SHEPPARD MULLIN
SHEPPARD MULLIN RICHTER & HAMPTON LLP
Covering Your Ads BLOG
Legal issues affecting interactive, sports and entertainment marketing and promotion

Covering Your Ads

Posted at 5:25 AM on April 14, 2010 by Sheppard Mullin

Efficiency v. Privacy: Is Online Behavioral Advertising Capable of Self-Regulation?

The Dilemma

In what began as an innovative way to improve advertising efficiency, online behavioral advertising has spawned "Big Brother"-type fear among watch-dog groups worried about consumer privacy. According to the advertising industry's "Self-Regulatory Principles For Online Behavioral Advertising," online behavioral advertising is "the collection of data from a particular computer or device regarding Web viewing behaviors over time . . . 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." In a recent Annenberg study, 66 percent of American adults indicated they did not want websites or networks targeting advertisements to them. Representing the other side of the spectrum, a representative of the American Association of Advertising Agencies has explained, "[M]arketers want their messages delivered to the customer most likely to buy—that is both economically efficient and completely sustainable in a consumer-driven, competitive marketplace." The dilemma is thus presented: how to balance the privacy concerns surrounding the collection of private information with the need to subsidize the availability of online content through effective and cost-efficient advertising. This is the dilemma that will eventually be addressed one way or another, either through continued industry self-regulation, or through actual regulation.

Self-Regulatory Principles for Online Behavioral Advertising

Despite a few states passing legislation regulating behavioral marketing, Congress has yet to enact a comprehensive federal law, nor has the Federal Trade Commission ("**FTC**") implemented mandatory rules. At least, not yet. Instead, the FTC offers "Self-Regulatory Principles For Online Behavioral Advertising" (the "**Guidelines**") which, as its name suggests, are nonbinding suggestions strongly encouraging the advertising industry to behave. The February 2009 revised Guidelines once again featured four key principles: Transparency and Consumer Control, Reasonable Security and Limited Data Retention, Affirmative Express Consent for Material Changes, and Affirmative Express Consent to Using Sensitive Data for Behavioral Advertising. While the interactive advertising industry promulgated its own "Self-Regulatory Principles For Online Behavioral Advertising" in July of 2009, the FTC's Guidelines make it clear that principles alone will not be enough to prevent rulemaking in this area, stating

that the FTC will continue to "evaluate the development of self-regulatory programs and . . . conduct investigations, where appropriate, of practices in the industry to determine if they violate Section 5 of the FTC Act or other laws."

Two particular concerns raised in the FTC Guidelines are the adequacy of opt-out or opt-in mechanisms and the scope of off-limits personal information. As reported in the Guidelines, the major search engines in the United States have introduced new tools that allow consumers to opt-*out* of receiving targeted online advertisements. However, critics have supported a more transparent opt-*in* mechanism, which would require consumers to affirmatively provide their express consent before their personally identifiable information is collected for behavioral advertising purposes. The Guidelines do not choose sides in the "opt-in" or "opt-out" debate, choosing instead to admonish advertisers that the choice mechanism should "be clear, easy-to-use, and accessible to consumers."

Two exclusions are particularly noteworthy in the Guidelines. The first is the exclusion of "first party" behavioral advertising and the second is the exclusion of "contextual advertising" from the scope of the Guidelines. Due to the "first party" (aka "intra-site") exclusion, an online retailer's website may collect consumer information to deliver targeted advertising at its own website so long as it does not share that information with third-parties. For example, Amazon.com may recommend a book based upon the consumer's prior purchases or browsing patterns, but it cannot transmit that information to other non-Amazon affiliated websites and still avail itself of the "first party" exclusion.

Under the "contextual advertising" exclusion, online retailers may target ads based on a search made by the consumer within the very website that the consumer is viewing. An ubiquitous example of this is Google AdWords, which triggers sponsored search results (i.e. ads) to be displayed based on the keywords that are used in the search. But the exclusion also arguably applies whenever a search functionality is used to search solely within the framework of the site that offers it.

Facebook's Beacon Settlement

Representing an example of the privacy issues associated with online behavioral advertising is Facebook's Beacon program. Launched in November 2007, Beacon allowed consumer information to be transmitted from affiliated retailers to Facebook and ultimately shared that information with the Facebook members' friends. Equipped with an allegedly ineffective opt-out mechanism (a brief pop-up window), every time a Facebook user purchased, downloaded, subscribed, or viewed something at one of the participating online vendors, Beacon first triggered a script that utilized cookies to obtain information from the user's computer, and then shared news of the Facebook members' activity with their friends. As an example of the process, Sean Lane reportedly bought a ring for his wife from overstock.com only to have the purchase, along with the 51 percent discount he received, automatically published as a news headline on his Facebook wall visible to everyone in his online network, including friends, co-workers, acquaintances, and his wife.

After a flurry of bad press, Facebook switched its Beacon program from an opt-out to an opt-in

arrangement. Nevertheless, a class action lawsuit was filed against Facebook, Blockbuster, Fandango, Hotwire, STA Travel, Overstock.com, Zappos.com, and Gamefly claiming that the Beacon program violated the Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Video Privacy Protection Act, California Consumer Legal Remedies Act, and California Computer Crime Law. Lane v. Facebook, Inc., N.D. Cal., Case No. 5:08-cv-038450. At the crux of the complaint were Beacon's allegedly "inadequate" and "deceptive" efforts to obtain a user's consent before involving them in the Beacon program.

On September 17, 2009, the class action plaintiffs filed a Settlement Agreement in the U.S. District Court for the Northern District of California calling for a settlement fund of $9.5 million, out of which up to $3 million in attorneys' fees and administrative costs will be paid. Also, "in recognition of their efforts on behalf of the [c]lass," the 19 representative plaintiffs will receive a total of $46,000, with awards of either $15,000, $7,500, or $1,000 depending on their contribution during litigation. Finally, Facebook, with what is left of the $9.5 million settlement fund, will establish a nonprofit Privacy Foundation "to fund projects and initiatives that promote the cause of online privacy, safety, and security." On March 17, 2010, Judge Richard Seeborg of the U.S. District Court for the Northern District of California approved this "cy pres" type of settlement, which often results in the creation of a foundation when locating every individual class plaintiff is difficult.

While on the surface it may seem like the plaintiff class "won" here, in fact, Facebook will likely receive much of the settlement fund back if class members fail to claim it, and Facebook will use those amounts to implement programs that, under state and federal law, it arguably has a legal duty to implement anyway (*See*, *e.g.*, *In re The TJX Companies, Inc.*, FTC Docket No. C-4227 (July 2008)(FTC consent order requiring the subject to implement "a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."); and Cal. Civ. Code § 1798.81.5 (b) (providing, "A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices . . . to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.").

Possible Congressional (Re)Action

With Beacon serving as a banner for their cause, various consumer groups, industry representatives and members of Congress have been calling for expansive government regulation of online behavioral advertising. Even FTC Commissioner Jon Leibowitz said, "Industry needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite legislation by Congress and a more regulatory approach by our Commission." On the other hand, Randall Rothenberg, President and CEO of the Interactive Advertising Bureau ("**IAB**"), said, and understandably so considering his business interests, "We support the FTC's call for industry self-regulation and we are very pleased that the commission endorsed the IAB's analysis of the value of the ad-supported Internet." Indeed, recognizing that actions speak louder than words, the IAB launched an educational campaign about behavioral advertising and recently declared that the campaign was a success.

Nonetheless, recent FTC hearings make it seem like some level of federal legislation is inevitable. Leading the charge is Rep. Rick Boucher, D.-Va., who heads the House Energy and Commerce Subcommittee on Communications Technology and the Internet, with the help of Rep. Cliff Stearns, R.-Fla., and Rep. Joe Barton, R.-Texas. They have drafted at least one bill that would regulate behavioral advertising and require heightened disclosure and visibility when users' internet activity is being tracked. In a June 2009 House subcommittee joint hearing, Boucher indicated that the new bill would require that: (i) consumers be given "clear, concise information in an easy-to-find privacy policy about what information a website collects about them," and how it is used and stored; (ii) consumers be able to opt-*out* of first party targeted ads including "use by third parties or subsidiaries who are part of the company's normal first party marketing operations;" and (iii) consumers be able to opt-*in* to sharing the collected information with unaffiliated third parties.

Conclusion

Without the *quid pro quo* between advertisers, publishers and consumers, premium content that is ad supported and, therefore, free or low-cost to users will be in jeopardy. But absent effective and continuously evolving self-regulation, the players in the online advertising ecosystem risk consumer mistrust, government regulation, and possibly much more.

Authored by:

Benjamin R. Mulcahy
(212) 634-3030
bmulcahy@sheppardmullin.com

and

Dante M. DiPasquale
(212) 634-3092
ddipasquale@sheppardmullin.com