NOVEMBER/DECEMBER 2012
VOLUME 18 NUMBER 6

DEVOTED TO INTELLECTUAL PROPERTY LITIGATION & ENFORCEMENT

Edited by the Law Firm of Grimes & Battersby

IP Litigator

Wolters Kluwer
Law & Business

Online Behavioral Advertising: A User's Guide

Lisa J. Sotto and Melinda L. McLellan

Lisa J. Sotto is the managing partner of the New York office of Hunton & Williams LLP where she heads the firm's global Privacy and Data Security practice. Melinda L. McLellan is a New York-based senior associate on the firm's Privacy and Data Security team.

Internet users have expressed increasing concern about efforts to track their online activities. As the online tracking methods used to target advertisements have expanded in both scope and complexity, regulators also have taken notice and have begun to respond to the public's growing privacy concerns. For its part, the advertising industry has asserted that online advertising is essential to maintaining a cost-free Internet for the public, and that privacy fears have been exaggerated given that behavioral advertising generally does not involve the collection of sensitive personal information. This article discusses how legislators, regulators and industry stakeholders are shaping the legal landscape concerning online behavioral advertising.

Online behavioral advertising involves the collection and analysis of information about consumers' online behavior for marketing-related purposes such as serving targeted ads or developing purchase propensity models. Many consumers first focused their attention on targeted marketing when they began to notice advertisements that seemed particularly well-tailored to their interests and previous Internet searches. Although not all reactions to behavioral advertising have been negative – some individuals like having their preferences reflected in marketing efforts directed at them – a fair amount of negative backlash followed revelations that online advertising networks, publishers and others have been monitoring consumers' browsing activities. Recent studies have shown that awareness of online behavioral advertising is up and that consumers are concerned about it.[1]

The Federal Trade Commission ("FTC") has expressed a willingness to work with industry to pursue an effective mechanism for self-regulation. As the United States' primary privacy enforcement agency, the FTC has addressed online tracking at length and has brought several high-profile enforcement actions. These actions illustrate the Commission's commitment to addressing the tracking issue and evidence its efforts to prevent companies from misleading consumers about how online behavior may be monitored. Moves to establish an effective "Do Not Track" ("DNT") mechanism are not proceeding as smoothly as some had hoped, and the current stalemate between industry and government with respect to certain elements of the DNT proposal has led to speculation that Congress may step in.

FTC Encouragement of Self-Regulatory Efforts

For several years, the FTC has urged the online advertising industry to develop a self-regulatory program to address privacy concerns related to behavioral targeting practices. In the interest of moving toward a comprehensive framework for self-regulation, in December 2007, the FTC released a staff report outlining a set of proposed self-regulatory principles related to online behavioral advertising. The principles articulated in the draft were (1) transparency and consumer control; (2) reasonable security and limited data retention for consumer data; (3) affirmative express consent for material changes to existing privacy promises; and (4) affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising.

In response to the FTC's draft principles, in late 2008, the Network Advertising Initiative, a coalition of more than 90 companies in the online advertising industry, developed and published its own self-regulatory code of conduct to encourage transparent use of consumer information (the "NAI Code of Conduct"). The NAI Code of Conduct was broken down into ten categories of requirements that apply to NAI members engaging in online behavioral advertising: (1) transparency; (2) notice; (3) choice; (4) use limitations; (5) transfer and service restrictions; (6) access; (7) obtaining data for online behavioral advertising and related activities from reliable sources; (8) security; (9) data retention limitations; and (10) compliance with applicable law, and to the extent the NAI Code of Conduct exceeds legal requirements, adherence to the NAI's higher standard.

After analyzing dozens of comments received from stakeholders on all sides of the issue, on February 12, 2009, the FTC published its follow-up to the 2007 proposal in a report entitled "Self-Regulatory Principles for

Online Behavioral Advertising." The report covered a wide range of issues including the increasingly blurred line between personally identifiable information and non-personally identifiable information and the applicability of online behavioral advertising regulations to "first party" advertising and contextual advertising. Although the four main principles set forth in the 2007 proposal remained the same, the 2009 report included revisions based on the feedback the Commission had received.

Later that year, on July 2, 2009, a group of five marketing industry associations jointly published its own set of voluntary behavioral marketing guidelines in response to the self-regulatory principles proposed by the FTC in its February 2009 report. Among other objectives, the "Self-Regulatory Principles for Online Behavioral Advertising" called on participating organizations to provide clear disclosures about their online behavioral advertising practices and to allow consumers to choose whether their data is used for behavioral advertising. The principles also referenced establishing an accountability program for monitoring compliance with the guidelines and reporting non-compliance to appropriate government agencies.

In November 2011, the Digital Advertising Alliance ("DAA"), which represents over 400 advertising and technology companies, unveiled self-regulatory principles for multi-site data. The goal was to expand the scope of industry self-regulation with respect to online data collection to encompass "all data collected from a particular computer or device" and not just data specifically collected for online behavioral advertising. The November 2011 principles stipulated that any third party or service provider that collects multi-site data for purposes other than online behavioral advertising should provide consumers with "transparency and consumer control" unless the data is de-identified, or if the collection is necessary for operations and systems management purposes, market research or product development.

Several months after issuing its self-regulatory principles, the DAA announced that its members would work "to add browser-based header signals to the set of tools by which consumers can express their preferences" regarding how they are tracked online. The DAA also stated its intention to work with browser providers to develop "consistent language across browsers . . . that describes to consumers the effect of exercising such choice." When it was released in February 2012, the DAA's announcement indicated that the browser-based consumer choice mechanism would be implemented within nine months.

Certain companies have made their own attempts to stave off government regulation of online tracking by developing and implementing more privacy-protective features that would limit default tracking by their online products. For example, Adobe Systems Incorporated announced in January 2011 more that it was working to integrate control features into browser user interfaces to allow users to easily control local shared objects ("LSOs") on their computers. LSOs, often referred to as Flash cookies, store information about online activity, including browsing history, login details and user preferences. Flash cookies have been the subject of numerous lawsuits against online advertising networks alleged to have used Flash cookies to re-create deleted browser cookies. In the FTC's March 2012 report on online privacy, the Commission addressed the use of Flash cookies and emphasized the importance of improving consumers' ability to control online tracking mechanisms. The report noted that although consumers "may believe they have opted out of tracking if they block third-party cookies on their browsers . . . they may still be tracked through Flash cookies or other mechanisms."

For its part, Microsoft announced in May 2012 that it intended to set DNT as the default option in the latest version of its browser. Microsoft's announcement of what it referred to as the "privacy by default" DNT setting in Internet Explorer 10 irked online advertisers. Tracking-related browser settings are included in most web browsers, but generally browsers are set to allow tracking unless a user turns on the DNT feature, which sends a signal to third-party websites that the user does not want his or her activity tracked. The efficacy of DNT mechanisms is contingent on advertisers' complying with the DNT requests that browsers transmit. Accordingly, although the advertising industry has indicated that it will begin honoring DNT requests by the end of 2012, if a company implements a certain type of DNT setting despite advertiser opposition, advertisers may choose to ignore DNT requests sent by the browser and defeat the purpose of the mechanism.

FTC Activity

The FTC's March 2012 Report

Building on its earlier efforts discussed above, in December 2010, the FTC issued a preliminary staff report addressing a host of consumer privacy issues associated with emerging technologies. After receiving and analyzing hundreds of comments from stakeholders, on March 26, 2012, the Commission released its landmark report entitled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The report, which adopted much of the 2010 staff report's framework, clarified and revised certain points and included an extensive discussion of DNT mechanisms to protect the privacy of consumers' online browsing data.

In introductory remarks, FTC Chairman Jon Leibowitz asserted his strong support for DNT and predicted that if effective DNT mechanisms are not available by the end of 2012, the new Congress likely would introduce a legislative solution. The FTC report identified its work on a DNT mechanism with browser makers, the DAA and the World Wide Web Consortium as one of the five main ways in which the FTC intends to promote the implementation of its proposed framework through policymaking in 2012. To that end, the FTC indicated it would host a workshop later in the year to consider issues surrounding large platform providers that track consumers' online activities (e.g., ISPs, operating systems, browsers and social media). A senior FTC staffer argued that these providers' ubiquitous information collection practices create privacy concerns that cannot effectively be managed by consumer choice alone.

Revisions to COPPA

The FTC also has been considering revising the Children's Online Privacy Protection Act ("COPPA") to address the behavioral tracking of children. In 2011, the FTC released proposed amendments to the COPPA Rule to address rapid changes in technology and the ways in which children access the Internet and use various mobile technologies. Particularly noteworthy is the FTC's proposal to expand the definition of "personal information" to include IP addresses, customer numbers held in cookies and geolocation information. A year later, the FTC revised its initial proposal to include screen or user names as personal information, and clarified that an IP address or customer number held in a cookie will be deemed personal information if it can be used to recognize a user over time or across different sites or services (unless the IP address or customer number is used for "support for internal operations"). These revisions to the definition of personal information undoubtedly would impact a number of online behavioral tracking and advertising practices. The FTC has requested additional comments on the September 2011 revisions, and has indicated repeatedly that updates to the COPPA Rule should be finalized in 2012.

FTC Enforcement Actions

In the absence of legislation, the FTC has stepped in to bring enforcement actions against a number of companies alleged to have engaged in unfair or deceptive trade practices through their use of online tracking mechanisms. For example, in April 2012, the FTC approved a settlement with Upromise, Inc., a company that offered consumers a web browser toolbar to highlight Upromise partner companies in consumers' search results, then gave cash rebates for college savings accounts to members who made purchases from those partners. In its complaint, the FTC alleged that, to facilitate targeted advertising, the "Personalized Offers" feature on the Upromise toolbar collected far more information about users' browsing behavior than was disclosed at the time of installation, including the names of all websites visited, all links clicked, and information entered on certain websites, such as usernames, passwords and search terms. Among other terms in the settlement agreement, Upromise was required to destroy the data it collected through the Personalized Offers feature, to provide clear and prominent disclosures to consumers and receive their affirmative consent before installing any similar product, and to provide certain information to current users of Personalized Offers (including how to disable and uninstall the feature).

About a month after the Upromise settlement, the FTC announced a settlement agreement with the social networking service Myspace after alleging that Myspace had allowed unaffiliated third-party advertisers to access users' names and information about their online browsing habits contrary to representations the company made in its privacy policy. Specifically with respect to behavioral advertising, the FTC charged that Myspace (1) failed to give users notice or obtain their permission before allowing advertisers to access personally identifiable information via the means through which Myspace customizes ads and (2) shared non-anonymized web-browsing activity with advertisers. The FTC settlement required Myspace to establish and maintain a comprehensive privacy program subject to biennial, independent, third-party audits for 20 years.

In August 2012 the FTC announced that Google Inc. agreed to pay $22.5 million to settle charges that the company's use of certain cookies on Apple Inc.'s Safari browsers violated a 2011 privacy agreement between Google and the FTC. As indicated in the complaint filed against Google by the Department of Justice and the FTC, Google had agreed under the terms of the 2011 Order to not "misrepresent . . . the extent to which [it] maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to. . . the extent to which consumers may exercise control over the collection, use, or disclosure of covered information." "Covered information" was defined to include persistent identifiers in cookies.

The FTC alleged that, although Google informed Safari users that a setting in the Safari browser could be used to block the deployment of certain Google cookies, Google circumvented that setting and deployed cookies to those users' browsers for advertising purposes. The FTC also alleged that Google's failure to provide adequate disclosure regarding its Safari cookie practices conflicted with the company's public representation that

it complies with the NAI Code of Conduct. Pursuant to the settlement, until early 2014, Google will cause the relevant cookies to expire on Safari users' browsers as Google encounters the cookies. Existing opt-out cookies will not be affected.

The Administration's Privacy Policy Framework

On February 23, 2012, the White House released a long-awaited report entitled "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Global Innovation in the Global Digital Economy." The report, which built on recommendations issued in December 2010 by the Department of Commerce, articulated a Consumer Privacy Bill of Rights. The Bill of Rights would allow consumers to exercise more control over how their personal data is collected and used by companies, emphasizing transparent privacy and data security practices and other fair information practices such as the ability to access and correct personal data maintained by companies and to set reasonable limits on the personal data that companies collect and retain. The report addressed online behavioral advertising, stating that a DNT mechanism would provide consumers with some control over how third parties receive and use consumer data, and discussed self-regulatory efforts to alert consumers to the presence of third party ads and direct them to sites that provide additional information about the ad networks' collection of data. Although the report indicated that these mechanisms "show promise," it acknowledged that they would require further development. The Administration expressed its intention to work with Congress to draft legislation based on the Consumer Privacy Bill of Rights and emphasized the critical role of the FTC in privacy enforcement, encouraging Congress to provide the FTC and state attorneys general with specific authority to enforce the Consumer Privacy Bill of Rights.

Congressional Efforts

The past few years have witnessed a number of legislative efforts aimed at controlling or restricting certain kinds of online tracking. Some of these efforts took the form of stand-alone proposals and others were included in the context of more comprehensive bills addressing privacy issues. Congressional focus on behavioral tracking intensified in December 2010, when a U.S. House of Representatives subcommittee held hearings to discuss the possibility of passing and implementing DNT legislation. The hearings focused on a variety of consumer privacy issues, including the implications and challenges of a DNT mechanism and the need to preserve an advertising-supported Internet that promotes economic growth through online business.

In his testimony, David Vladeck, Director of the FTC's Division of Consumer Protection, discussed the viability of a mechanism to provide consumers better control over online tracking. Although he left open the possibility of an industry-administered program, he indicated that the pace of industry self-regulation had been too slow and industry efforts insufficient. Other testimony during the hearings indicated the Department of Commerce's support for the kind of "consumer empowerment" that a DNT mechanism would allow, but concerns were raised about the challenges of implementing and enforcing DNT even if formal legislation were to be passed.

In 2011, Congressmen Edward Markey (D-MA) and Joe Barton (R-TX) reiterated their privacy concerns over the handling of customer preferences in connection with an advertising initiative by Verizon. After learning that Verizon had notified its customers of the implications of a targeted advertising campaign, Representatives Markey and Barton, co-chairs of the bipartisan Congressional Privacy Caucus, issued an inquiry letter to both Verizon and Verizon Wireless. In particular, the Congressmen requested clarification regarding the companies' potential disclosure of website viewing history to third parties.

In Verizon's response letter, the company stressed that its new programs "do not disclose any personal information about [Verizon or Verizon Wireless] customers." Representative Markey indicated on his website, however, that he was "still concerned that Verizon has required customers to opt-out of this new program rather than opt-in. An opt-in mechanism would allow consumers, not the company, to decide whether to grant permission to use consumer information for targeted advertising purposes, especially in a program focused on geolocation from customer postal addresses."

In late 2011, Senator Jay Rockefeller (D-WV), Chair of the Senate Committee on Commerce, Science and Transportation, issued a statement emphasizing the need for increased consumer protection on the Internet. Rockefeller cited "disturbing" reports indicating that Facebook has the ability to track the browsing patterns of both non-members and members, including after members have logged out of the site. Earlier in 2011, following Senate hearings on consumer privacy issues, Senator Rockefeller introduced the "Do-Not-Track Online Act of 2011", which would have instructed the FTC to develop standards for the implementation of a DNT mechanism. Representative Jackie Speier (D-CA) introduced companion legislation in the House with the "Do Not Track Me Online Act of 2011." Speier's legislation would have directed the FTC to promulgate regulations that establish standards for a "Do Not Track" mechanism. The bill

also would have required covered entities to disclose their information practices to consumers, and to respect consumers' choices regarding the collection and use of their information. Both bills died in Committee.

EU Regulation of Online Behavioral Advertising

In 2009, the European Union's e-Privacy Directive was amended to include more stringent restrictions on the use of cookies, a necessary component of most behavioral advertising. The most significant change was from the previous default requirement to provide clear notice and an opt-out mechanism, to the new requirement to provide notice and obtain consent for the placement of cookies and similar technologies that store and access information on a user's device. Recital 66 of the amendment indicated that consent may be obtained through browser settings, but the browser settings available in current technology likely are inadequate for this purpose.

The amendment included certain exceptions to the rules – for example, placing a cookie may not require informed consent if the cookie is necessary to carry out "the transmission of an electronic communications network" or if "it is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user to provide that service" – but finding practical ways to comply with the new cookie requirements has proven challenging for the behavioral advertising industry. Because the Directive is implemented by national law in each EU Member State, specific requirements and enforcement actions may vary by country. Although the Member States were obligated to transpose the new requirements into their respective national laws by May 25, 2011, as of August 2012, not all of the Member States had implemented the amendment.

The European Union's Article 29 Working Party (the "Working Party"), which has adopted several Opinions relevant to this issue, has indicated that the types of cookies that may not require informed consent include secure login session cookies, shopping basket cookies and security cookies. The Working Party also has provided certain practical examples (that are more user-friendly than pop-up screens) of how to legally obtain consent where required, and has published best practice recommendations for the online behavioral advertising industry to comply with the cookie requirements.

On June 7, 2012, the Working Party adopted an Opinion analyzing the exemptions to the prior opt-in consent requirement for cookies and providing some general guidelines regarding the application of the exemptions. Although the Opinion focused on cookies, the Working Party noted that the same analysis would apply to any technology that allows information to be stored or accessed on a user's computer or mobile device. According to the Opinion, cookies used for third-party advertising purposes are not covered by the exemptions, and thus require prior opt-in consent.

Looking Ahead

As entities such as the World Wide Web Consortium's Tracking Protection Working Group continue their efforts to develop DNT mechanisms that are acceptable to both businesses and regulators, the specter of legislation looms large. At present, the stakeholders working on a non-legislative solution still disagree on what DNT should include, and key aspects of how a DNT mechanism should function remain the subject of intense debate. Given that privacy protective proposals often benefit from bipartisan support, a law mandating the implementation of DNT features may be one of the few types of legislation capable of bypassing Congressional gridlock. In the meantime, companies should remain vigilant to avoid regulatory scrutiny given the FTC's clear intention to pursue entities engaging in online tracking practices that do not conform to their public representations and consumer expectations.

1. *See, e.g.,* Kristen Purcell et al, Pew Internet & American Life Project, *Search Engine Use 2012,* Mar. 9, 2012, available at *http://www.pewinternet.org/Reports/2012/Search-Engine-Use-2012.aspx* (last visited Aug. 30, 2012).