THE
NATIONAL LAW REVIEW

Technology: Federal Trade Commission (FTC) and Self-Regulatory Frameworks Regarding Online Behavioral Advertising

Tuesday, October 22, 2013

There is no federal statute that speaks directly to OBA, but the FTC has made numerous recommendations.

The online and mobile collection of consumer data for purposes of online behavioral advertising (OBA) raises significant privacy concerns. Many consumers want advertising that is more tailored to their interests. Others may be less enthusiastic about the collection and use of data to serve advertising to them based on inferred or predicted interests.

In the last article in this series, we discuss OBA, the FTC's proposed regulatory framework and guidance for protecting consumer data online, as well as the advertising industry's self-regulatory efforts.

Article By
Labor & Employment Neal Gerber
Neal, Gerber & Eisenberg LLPPublications

Consumer Protection
Antitrust & Trade Regulation
Communications, Media & Internet
All Federal

OBA is generally understood as the collection of data (through a specific computer or device) over time and across multiple, unrelated websites, regarding online activity for purposes of delivering online advertising to consumers based on predictions or inferences drawn from online behavior. OBA is not first-party advertising or in-site contextual advertising. Behavior is tracked and data collected, for example, by the placement of cookies on a consumer's browser, or through apps on and functionality of mobile devices. This information is compiled and used to more effectively serve advertising.

There is no federal statute that speaks directly to OBA. The FTC has made certain recommendations in staff reports over the last several years on privacy issues regarding online data collection, and the advertising industry has responded to these recommendations with its self-regulatory framework. In this regard, the FTC and the advertising industry appreciate the importance of providing consumers with notice and choice in terms of OBA while recognizing OBA as an effective way to serve advertising to consumers.

FTC guidance and recommendations

The FTC has focused on online and mobile data collection issues for several years. In December 2007, the FTC released *Online Behavioral Advertising – Moving the Discussion Forward to Possible Self-Regulatory Principles*, which proposed certain principles to guide the advertising industry self-regulatory efforts. Following a comment period, the FTC issued *Self-Regulatory Principles for Online Behavioral Advertising* in February 2009 (the 2009 FTC Staff Report). The 2009 FTC Staff Report set forth several principles, the most prominent of which were transparency, consumer control and consent.

In December 2010, the FTC released *Preliminary FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (the 2010 FTC Staff Report), again focusing on principles to guide self-regulation of computer-based data collection and OBA through what the FTC calls privacy by design, simplified choice, and greater transparency. In the 2010 FTC Staff Report, the FTC endorsed a Do Not Track mechanism pursuant to which consumers would have increased control over data collection and OBA.

In response to the additional privacy issues associated with mobile devices that enable traditional browsing, but

also allow for geo-location tracking and the existence of thousands of apps that collect data, the FTC issued *Mobile Privacy Disclosures: Building Trust Through Transparency* in February 2012 (the 2012 FTC Staff Report). The 2012 FTC Staff Report called for notice, choice and more transparency with regard to data collection and use in the mobile environment and recognized that there are no clear-cut mobile environment rules to guide consumers or companies.

In March 2012, the FTC issued *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, which set forth the FTC's "best practices" and recommendations for the protection of consumer privacy and control over the data collected in the mobile environment. In this staff report, the FTC again called on companies to adhere to the core principles of privacy by design, simplified consumer choice and enhanced transparency. As with the preliminary staff report of the same name, the FTC again endorsed the development of a uniform Do Not Track mechanism for both online and mobile platforms to prevent tracking and data collection across mobile applications. This staff report also discussed an apparent lack of consumer understanding with regard to the nature and scope of data collection through mobile devices and mobile apps, the need to develop effective privacy disclosures for space-constrained mobile devices and the importance of providing consumers with choice options regarding data collection at the time of download or actual collection or transmission of data ("just-in-time" disclosures).

In terms of OBA, this staff report instructed that, because ad networks and other third parties use and provide code to mobile app developers that facilitate online advertising, these third parties and app developers should have a better understanding of the privacy considerations, how and in what way data is collected and used, and work towards the implementation of a Do Not Track mechanism for mobile consistent with the Do Not Track mechanism endorsed by the FTC for other online activity.

In what may be viewed as a complimentary approach by the FTC with regard to data brokers and the role they play in OBA, the FTC introduced the Reclaim Your Name initiative earlier this summer. With this initiative, the FTC called on the data broker industry to work towards a self-regulatory program that would provide consumers with notice, choice, the ability to access information collected about them online, as well as an opportunity to correct mistakes in the data collected and potentially opt out. Notably, Axiom, one of the largest data brokers, recently launched a site that allows consumers to see the data collected about them and elect to opt out.

Industry self-regulation

In response to the FTC, the advertising industry developed its proposed self-regulatory framework to promote the responsible continued use of OBA and consumer privacy interests. In July 2009, the Digital Advertising Alliance (DAA) released *Self-Regulatory Principles for Online Behavioral Advertising* (the same name as the 2009 FTC Staff Report), which was followed thereafter by the DAA's Implementation Guide in October 2010 (the Self-Regulatory Program). The Self-Regulatory Program corresponds to the FTC guidance and recommendations in the 2009 FTC Staff Report.

Like the FTC's framework, the DAA focused on, among other concepts, education, transparency, consumer control and data protection, and defined OBA to not include collection activities for analytics, first-party and contextual advertising. The DAA principles were designed to apply to the primary entities involved in OBA, including web site publishers or operators, entities engaging in OBA on non-affiliated websites (ad networks and exchanges, and advertisers) and the service providers themselves, and provides for overlapping, coextensive and joint obligations at each level to promote the DAA's principles and ensure appropriate notice and choice for consumers.

The DAA's Implementation Guide also endorsed the use of the Ad Option icon, which is similar to the Do Not Track program, and links consumers directly from an advertisement or site utilizing OBA to consumer notice and choice options. If you look closely at some advertisements served to you online, you may see the Ad Option icon, or a link with text that will take you to a privacy choice menu. The DAA Ad Option is not a one-stop-shop for OBA. Although providing for transparency, notice and choice, the DAA framework still requires consumers to opt-out on a company-by-company basis.

In July 2013, the DAA released *Application of Self-Regulatory Principles to the Mobile Environment*. This self-regulatory program for mobile device and mobile app-based data tracking and collection is consistent with the DAA notice and choice principles for desktop online data collection. The focus of the DAA's mobile program is on companies that engage in OBA through mobile device apps or mobile sites, geo-location tracking and contact information collection.

Additionally, over the last couple of years, the World Wide Web Consortium Tracking Protection Working Group has been working to develop a technical "do not track" standard that could be endorsed by the advertising industry. The DAA had proposed that its self-regulatory program, including Ad Option, should be endorsed by the Working Group. This summer, however, the Working Group rejected the DAA's proposal, which appears to have

resulted in, at least, a halt in this process.

There has been significant effort by both the FTC and the advertising industry to tackle some of the privacy concerns brought into focus by OBA. There are layers of the analysis and additional FTC and industry resources that cannot be addressed in this short article. The point, however, is to recognize that the FTC and the advertising industry are focused on these privacy concerns, and they have set forth recommendations and a self-regulatory framework focused on notice and consumer choice. If you or your client is a publisher, service provider, app developer, advertiser or one of the other entities involved in the interdependent web of online or mobile data collection and OBA, consider these notice and choice frameworks and whether you or your client have or should address potential responsibilities.

This article first appeared on InsideCounsel.com.