

Cookies & Advertising Networks

What is a Cookie?

A cookie is (usually) a small amount of information sent by a Web server to a Web browser with the expectation that, when the user visits the server (website) again, the browser will send the information back to the server. Web servers use cookies to store user-specific information on the user's computer. For example, a cookie may be used to store the user's website id on his/her computer so that the user does not have to supply the id every time when visiting the website. In successive visits to the website, the browser will send the cookie with the id to the server, thereby identifying the user.

What is an Advertising Network?

Many websites sell advertising space. Many such websites, instead of delivering ads from their own servers, put URLs in their pages that point to ads on an advertising network's servers. The advertising network decides which ad to show to a user, and it does the bookkeeping for "hit counts." Advertising networks use cookies to keep track of ads they have already shown to a user. They can control the ads they show to a user based on a parameters such as the page the user is downloading, the number of times the user has seen a particular ad, the time of day, etc.

Here is an example illustrating the interaction with an advertising network. Suppose a user visits the website www.a.com and gets back an HTML page that contains a URL for an ad on www.ads.com, an advertising network website. Besides returning an ad, www.ads.com will send a cookie to the user's browser, which the browser will return to the advertising network with every visit to www.ads.com.

The advertising network's awareness of the ads shown to a user spans all the websites affiliated with the advertising network. This is possible because the "ad" cookies come from the advertising network, not from the individual websites visited by the user,

Privacy Issues

The same caveats apply to the cookies from an advertising network as those that apply to other cookies. That is, if a user does not disclose personal information at any of the websites using the advertising network, the advertising network will not know who the user is, although it can assemble a portrait of the user. The portrait could comprise information about the websites visited and the pages seen by the user.

Third-Party Cookies

The Internet Engineering Task Force (IETF) standardization effort for cookies led to specification RFC 2965, titled *HTTP State Management*. RFC 2965 pays special attention to third-party cookies, the kind that advertising networks use, for example, and calls the transactions that give rise to them “unverifiable transactions.” The cookie is “third-party” because it came from a site other than the one originally contacted by the user.

The reason the transactions are called “unverifiable” relates to the way the user experiences them. When a user clicks on a link for the website www.a.com, the user will not be surprised to get a cookie from www.a.com. But many users will be surprised if, while waiting for content to arrive from www.a.com, they get cookies from a different website, say www.ads.com. Since most browsers tell the user what site will be contacted if the user clicks on a link that the user’s mouse is placed over, the user can verify which site will be contacted. But because automatic image loading is usually enabled, and because a user cannot preview the site that the browser will contact to download an ad before it actually does so, the ad-loading transaction is unverifiable.

RFC 2965 calls for special handling of cookies that arrive during an unverifiable transaction if they come from a server different from the one originally contacted. In the above example, cookies that arrive along with images from www.a.com would be okay, even though the user could not verify the image-load. The RFC says browsers must, by default, disable cookies in unverifiable transactions, although browsers may provide an option to enable them.

As written, RFC 2965 would impede the way some advertising networks now work. The RFC did not set out with that aim, but it evolved while advertising networks were just forming. More recently, advertisers have explored coupling Platform for Privacy Preferences (P3P) information to the uses of third-party cookies, so the privacy intentions of the cookie sender can be described automatically.

Where Can I Find More Information?

- o [Cookie Specification](ftp://ftp.isi.edu/in-notes/rfc2965.txt) (ftp://ftp.isi.edu/in-notes/rfc2965.txt)
- o [Platform for Privacy Preferences Information](http://www.w3.org/P3P/) (http://www.w3.org/P3P/)

Author: [David M. Kristol](mailto:info@silicon-press.com), info@silicon-press.com