

Google's Safari Tracking Dilemma: Reality Check

Google appears to be busted abusing user privacy by tracking users across the web without their permission, but Google denies the charge.

By Ian Paul Feb 17, 2012 8:41 AM



Google reportedly breached the privacy of millions of Apple Safari users by fooling the web browser into accepting tracking cookies it normally wouldn't take. Google, however, says this is an unhappy accident and that Google never intended to track its users in this manner.

It's a classic case of he said, she said. Here's what's going on.



Apple's Safari is more aggressive by default than many browsers about blocking cookies that do not originate from the site you're visiting, such as cookies served by online advertising firms. These are referred to as third-party cookies and are used by most online advertising companies and common on major websites. Google got around Safari's privacy restrictions by exploiting a loophole that allowed the search giant to install a temporary cookie if a user clicked a +1 button embedded in online advertising, according to a report in The

Wall Street Journal.

The matter primarily affects users of iOS and OS X devices where Safari is the default browser, but it potentially affects any system running Safari, which is also available for Windows.

How Google Did it

The trick, according *Journal* reports, involves sticking a hidden web form inside an online ad with a +1 button, similar to Facebook "likes," on it. If the user clicks on the +1 button, the web form tells Safari that the user filled out the phony form when in fact she or he had not, which allowed Google to install the cookie.



When a user appears to have explicitly interacted with content on a Website, Safari allows the site to install temporary cookies that are supposed to expire after 12 to 24 hours. As a result of this workaround, Google could then catalog a user's browsing habits for its DoubleClick advertising business, according to research by Johnathan Mayer, a graduate student at Stanford University who first discovered Google's tracking behavior.

For its part, Google says it wasn't tracking people on purpose and only wanted to ascertain when a user was logged into a Google account. "We used known Safari functionality to provide features that signed-in Google users had enabled," says Rachel Whetstone, Google's senior vice president of communications and public policy, in a statement to *PCWorld*. If you were logged in, Google could then deliver personalized advertising and perform other functions, such as sending +1's back to a user's Google+ social networking profile.

"However, the Safari browser contained functionality that then enabled other Google advertising cookies to be set on the browser," Whetstone says. "We didn't anticipate that this would happen, and we have now started removing these advertising cookies from Safari browsers." Google also emphasizes that its advertising cookies do not collect any personal information.

This is Google's cache of <http://www.google.com/ads/preferences/plugin/browsers.html>. It is a snapshot of the page as it appeared on 14 Feb 2012 05:39:36 GMT. The [cache](#)



Advertising Cookie Opt-out Plugin

[Home](#)

[FAQs](#)

Browser Instructions

Opting out permanently: Browser Instructions

See instructions for: [Internet Explorer, Firefox & Google Chrome](#) | [Safari](#) | [Other browsers](#)

Internet Explorer, Mozilla Firefox & Google Chrome

You can download the plugin for Internet Explorer, for Firefox and for Google Chrome from the homepage of the [Google advertising opt-out plugin](#).

Instructions for Safari

While we don't yet have a Safari version of the Google advertising cookie opt-out plugin, Safari is set by default to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as setting the opt-out cookie. To confirm that Safari is set up to block third-party cookies, do the following:

1. From Safari, select "Safari" in the menu bar, and then select "Preferences"
2. In the Preferences Dialog Box, select the "Security" tab
3. Make sure the "Accept cookies:" setting is set to "Only from sites you navigate to". You can also set this option to "Never", but this will prevent many web sites that rely on cookies from working.

Instructions for other browsers

Unfortunately, the plugin is not available for other browsers. You can always opt out using the [Ads Preferences Manager](#), but without a special browser plugin, your opt-out setting will go away when you delete your browser's cookies (you would need to set it again manually).

If you're using another browser that's not mentioned above, you can look for a common feature, which accomplishes the same as setting the DoubleClick opt-out cookie: Find a setting in your browser's settings that allows you to only accept cookies from sites you visit, or only "first-party cookies". This option may also be described as "blocking third-party cookies."

©2010 Google - [Home](#) - [New Privacy Policy](#)

Google's privacy policy page was edited regarding Safari. (click to enlarge)

Google has also deleted language from one of its privacy policy pages that appeared to contradict its tracking practices as detailed by the *Journal*. Google allows you to install a browser cookie that tells the search giant not to store your browsing habits for online advertising purposes. But the company does not have a working version of this opt-out program for Safari users.

The text on the page used to read: "While we don't have a Safari version of the Google advertising cookie opt-out plugin, Safari is set to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as setting the opt-out cookie." Google has since removed that language from its site, but **PCWorld** was able to find the language in a cached version of the page dated February 14.

Common Practice by Default

Installing third-party tracking cookies on your browser is common practice for online advertising companies. Your browsing information is then mined so the sites serve up targeted advertising that, in theory, you are more likely to click on. Given that Safari is one of the most popular mobile browsers owing to the success of iOS devices such as the iPhone and iPad, Google and other firms were handicapped by Apple's policies of disallowing third-party cookies by default. So Google, along with advertising firms such as Vibrant Media, Media Innovation Group, and PointRoll, used this workaround -- Google called it "known functionality."

It's not clear when this Safari loophole that enables advertising to circumvent a browser's privacy settings will be closed. Apple is reportedly working to stop this kind of activity, and the loophole has already been closed in WebKit, the open source version of Apple's Safari. The patch was created in August, and the *Journal* says in a blog post that the fix was made, ironically enough, by two Google engineers.

Connect with Ian Paul (@ianpaul) on Twitter and Google+, and with Today@PCWorld on Twitter for the latest tech news and analysis.