Arnall Golden Gregory LLP

Client Alert

Contact Attorneys Regarding This Matter:

Seth A. Cohen
404.873.8102 - direct
404.873.8103 - fax
seth.cohen@agg.com

Matthew V. Wilson
404.873.8551 - direct
404.873.8552 - fax
matthew.wilson@agg.com

If You Give a Mouse a Cookie: Practical Observations on the FTC's Revised Self-Regulatory Principles for Online Behavioral Advertising

Last month the Federal Trade Commission (the "Commission"), as part of its ongoing public dialogue regarding consumer privacy protection online, released a staff report (*FTC Staff Report: Self Regulatory Principles for Online Behavioral Advertising*) (the "Report") assessing the effectiveness of the current self-regulatory environment as it pertains to online behavioral advertising. The Report (i) summarizes the comments received from online advertising companies, trade associations and consumer advocacy groups that were submitted to the Commission in response to the proposed "self-regulatory principles for online behavioral advertising," released in December, 2007 (the "Principles"), and (ii) provides specific analysis of, along with additional modifications to, the Principles.

Rather than summarize the Report (summaries of the report are available at the FTC's website (www.FTC.gov) and in articles that have been recently published by other topical commentators), this Client Alert provides certain practical suggestions and related advice that all online advertising companies should consider when incorporating the Principles into their own practices. It is important to note, however, while the Principles generally reflect the standards of existing U.S. law, they are simply guidelines for self-regulation and do not alter, enhance or diminish the obligation of any company to comply with applicable federal and state laws.

1. **"PII – It is more than what you think it is."** One conclusion that may be drawn from the Report is that the Commission staff recognizes the rapidly diminishing distinction between the traditional concept of personally-identifiable information (PII) and non-PII. Although several commentators and industry insiders have argued in favor of limiting the scope of information that constitutes PII, the Report outlines several reasons why the traditional definitions and distinctions are quickly losing their validity as the result of technological innovation and shifting consumer expectations. Moreover, as the proliferation of online advertising generates more geospatial data, this antiquated distinction will continue to fade at an even faster rate as identities become more inferable based on geographic inquiries and preferences. In light of this convergence of what has been historically viewed as two mutually exclusive categories of information (subject to different levels of regulation), online advertisers should consider implementing policies that address each of the following:

Arnall Golden Gregory LLP
Attorneys at Law
171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031
404.873.8500
www.agg.com

a. **Periodic internal audits reviewing the types and nature of information collected with respect to online consumers, as well as "blind-testing" of that data to determine whether the identities of online consumers can be inferred from the data.**
b. **Assessments of the nature of any geospatial data collected to determine whether that data is being maintained, stored and secured like "traditional" PII.**
c. **Consider strategies that may anonymize certain data that may be deemed non-PII by traditional standards, but that, understanding the Commission's position, might be categorized as "merged" PII so as to avoid having such information subject to the heightened security and retention standards that apply to "traditional" PII.**

2. **"If you give a mouse a Cookie…"** In addition to discussing the nature of, and the eroding distinctions between, the traditional categories of information collected (PII vs. non-PII), the Report also provides various cautionary observations that apply to the storage, use and security of certain non-PII data captured electronically. To paraphrase from a popular children's storybook, "if you give a mouse a cookie, he will probably want a glass of milk. And if you give him a glass of milk, he'll probably…" and so on. In many respects, the use of electronic "cookies" to collect consumer data creates similar temptations and consequences for advertisers; once an opportunity to capture and utilize information collected utilizing "cookies" is known within an organization, it is often difficult to limit the desire of such advertisers to use that information in a myriad of ways.

   This temptation is not only internal to the party collecting the information; it also extends to third-parties who may have access to the "cookie" information. As a result, advertisers that collect and retain such information should also confirm that third parties with access to "cookie" data implement security measures that are reasonable in light of the sensitivity of such data. Furthermore, advertisers that share collected information with unaffiliated third parties should employ policies that ensure that those third-parties secure the shared data in a manner that is consistent with the advertiser's own policies and contractually limits the receiving party's use and retention of the information such that it is not misused or retained for an unreasonable period of time. Based on the foregoing, businesses that engage in online advertising should consider implementing policies that address each of the following:

   a. **Conduct periodic internal audits concerning the company's usage and retention of cookie-derived PII and non-PII.**
   b. **In connection with discussions with any third-party that may have access to cookie-obtained information or other clickstream data, employ a "due diligence" checklist to assess such party's alignment with the Principles and the "scalable standard" of security referenced in the Report.**
   c. **In addition to maintaining and adhering to external-facing privacy policies, develop an internal protocol incorporating a "scalable standard" relating to employee access to, and usage of, information derived from behavioral advertising technologies.**

3. **"First Party" Uses – Make sure nobody else is at the party.** As stated in the Report, the Commission staff believes that "first-party" uses of collected data (use of data tracking technologies on and for a single website) does not necessarily warrant the protections suggested by Principles because such collection and use is largely transparent and is consistent with typical consumer expectations. However, the Report carefully hedges this conclusion, noting that their receipt of limited comments on this issue and the rapid technological changes may cause them to revisit their assessment of this issue in the near future. One thing is certain, for online advertisers that use a "front page" format utilizing third-party links and/or frames, the determination as to whether the host or the third-party constitutes the "First Party" with respect to certain data may be a matter of dispute. Similarly, while sophisticated advertisers have developed interstitial tactics designed to demark when an online consumer is departing from a first party website, evolving mobile technologies tend to make this distinction and capability more challenging. Accordingly, businesses that engage in online advertising should consider implementing policies that address each of the following:

    a. **Assess whether your current privacy policy adequately covers various first party usages of collected information that may not be reasonably inferred by the existing policy terms.**
    b. **In connection with negotiations or discussions with any third-party that may provide data to be incorporated in a website, clarify the relative usage limitations applicable to such information and clearly designate the "First Party" user.**

The current iteration of the Principles and the Report are the Commission's most recent, but certainly not its final, word on this subject. As technology evolves and the overlapping nexus between the goals of online advertisers and consumer privacy advocates become more difficult to discern, the likelihood for expansive regulation will increase. To be sure, the Commission will maintain a watchful eye over the industry, particularly as competitors seek to employ the use of new tools designed to strengthen the effectiveness of online behavioral advertising (see the recent reports that Google and WPP have joined together to research the way psychology and neuroscience help assess the relevancy of web advertising). Accordingly, prudence dictates that companies and their advisors remain diligent in their collective efforts to anticipate the regulatory nuances that are certain accompany each new advancement in technology.

For more information on the Report, the Principles, PII/non-PII and other matters raised in this Client Alert, please call **Seth A. Cohen, Esq.** at 404-873-8102 or **Matthew V. Wilson, Esq.** at 404-873-8551.