a webpage that can collect: (i) a user's IP address; (ii) the browser being used; (iii) the time the page is viewed; (iv) the URL of the page; and (v) the physical location of the user at the time of viewing. New entities known as web analytics enterprises aggregate these data from different users and create *anonymous* user profiles based on information including geographic location, content interests, time spent viewing certain web pages, shopping history, travel locations, entertainment interests, etc. Advertising networks use these behavioral profiles to deliver unsolicited but relevant advertisements to potential consumers as they continue to visit other web pages.

### **The Privacy Debate on Tracking and Gathering User Information**

The development of increasing e-havioral information and advertising has led to enhanced privacy concerns. Behavioral profiles are sold or shared with third parties, typically without the user's knowledge. While most ad networks do not collect personally identifiable information such as name, address, phone number, social security number etc., it is still possible to piece together a real person from these *anonymous* profiles.

Two years ago, for example, AOL intentionally released a cache of users' search requests. No user names or IP addresses were disclosed and users were identified only by randomly assigned numbers. However, it was possible to identify individuals by name through careful review of their *anonymous* search queries. Taking the publicly released information, The New York Times was able to make personal identifications and, as an example and with her permission, revealed the identity of a 62 year old woman, among others. Fear of inadvertently leaking sensitive information and other personally identifiable information contributed to AOL's rapid take-down of the data it had posted. In this case, despite efforts to make information anonymous, potential identification became actual identification.

In order to build trust with the user community, self-regulating advertising groups have emerged. Most notably among such groups is, the Network Advertising Initiative ("NAI"), a

collaboration of online marketing and analytics companies created to establish privacy standards and practices for the industry. Many large advertising networks voluntarily follow the standards set by the NAI, including AOL's Tacoda, DoubleClick, Yahoo, and Traffic Marketplace. These standards include a requirement that ad networks not collect personally identifiable information and a requirement that ad networks provide an opt-out cookie so that a user can choose not to be tracked. Opt-outs allow a user either to opt out through the specific ad network's website or to opt out of all participating networks through the NAI's website.

### **Regulatory Developments**

While the on-line advertising industry is creating bodies of privacy standards through self-regulating initiatives, most consumers remain ignorant of how and when behavioral profiles are created through their web use. In December 2007, the U.S. Federal Trade Commission echoed the NAI's work and proposed a list of principles similar to those of the NAI, giving a sort of seal of approval to the manner in which the industry is regulating itself. On the heels of the Google – DoubleClick merger and amidst growing privacy concerns, the New York Assembly introduced Bill A09275 known as, the "Third Party Internet Advertising Consumers Bill of Rights Act of 2008," to establish policies for how advertising networks collect the behavioral profiles of online consumers. If enacted, this law would codify in large part the principles to which many ad networks voluntarily prescribe by agreeing to the standards set forth by the NAI.

### **Finding Balance**

Recognizing that e-havioral marketing has strengths for both advertisers and consumers due to the high relevance of targeted advertisements, we predict that the battle of information collection versus privacy will continue. The level of anonymity users' desire in their web experiences will have to be balanced with the convenience of free online services funded by advertising dollars.

*If you are interested in more information regarding e-havioral marketing or internet related enterprises, please contact Jill Fishbein, a partner at Carr & Ferrell, a Silicon Valley technology law firm specializing in representing emerging companies and investors.*