# FTC Privacy Enforcement Targets ScanScout's Failure to Toss Its Cookies

## Media Law Bulletin

By Matthew Fischer

December 09, 2011

The Federal Trade Commission (FTC) has served notice that it is not messing around when it comes to zombies and cookies. ScanScout, Inc., a Boston-based online advertising network, recently settled FTC charges that it deceptively claimed that consumers could opt out of receiving targeted ads by changing their computer's web browser settings to block cookies, despite the fact that ScanScout used Flash cookies that are difficult to block through standard browser settings. ScanScout's practices and the FTC's enforcement action offer a cautionary tale for disclosure policies and practices of companies with an online presence.

Companies recognize that customers are concerned about guarding their privacy in relation to their online activities. By now, even the non-geeks roaming the Internet have likely heard about the privacy dangers associated with Flash cookies which, like naked licensing, are not nearly as fun as they sound.

Users have become more knowledgeable about cookies and attentive to purging them from their computers. This practice of "cookie tossing" caused some online advertisers to use more invasive methods to track users. Flash cookies, properly termed "Local Shared Objects," permit websites using Adobe Flash Player to store 100 kilobytes of information on a computer indefinitely by allowing a user's custom settings to continue between visits. While Flash cookies have many benefits (*e.g.*, memorizing user content and custom settings for future logins and user verification), websites can also use them to track people's online activities. Although people frequently clear out their cookies to stop long-term tracking, many are unaware of Flash cookies and the means for deleting them are relatively arcane. A script stores the content of the cookie in the local storage available to Flash content and then recreates the cookie from backup stores when the cookie's absence is detected. This ability to respawn is why Flash cookies are also called "zombie" cookies. However, these zombies can be stopped — and you don't even have to resort to decapitation or cricket bats as portrayed in the cult zombie film "Shaun of the Dead." Since the beginning of 2011, Adobe has offered a programming interface that allows Flash cookies to be more easily deleted from within the settings panel of most browsers.

ScanScout is an advertising network that places video ads on websites for advertisers. Its online privacy policy stated, *"You can opt out of receiving a cookie by changing your browser settings to prevent the receipt of cookies."* However, for a two-year period ScanScout used Flash cookies and the FTC charged that changing browser settings did not remove or block the Flash cookies so that ScanScout could continue to monitor its users' browser histories and serve targeted ads to people who mistakenly believed they had opted out. The FTC complaint alleged that ScanScout's privacy policy was false and misleading and therefore violated the FTC Act. During the agency's investigation, ScanScout merged with Tremor Video, Inc, which is also subject to the settlement order.

Part I of the consent order precludes ScanScout from misrepresenting the extent to which it collects, uses, discloses or shares data about users or their online activities or how users may exercise control over the collection or disclosure or data collected about them.

Part II of the order requires ScanScout to take the following measures to improve the transparency of its data collection activities for online behavioral advertising:

- For a period of at least five years, ScanScout must place a clear and prominent notice with a hyperlink on the homepage of its website that states: "We collect information about your activities on certain websites to send you targeted ads. To opt out of our targeted advertisements, click here." The notice must direct

users to a mechanism that allows them to prevent ScanScout from: (1) collecting personally identifiable information; (2) redirecting its browser to third parties that collect data, absent a user's affirmative consent; and (3) associating any previously collected data with them.

- Near the opt-out mechanism, ScanScout must disclose: (1) that it collects information about users' activities to deliver targeted ads; (2) it will not collect information of those users who opt out; (3) whether or not a user chose to opt out; and (4) that if users switch browsers or devices, or if they delete cookies, they will have to opt out again.

- As part of any behaviorally targeted display advertisement that it serves, ScanScout must embed a hyperlink that takes users directly to the required choice mechanism and lets them know that clicking the hyperlink will give them choices about getting targeted ads. ScanScout will work to develop the technology that will allow it to develop and implement a similar hyperlink for video advertisements.

- ScanScout must make available to the FTC for inspection and copying for a period of five years consumer complaints or inquiries directed or forwarded to ScanScout concerning certain aspects of its information practices, such as its collection of data, its opt-out practices, documents demonstrating compliance with the consent order, past terms of use, end-user license agreements, and privacy policies.

The financial terms of the settlement were not disclosed and the proposed order does not impose a monetary penalty. In conjunction with the consent order, the FTC released a new consumer education article titled "Cookies: Leaving a Trail on the Web," which explains how cookies are used to connect your online activities over time, and how you can control information about your browsing.

Although Flash cookies have been in existence since before 2006, the last couple of years have seen a rash of putative class action lawsuits for the use of Flash cookies in online behavioral advertising. The lawsuits have targeted a number of Internet advertising companies such as ScanScout, but have also included major players in the hospitality, media and entertainment sectors. Several of these private lawsuits were dismissed due to the plaintiffs' inability to articulate an injury that could be quantified in the requisite monetary amounts required by the underlying statutes, such as the $5,000 threshold under the Computer Fraud and Abuse Act. However, a number of defendants paid multimillion-dollar settlements. The FTC had not entered the fray with respect to Flash cookies litigation until it initiated its complaint this year against ScanScout.

The FTC's most notable recent online privacy action preceding ScanScout illustrates the agency's focus on the deceptive nature of companies' representations with respect to their privacy policies and terms of use. In the Spring of 2011, the FTC settled with Google after leveling charges that it violated its terms of service with respect to its unsuccessful social-networking platform "Buzz." Like the charges against ScanScout, the FTC action against Google was not premised on the notion that the search engine's practices were intrinsically invasive. Rather, the FTC charged that the company's terms of service misled consumers into erroneously believing that they could opt out of the Buzz network.

Any company with an Internet presence — which is just about everyone these days — is cognizant of the public concern over data privacy and online tracking. The ScanScout settlement, like the Google settlement, provides some clear guidelines to avoid FTC online privacy enforcement actions.

- Make sure your privacy policy and/or terms of use are clear and accurate.

- Review and understand the specific technologies being used and ensure they are being implemented in a way that corresponds with your company's privacy policy and terms of use.

- Verify the methods and privacy policies and terms of third-party data collectors with which you do business.

- Make sure users have appropriate opt-in/opt-out and disclosure options when it comes to online tracking and/or the collection of personally identifiable information.

The FTC's enforcement actions against ScanScout and Google demonstrate the agency's commitment to prosecuting false claims with respect to any method of online tracking, identification or data collection.

**Related Practices:**

Commercial Practices

Intellectual Property

Media, Entertainment & Sports Law