

FTC Releases Online Behavioral Advertising Principles: Industry Put On Notice to Comply or Face Further Investigation, Enforcement and Legislation

INTRODUCTION AND WHY THIS IS IMPORTANT TO YOU

On February 12, 2009, the Federal Trade Commission (“FTC”) Staff issued a report entitled “**FTC Staff: Principles for Self-Regulation of Online Behavioral Advertising**” (“Staff Report”), approved for release by a unanimous Commission vote. The report details the findings of the FTC Staff’s continued review of online behavioral advertising practices and revises its proposed principles for the self-regulation of such practices (“Revised Principles”). The report and the Revised Principles themselves are crucial for any online advertiser and any operator of a website that accepts online advertising, and could foreshadow enforcement actions, possible legislative action, and further investigation of the industry by the Commission, perhaps in the form of compulsory process, all in the near term. Needless to say, 2009 will be an important year for online advertisers and their service providers.

The Revised Principles are advisory only, as a matter of strict legal interpretation, but, significantly, the Staff Report makes clear that “where appropriate [the Commission will] investigate possible unfair or deceptive acts or practices in violation of the FTC Act.” The Report is therefore as notable for what it does say as what it does not: nowhere in the document does the Staff make clear the extent to which the Commission considers the Revised Principles as a whole, or any one of them, to be at or near the threshold necessary to comply with Section 5 of the FTC Act. Clarification may come in the form of enforcement actions and/or legislative proposals.

It is also notable that the Commission believes that the behavioral advertising industry may be close to losing control over its own regulatory regime. Commissioner Leibowitz, the most active Commissioner on behavioral advertising issues, states in his **concurrence** that “this could be the last clear chance to show that self-regulation can – and will – effectively protect consumers’ privacy in a dynamic online marketplace.” The implication is that the Commission is close to proposing or supporting legislation governing the behavioral advertising industry. Some in Congress, including Rep. Boucher (D-VA), chairman of the House Subcommittee on Communications, Technology and the Internet, have **signaled similar reservations** about the effectiveness of self regulation of online behavioral advertising and an interest in legislating in this area. Now is the time for behavioral advertisers and their service providers to join and support strong self-regulatory programs such as the Network Advertising Initiative (“NAI”).

A detailed review of the Staff Report and Revised Principles follows.

BACKGROUND

The Revised Principles are the latest step in the FTC’s effort to address how online behavioral advertising should be self-regulated. Recent activity includes the FTC’s Town Hall meeting discussing online behavioral advertising on November 1-2, 2007, as well as the **FTC’s proposed self-regulatory principles, released on December 20, 2007**. The NAI released its revised NAI Principles Code of Conduct in

December 2008 (“NAI 2008 Principles”). **The NAI 2008 Principles** were created in response to the FTC’s proposed principles and as a timely update of the NAI’s Principles for Online Preference Marketing, which were approved by the FTC in 2000.

Scope: Principles Do Not Include Behavioral Advertising in First Party Context, Contextual Advertising, or Certain Non-PII

The Commission’s 2007 proposed principles used a very broad definition of behavioral advertising: “the tracking of a consumer’s activities online 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.” Notably, this definition included not only cross-site tracking, such as that used by network advertisers, but also (1) single-site or domain tracking that is now commonly used by website operators to personalize their sites’ content and advertising (“first party” relationship), (2) contextual advertising, and (3) all data collected for purposes of behavioral advertising, even if the data are not personally identifiable.

First Party Relationships and Contextual Advertising

The Revised Principles narrow this definition significantly. Specifically, they exclude from their coverage advertising that would otherwise meet the definition of “Behavioral Advertising” if it is in the form of a first party relationship, or if it is merely contextual. Contextual advertising is defined as “the delivery of ads based upon a consumer’s current visit to a single web page or a single search query, without the collection and retention of data about a consumer’s online activities over time.”

PII/Non-PII Distinction Revised

Moreover, the Revised Principles do not cover *all* information collected about consumers for behavioral advertising purposes, but rather only that information that “reasonably could be associated with a particular consumer or with a particular computer or device.”

This position is a middle ground between what industry and some advocates pushed for and is significant for its clear implication that even certain data that has traditionally been considered non-personally identifiable information (“PII”) should be subject to privacy protections. The scope of information covered is potentially vast. As the Staff Report explains: “Whether information ‘reasonably could be associated’ with a particular consumer or device will depend on the factual circumstances and available technologies, but would include, for example: clickstream data that, through reasonable efforts, could be combined with the consumer’s website registration information; individual pieces of anonymous data combined into a profile sufficiently detailed that could become identified with a particular person; and behavioral profiles that, while not associated with a particular consumer, are stored and used to deliver personalized advertising and content to a particular device.” The Commission staff appears to have taken the position that the era of arguing that privacy regulation turns on whether or not the data collected or used are personally identifiable is over.

The Revised Principles

Transparency and Consumer Control – Call For Notice Outside of the Privacy Policy

The Revised Principles retain, from the 2007 proposal, the principle of transparency and control. The FTC Staff’s implementation of this principle, however, is striking in its departure from current industry practices. The Revised Principle calls for every website where data is collected for behavioral advertising to provide consumers with “a clear, concise, consumer-friendly, and prominent statement” disclosing the collection of consumer data and that consumers can choose whether to have information about their activities collected and used for these purposes. The Staff Report further calls for “a clear, easy-to-use, and accessible means” for consumers to exercise their choice. While the Report does not say so expressly, this is not an opt-in standard.

That said, it is a very high disclosure standard. The FTC Staff recognizes that it is customary to provide notice and choice in a website's privacy policy, but it notes that "privacy policies have become long and difficult to understand, and may not be an effective way to communicate information to consumers." Staff therefore "encourages" companies to develop innovative methods of providing notice and control over data collection for behavioral advertising *outside* of the privacy policy. Staff also suggests that in developing effective disclosure mechanisms, companies should look to empirical research.

Finally, the Staff Report is critical of the cookie based opt-out method used by most in the industry today, since, by using anti-spyware software or deleting cookies from their browsers, consumers may block or delete their opt-out cookies. The Staff "encourages interested parties to examine this issue and explore potential standards and other tools to assist consumers."

Data Security and Data Retention for Information Collected Through Behavioral Advertising – Sliding Scale Used by FTC in Other Contexts

The Revised Principles do not include any substantive revisions regarding data security and data retention, but rather clarify that data retention is one part of providing reasonable security. As a result, the Revised Principles combine the previously separate data security and data retention principles. The Revised Principles continue to call for companies to provide reasonable security for consumer data collected for behavioral advertising purposes, consistent with data security laws and FTC enforcement actions and guidance. Further, the type of protection may be flexible, on a sliding scale depending on the sensitivity of the data, the nature of a company's business, the risks faced, and the reasonable protections available. Additionally, the Principles provide that the data should be retained only as long as is necessary to fulfill a legitimate business or law enforcement need.

Changes to Privacy Policies – Notice and Opt-In Consent for Material Changes Applied Retroactively

The Revised Principle clarifies that the FTC Staff intended for its previously proposed principle to apply only to privacy policy changes that are both *material* and *retroactive*. Under the Revised Principle, a company must obtain affected consumers' affirmative express consent before using their previously collected data in a way that is materially different from the uses permitted under the privacy policy in place when the data was collected. The FTC Staff states that material *prospective* changes to privacy policies would require a more flexible approach that could include prominent notice and opt-out choice. The Revised Principle is consistent with the NAI 2008 Principles, which state that consumer data collected prior to a material change in a privacy policy may only be used as described in the privacy policy in place when the data was collected, unless the consumer opts into permit the previously collected data to be used in the new way.

Implications Outside the Behavioral Advertising Industry

The FTC Staff cite to two matters – *In the Matter of Gateway Learning Corp.* and *In the Matter of Orkin Exterminating Co.* – in support of its call for opt-in to retroactive, material changes to privacy policies. Significantly, neither of these cases involved network advertising. It may, therefore, be fairly assumed that the Commission believes that this principle is a requirement for *all* companies with privacy policies – not just to meet industry best practices, but also to avoid an enforcement action under Section 5 of the FTC Act, which prohibits unfair and deceptive practices in or affecting commerce. This principle would require a significant departure from current industry practices. It also leaves open the question of whether a statement in a privacy policy about how the policy may be revised would trump the opt-in principle. If not, we may be headed toward a conflict between consumer protection

law and developing jurisprudence regarding the enforceability of online contracts. This may be especially true for privacy policies to which consumers must agree through an affirmative act, such as by clicking on an “I Agree” button.

Sensitive Data – Opt-In Consent for Use in Behavioral Advertising

The Revised Principles urge companies to obtain affirmative express consent before collecting sensitive data for behavioral advertising. While the FTC Staff does not provide an exhaustive definition of “sensitive data,” the Staff Report indicates that financial data, data about children, health information, precise geographic location information, and Social Security numbers would be considered sensitive data. The FTC Staff calls on industry members and relevant stakeholders to develop specific standards surrounding the definition and use of sensitive data. The Revised Principle is consistent with the NAI 2008 Principles, which also require a consumer’s opt-in consent before using his/her sensitive information for behavioral advertising.

CONCLUSION

If nothing else is clear from the FTC Staff Report and Revised Principles, it is that the Commission believes self-regulation can and should be improved, and that this needs to happen quickly. Whether or not this is true is almost immaterial: if the Revised Principles are not embraced by industry, the FTC will almost certainly undertake further, more formal investigation of the industry, enforcement actions, and/or potential calls for legislation. How the industry reacts to the principles in 2009 will therefore very likely determine how the industry will be regulated for years to come.

KELLEY DRYE & WARREN LLP

Kelley Drye & Warren’s Privacy and Information Security Practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients’ customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

For more information about this Client Advisory, please contact:

D. REED FREEMAN, JR.

Kelley Drye & Warren LLP

(202) 342-8880

rfreeman@kelleydrye.com