ReedSmith

Advertising, Technology & Media Alert

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Amy S. Mushahwar
Associate, Washington, D.C.
+1 202 414 9275
amushahwar@reedsmith.com

John P. Feldman
Partner, Washington, D.C.
+1 202 414 9230
jfeldman@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

FTC Releases Revised Behavioral Advertising Guidelines

Staff Report May Trigger New Marketing Practices for Your Organization

On February 12, 2009, the Federal Trade Commission (FTC) staff issued a *supplemental report* of its December 2007 draft "Self-Regulatory Principles for Online Behavioral Advertising." The report further develops the FTC's voluntary best practices for the behavioral advertising industry and supports continued self-regulatory treatment. However, the document is not an endorsement of the status quo. The revised principles are likely to spur the following changes to your company's treatment of behavioral advertisements, including: (1) the development of more consumer education content regarding behavioral advertising, (2) the development of internal privacy protections for anonymous data profiles, (3) the creation of opt-in customer notice mechanisms for use and collection of information perceived as sensitive (such as, information related to health, finance, or children), and (4) the creation of opt-in customer notice mechanisms for retroactive changes to your company's privacy practices.

Further, you may think that existing website billboard privacy polices are sufficient for conformance with the FTC's revised guidelines. This is unlikely. The staff report clearly indicates that static privacy policies may not be sufficient notice for behavioral advertising purposes, and disclaimers in proximity to the targeted advertisements may be needed. Notwithstanding the additional disclaimers outside the privacy policy, traditional billboard privacy policies may need revision to conform to the new guidelines, as well. Specifically, the staff report adopted a very broad and open-ended definition of PII[1] for these purposes, and indicated that the sharing of information inside a corporate family could fall outside the "first party" sharing of data exemption.

While it is tempting to ignore a cumbersome (and voluntary) examination of information policy, the staff report also comes with a fair warning to take these guidelines seriously. The concurrences of Commissioners *Jones Harbour* and *Liebowitz* indicate that if companies do not engage in these voluntary regulatory efforts, mandatory behavioral advertising regulation could lie ahead. As stated by Commissioner Leibowitz, "[p]ut simply, this could be the last clear chance to show that self-regulation can—and will—effectively protect consumers' privacy in a dynamic online marketplace."

What is Behavioral Advertising?

Behavioral advertising is the practice of tracking an individual's online activities in order to deliver advertising tailored to the person's specific interests. Since 1995, the FTC sought to understand the online marketplace and the attendant privacy concerns for consumers. As a part of this effort, in 2007, the FTC held a town hall meeting regarding behavioral advertising, and published the *initial staff report* for public comment. The initial staff report identified four self-regulatory online behavioral advertising principles, including:

- Greater transparency and consumer control of behavioral advertising issues by offering consumers notice and choice before collecting behavioral advertising data
- Limits regarding the length of time companies retain consumer data and the provision of reasonable security for that data
- Customer notice and consent in the event of a material change in the company's privacy practices
- Affirmative notice before "sensitive data" is collected regarding an individual's activities online.

The current staff report responds to the comments submitted by individual companies, business groups, academics, advocates and individual consumers in this proceeding. And, most of the changes to the principles are intended to clarify the applicable scope of the principles and the steps necessary to conform to the principles, as more fully discussed below.

Scope of the Principles

In the report, FTC staff defines behavioral advertising as "the tracking of a consumer's online activities over time—including the searches the consumer has conducted, the web pages visited, and the content viewed—in order to deliver advertising targeted to the individual consumer's interests." As described more fully below, FTC staff clarified that this definition and the corresponding guidelines, (1) apply to the collection and use of PII and non-PII, (2) does not apply to "first party" collection and use of data, and (3) does not apply to contextual advertising—advertising based only on the content of a particular website or search query.

Applicability to Non-PII

Despite considerable industry criticism that the principles should not impose obligations to the collection and use of non-PII, the staff report clearly indicates that distinction of PII versus non-PII is not determinative of the applicable privacy treatment. Historically, the FTC only directed its privacy concerns toward PII or information that would make an individual uniquely identifiable. But, in the behavioral advertising marketplace, the staff report acknowledges that the traditional PII distinctions are becoming obsolete. Anonymous user data (non-PII) can be linked to PII if a user enters in personal data during a web session. Or, data that was traditionally considered anonymous non-PII can morph into PII with the advent of new technologies. For example, staff mentions the transition to Internet Protocol version 6 (IPv6), as a case where a traditional form of non-PII, an IP address, could become a uniquely identifiable piece of data.[2]

As a result, the FTC has retooled its previous approach and "any data collected for online behavioral advertising that reasonably could be associated with a particular consumer or a particular computer or device" should be subject to the privacy principles. With this approach, a company does not need to possess the individual's email address, name, or other unique identifier to be subject to the rules. The fact that an advertiser, over time, could develop a profile sufficiently detailed that it could become identified with a particular person is enough.

First Party Behavioral Advertising

"First Party" behavioral advertising is exempt from the guidelines. The practice is defined as behavioral advertising by and at a single website. Staff identified that behavioral advertising targeted at a specific website is more likely to be consistent with existing consumer expectations. Given the direct relationship between the consumer and the website, the consumer should understand why he received the targeted recommendation. The direct relationship also permits the customer to raise concerns with the website if the consumer objects to the advertising practices at issue.

The staff report also clarifies that website publishers may contract with third-party vendors to facilitate "first party" behavioral advertising. So, a web publisher could contract with third-party advertisers for behavioral advertising *limited to that website*. The typical practice of third-party network ad servers would not be exempt—if network servers collect data for use on more than one website. And, even third-party data-use among affiliated company websites could be subject to the principles.

Contextual Advertising

"Contextual Advertising" is also exempt, but the staff devised a very limited definition of this practice. Contextual advertising is limited to advertising based on a consumer's current visit to a single web page or a single search query that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or a search result. Any time that the advertiser collects or retains "consumer data for future purposes beyond the immediate delivery of an ad or search result, the practice does not constitute contextual advertising." This narrow definition would require any aggregator website[3] (search, shopping or otherwise) to carefully limit data-retention to the immediate delivery of a search result to rely on this exclusion.

Self – Regulatory Principle Revisions

Notice and Choice

In 2007, staff sought comment on whether websites using behavioral advertising must give consumers notice and choice before collecting any behavioral advertising data. The supplemental report issued the following clarifications:

> **Disclosure & Consent:** To conform to these principles, websites must give consumers notice and choice before collecting behavioral advertising data. The staff report did not clarify if the

choice should be opt-in or opt-out. Instead, the staff report states that the disclosure and choice mechanism must be "clear, easy-to-use and accessible." Because the FTC requires opt-in consent for specific circumstances, such as "sensitive data," described more fully below, it could be reasonable to assume that all other circumstances could be undertaken with opt-out consent.

Traditional Notice Mechanisms Questioned: As discussed above, staff cast into doubt the sufficiency of current means of providing privacy notice and choice to consumers. The first means discussed was the consumer privacy policy. Staff indicated that privacy policies are long and difficult for most consumers to understand. Further, traditional privacy policy billboards are not always formatted to be seen on the increasing number of hand-held devices accessing the Internet. The second means discussed was the use of opt-out cookies.[4] The staff report mentioned that consumers often delete opt-out cookies by choice or automatically thorough the use of anti-spyware applications. Thus, if an opt-out cookie is deleted, it would appear to the behavioral advertiser as if the user consented to behavioral advertising.

Recommended Disclosure Methods TBD: The staff report made no firm recommendations for alternative consumer disclosure. Instead, staff encouraged the industry to create innovative disclosure methods outside of the privacy policy. The staff's report only identified that some solutions that "looked promising" with future study (one example of this includes a "why did I get this ad" link in proximity to a behavioral advertisement). While lack of defined notice standards allows industry to innovate and develop custom solutions, there is a potential for regulatory uncertainty as the FTC did not provide a "safe harbor" method to avoid inadvertent deceptive advertising violations.

Reasonable Security and Limited Data Retention

Under this principle, companies that collect or store data for behavioral advertising should provide "reasonable security" for that data. The staff report clarified the reasonable security requirement in response to commenters' objections that the principle was too vague. By clarifying the requirement, the staff report did not mandate a particular technology. Instead, the FTC staff developed a scalable standard based on the context of the data at issue and in keeping with existing data security law. "Protections should be based on the sensitivity of the data [and] the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company." As for data retention, staff clarified that data retention requirement is merged into the data security principle. The text of the data retention provision remained unchanged and states that companies should retain data only as long as it is necessary to fulfill "a legitimate business or law enforcement need."

Affirmative Consent for Changes in Privacy Practices

The FTC initially proposed that companies obtain affirmative express consent before they use data in a manner that is different from the privacy practices in place at an earlier date. A number of commenters objected to this proposal as administratively cumbersome, and ultimately unworkable. Thus, the staff report limited the affirmative express consent principle to *retroactive* material changes. Under this limitation, if a company makes material changes to its data collection practices and seeks to apply those changes to data collected under earlier privacy practices, it must seek opt-in consent from the affected consumers. However, opt-in consent would not be required for any data collected after the change in privacy practices occurs (and due notice and choice is provided to the consumer, as described above).

The staff report also states that a term would be "material" if it "would likely affect the consumer's conduct or decisions with respect to the company's products or servicers." Staff provided examples of material changes such as, (i) using data for different purposes than described at the time of collection or (ii) sharing data with third parties, contrary to promises made at the time of collections.

Affirmative Consent for the Collection of Sensitive Information

Even though staff acknowledges that the definition of the term "sensitive information" may be complex, the staff report retained this opt-in consent guideline. The staff report did not provide an exhaustive list of what constitutes sensitive data, and instead it called upon those in the industry to address this issue. Staff did reference that some examples of sensitive information would include, "financial data, data about children, health information, sexual orientation, precise geographic location information and Social Security numbers."

Why This Matters

The principles, for the moment, are voluntary guidelines and do not confer legal liability in the event of noncompliance. However, as stated above, mandatory regulations could emerge if the FTC remains concerned about the industry use of behavioral advertising data. Further, in the event that a consumer alleges that your company's behavioral adverting practices are deceptive and unfair trade practices, evidence that your company complied with the FTC's guidelines may be used to avoid liability.

_____

1 Personally Identifiable Information: traditionally, this term is defined as an individual's name, social security number, or any other information that would make an individual uniquely identifiable.

2 IPv6 will exponentially increase the number of unique IP addresses, lessening the current reliance on DHCP servers that recycle a pool of IP addresses assigned to a particular network. Instead, more networks will assign static IP addresses, which can link a particular IP address to an individual's device on a network.

3 Aggregator websites are websites that cross reference sales inventory databases on other websites. This enables the consumer to receive competitive quotes from multiple vendors. To complete the sale, aggregator websites can have independent online shopping-cart features or can link to the original inventoried website.

4 Opt-out cookies are essentially cookies used to avoid other cookies. Accepting an opt-out cookie blocks future cookies from being installed on your browser by a particular website server or advertiser. It essentially lets you declare that you do not wish to participate in targeted ad delivery, profiling or otherwise have your web browsing tracked. An opt-out cookie will only block cookies from a particular server and is not a generic tool to block cookies from any site you visit.

About Reed Smith

Reed Smith is a global relationship law firm with nearly 1,700 lawyers in 23 offices throughout the United States, Europe, Asia and the Middle East.

Founded in 1877, the firm represents leading international businesses, from Fortune 100 corporations to mid-market and emerging enterprises. Its lawyers provide litigation services in multi-jurisdictional matters and other high-stakes disputes; deliver regulatory counsel; and execute the full range of strategic domestic and cross-border transactions.

Reed Smith is a preeminent advisor to industries including financial services, life sciences, health care, advertising, technology, media, shipping, energy trade and commodities, real estate, manufacturing, and education. For more information, visit **reedsmith.com**

This *Alert* is presented for informational purposes only and is not intended to constitute legal advice.

© Reed Smith LLP 2009. All rights reserved.

"Reed Smith" refers to Reed Smith LLP, a limited liability partnership formed in the state of Delaware.

ReedSmith
The business of relationships.℠

NEW YORK
LONDON
HONG KONG
CHICAGO
WASHINGTON, D.C.
BEIJING
PARIS
LOS ANGELES
SAN FRANCISCO
PHILADELPHIA
PITTSBURGH
OAKLAND
MUNICH
ABU DHABI
PRINCETON
N. VIRGINIA
WILMINGTON
SILICON VALLEY
DUBAI
CENTURY CITY
RICHMOND
GREECE