

Developments in Online Behavioral Advertising

Melissa J. Krasnow, Dorsey & Whitney LLP

There were developments in online behavioral advertising—the practice of tracking an individual's online activities to deliver advertising tailored to the individual's interests—over the past year. This is an area to watch as developments are likely to continue.

Companies engaged in online behavioral advertising should review their privacy policies, terms of use, and agreements and similar documents against their actual and contemplated online behavioral advertising practices, particularly in light of the Federal Trade Commission's focus on this area.

In 2009, the FTC brought the enforcement action *In the Matter of Sears Holdings Management Corp.*, FTC File No. 082 3099.¹ Sears Holdings Management Corporation ("Sears Holdings") disseminated via the Internet a software application for consumers to install onto their computers (the "Application") to participate in an online community. The "Privacy Statement and User License Agreement" (the "Agreement") on the consumer registration page described the Application's specific functions beginning at the 75th line, including how consumers could stop participating and remove the Application from their computers. The Agreement also included a reservation of right to continue to use information collected before a consumer's "resignation." Consumers needed to indicate through a blank checkbox next to a statement that they had read and agreed to the terms and conditions of the Agreement before installation. The Application functioned and transmitted information substantially as described in the Agreement when installed.

The FTC alleged that the following facts would be material to consumers in deciding to install the Application and the failure to disclose these facts, in light of the representations made, was a deceptive practice in violation of Section 5 of the Federal Trade Commission Act.² The Application when installed would (i) monitor nearly all of the Internet behavior occurring on consumers' computers, including (A) information exchanged between consumers and websites other than those owned, operated, or affiliated with Sears Holdings, (B) information provided in secure sessions when interacting with third-party websites, shopping carts, and online accounts, and (C) headers of web-based email; (ii) track certain non-Internet related activities on those computers; and (iii) transmit nearly all monitored information to the remote computer servers of Sears Holdings.

The FTC issued and approved a consent order in late 2009.³ This order is in effect for approximately 20 years. First, Sears Holdings must cease collecting any data transmitted, and destroy any information or data transmitted from a computer, by an Application installed before the order to any Sears Holdings computer server.

Second, Sears Holdings must notify affected consumers who downloaded and installed the Application on a computer in connection with the on-line community (i) that they have installed the Application on their computers (which collects and transmits to Sears Holdings and others the data described in the Agreement) and (ii) of how to uninstall the Application. Sears Holdings must provide prompt, toll-free, telephonic and electronic mail support to help affected consumers uninstall any Application. Notification must be made for two years by posting of a clear and prominent notice on the on-line community website. The order defines "clearly and prominent" with respect to text, video, audio and interactive media. For three years, Sears Holdings must notify affected consumers who complain or inquire about any Application.

Third, in connection with the advertising, promotion, offering for sale, sale, or dissemination of any Application before the consumer downloading or installing it, Sears Holdings must disclose clearly and prominently, and before the display of, and on a separate screen from, any final "end user license agreement," "privacy policy," "terms of use" page, or similar document: (i) all types of data that the Application will monitor, record, or transmit (including, without limitation, whether (A) the data may include information from the consumer's interactions with a specific set of websites or from a broader range of Internet interaction, (B) the data may include transactions or information exchanged between the consumer and third parties in secure sessions, interactions with shopping baskets, application forms, or online accounts, and (C) the information may include personal financial or health information); (ii) how the data may be used; and (iii) whether the data may be used by a third party.

Fourth, Sears Holdings must obtain express consent from the consumer to the download or installation of the Application and the collection of data by having the consumer indicate assent to those processes by clicking on a button or link that is (i) not pre-selected as the default option and (ii) clearly labeled or otherwise clearly represented to convey that it will initiate those processes or by taking a substantially similar action.

Finally, Sears Holdings must (i) file with the FTC written reports regarding the manner and form of its compliance with the order and (ii) maintain and upon request make available to the FTC copies of all documents relating to compliance with the order for four years.

According to FTC Chairman Jon Leibowitz at the FTC Privacy Roundtable in December 2009, "[t]he thrust of our case was that, while the extent of tracking was described in the [Agreement], that disclosure wasn't sufficiently clear or prominent given the extent of the information tracked, which included online bank statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject, and size for web-based e-mails. So consumers didn't consent with an adequate understanding of the deal they were making."⁴

This enforcement action followed the FTC's issuance of its Staff Report on Self-Regulatory Principles for Online Behavioral Advertising in February 2009, which describes the following four Principles: (i) transparency and consumer control, (ii) affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising, (iii) reasonable security and limited data retention for consumer data, and (iv) affirmative express consent for material changes to existing privacy promises.⁵ The first and second Principles below are relevant to the enforcement action. First, every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (A) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (B) consumers can choose whether or not to have their information collected for this purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option. Second, companies should collect sensitive data for behavioral advertising only after they obtain affirmative express consent from the consumer to receive this advertising. Third, companies that collect and/or store consumer data for behavioral advertising should provide reasonable security for that data, based on the sensitivity of the data, the nature of business operations, the types of risks companies face, and the reasonable protections available. Also, companies should retain data only as long as necessary for legitimate business or law enforcement needs. Fourth, companies must keep any promises that they make regarding how they will handle or protect consumer data, even if they decide to change their policies at a later date. Accordingly, before companies can use previously collected data in a manner materially different from promises they made when they collected the data, they should obtain affirmative express consent from affected consumers, including in a corporate merger situation to the extent the merger creates material changes in the way the companies collect, use, and share data.

Finally, in July 2009 the Direct Marketing Association, Interactive Advertising Bureau, Association of National Advertisers, the American Association of Advertising Agencies, and the Council of Better Business Bureaus issued Self-Regulatory Principles for Online Behavioral Advertising, consisting of the following seven Principles—education, transparency, consumer control, data security, material changes, sensitive data, and accountability.⁶

Melissa J. Krasnow is a partner in the Corporate Group of Dorsey & Whitney LLP, whose practice includes privacy and social media. For additional information, please go to http://www.dorsey.com/krasnow_melissa/.

¹ Available at <http://www.ftc.gov/os/caselist/0823099/index.shtm> (last visited Feb. 2, 2010).

² 15 U.S.C. § 45 et seq.

³ *In the Matter of Sears Holdings Management Corp.*, Decision and Order, FTC File No. 082 3099 (Aug. 31, 2009), available at <http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf> (last visited Feb. 2, 2010).

⁴ Introductory Remarks, Chairman Jon Leibowitz, FTC Privacy Roundtable (Dec. 7, 2009), available at <http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf> (last visited Feb. 2, 2010).

⁵ See *Self-Regulatory Principles for Online Behavioral Advertising*, FTC Staff Report (Feb. 2009), available at <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf> (last visited Feb. 2, 2010).

⁶ Available at <http://www.iab.net/media/file/ven-principles-07-01-09.pdf> (last visited Feb. 2, 2010).