THE WALL STREET JOURNAL.
WSJ.com

TECHNOLOGY | FEBRUARY 17, 2012

Google's iPhone Tracking

Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy

By JULIA ANGWIN And JENNIFER VALENTINO-DEVRIES

Google Inc. and other advertising companies have been bypassing the privacy settings of millions of people using Apple Inc.'s Web browser on their iPhones and computers—tracking the Web-browsing habits of people who intended for that kind of monitoring to be blocked.

The companies used special computer code that tricks Apple's Safari Web-browsing software into letting them monitor many users. Safari, the most widely used browser on mobile devices, is designed to block such tracking by default.

Google disabled its code after being contacted by The Wall Street Journal.

Tracking Leaves a Trail

The Google code was spotted by Stanford researcher Jonathan Mayer and independently confirmed by a technical adviser to the Journal, Ashkan Soltani, who found that ads on 22 of the top 100 websites installed the Google tracking code on a test computer, and ads on 23 sites installed it on an iPhone browser.

The technique reaches far beyond those websites, however, because once the coding was activated, it could enable Google tracking across the vast majority of websites. Three other online-ad companies were found using similar techniques: Vibrant Media Inc., WPP PLC's Media Innovation Group LLC and Gannett Co.'s PointRoll Inc.

In Google's case, the findings appeared to contradict some of Google's own instructions to Safari users on how to avoid tracking. Until recently, one Google site told Safari users they could rely on Safari's privacy settings to prevent tracking by Google. Google removed that language from the site Tuesday night.

In a statement, Google said: "The Journal mischaracterizes what happened and why. We used known Safari functionality to provide features that signed-in Google users had enabled. It's important to stress that these advertising cookies do not collect personal information."

Google's privacy practices are under intense scrutiny. Last year, as part of a far-reaching legal settlement with the U.S. Federal Trade Commission the company pledged not to "misrepresent" its

Tracking Apple Users

The Wall Street Journal tested the 100 most-visited U.S. websites, as ranked by Quantcast on Feb. 11, for the tracking technology -- known as cookies -- placed by Google's display ad network. Tests were conducted on Apple's Safari Web browser on a Macintosh computer, as well as on software that simulated the iPhone's browser. There is no indication that any of the sites knew of the code.

Rank	Domain	Safari	iPhone Browser
3	youtube.com	✓	✓
20	ehow.com		✓
23	aol.com		✓
26	about.com	✓	
31	reference.com	✓	✓
32	whitepages.com		✓
33	comcast.net	✓	✓
36	manta.com	✓	✓
42	wikia.com	✓	✓
44	yellowpages.com	✓	
47	chacha.com	✓	✓
48	photobucket.com		✓
54	nytimes.com	✓	
56	hubpages.com	✓	✓
61	deviantart.com		✓
63	tmz.com	✓	
64	squidoo.com	✓	✓
67	people.com	✓	✓
68	webmd.com	✓	
74	metrolyrics.com	✓	✓
83	bleacherreport.com		✓
88	merriam-webster.com	✓	✓
90	wunderground.com	✓	✓
91	match.com		✓
95	inbox.com	✓	
97	drugs.com	✓	✓
98	urbandictionary.com	✓	✓
99	fandango.com	✓	✓
100	howstuffworks.com	✓	✓

Source: Ashkan Soltani, WSJ research

See comments from the companies

---

privacy practices to consumers. The fine for violating the agreement is $16,000 per violation, per day. The FTC declined to comment on the findings.

An Apple official said: "We are working to put a stop" to the circumvention of Safari privacy settings.

Of the ad companies found to be using the technique, Google has by far the largest reach. It delivers Internet ads that were viewed at least once by 93% of U.S. Web users in December, according to comScore Media Metrix.

A Vibrant Media spokesman called its use of the technique a "workaround" to "make Safari work like all the other browsers." Other major Web browsers don't block tracking by default. Vibrant, a top 25 ad network in the U.S. according to comScore Media Metrix, uses the technique "for unique user identification," the spokesman said, but doesn't collect personally identifiable information such as name or financial-account numbers.

WPP declined to comment. A spokeswoman for Gannett described its use of the code as part of a "limited test" to see how many Safari users visited advertisers' sites after seeing an ad.

PointRoll's coding was found in some ads on WSJ.com. "We were unaware this was happening on WSJ.com and are looking into it further," a Journal spokeswoman said.

To test the prevalence of Google's code, the Journal's technology adviser, Mr. Soltani, surveyed the top 100 most popular websites as ranked by Quantcast earlier this month. He found Google placed the code within ads displayed on major sites including movie site Fandango.com, dating site Match.com, AOL.com, TMZ.com and UrbanDictionary.com, among others. These companies either declined to comment or didn't respond. There is no indication that they or any other sites knew of the code.

"We were not aware of this behavior," said Michael Balmoris, AT&T Inc. spokesman. Google's code was found on AT&T's YellowPages.com. "We would never condone it," he said.

Google has already been facing broader questions about privacy. Last month, Google—which offers many services including YouTube, Gmail and of course, Google search—said it would revise its privacy policy to combine nearly all the information it possesses about its users.

The move prompted an international outcry. European Union privacy officials asked Google to "pause" its changes until it can ensure the privacy of EU citizens. Google said it briefed European officials in the weeks before its announcement and plans to roll out the new privacy policy March 1.

Across the digital landscape, the issue of online privacy is taking center stage. In recent months, large institutions and tiny app-makers alike have been accused of mishandling personal data. Trying to reassure a worried public, lawmakers have introduced more than a dozen privacy bills in Congress. The Obama administration has called for a Privacy Bill of Rights to encourage companies to adopt better privacy practices.

Trade in personal data has emerged as a driver of the digital economy. Many tech companies offer products for free and get income from online ads that are customized using data about customers. These companies compete for ads, in part, based on the quality of the information they possess about users.

Google's tracking of Safari users traces its roots to Google's competition with social-network giant Facebook Inc. After Facebook launched its "Like" button—which gives people an easy way to indicate they like various things online—Google followed with a "+1" button offering similar functionality on its rival social network, known as Google+.

Last year, Google added a feature to put the +1 button in ads placed across the Web using Google's DoubleClick ad technology. The idea: If people like the ad, they could click "+1" and post their approval to their Google social-networking profile.

Google's Technique: How It Worked
The Internet giant circumvented privacy settings on Apple's Safari browser.

But Google faced a problem: Safari blocks most tracking by default. So Google couldn't use the most common technique—installation of a small file known as a "cookie"—to check if Safari users were logged in to Google.

To get around Safari's default blocking, Google exploited a loophole in the browser's privacy settings. While Safari does block most tracking, it makes an exception for websites with which a person interacts in some way—for instance, by filling out a form. So Google added coding to some of its ads that made Safari think that a person was submitting an invisible form to Google. Safari would then let Google install a cookie on the phone or computer.
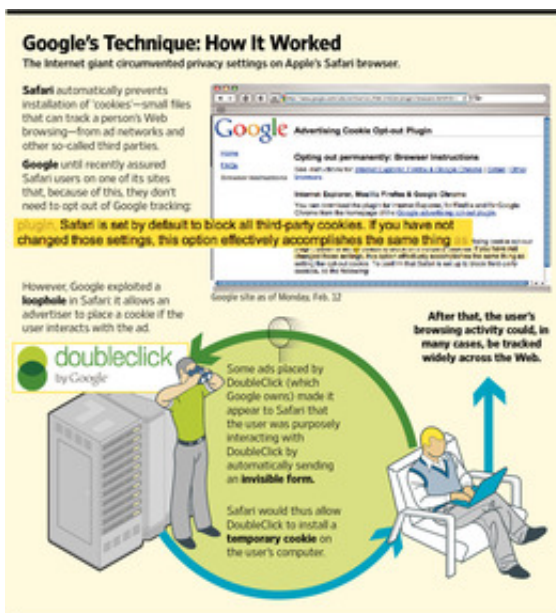
The cookie that Google installed on the computer was temporary; it expired in 12 to 24 hours. But it could sometimes result in extensive tracking of Safari users. This is because of a technical quirk in Safari that allows companies to easily add more

cookies to a user's computer once the company has installed at least one cookie.

Google said it tried to design the +1 advertising system to protect people's privacy and that the placement of further tracking cookies on Safari browsers wasn't anticipated.

Among some Web programmers, the type of maneuver used by Google appears to have been an open secret for some time. Anant Garg, a 25-year-old Web developer in Mumbai, India, blogged about the technique two years ago.

Mr. Garg said when he developed the Safari workaround he didn't consider the privacy angle. He came up with the idea simply to "ensure a consistent experience" for a group of people accessing a chat system from different Web browsers, he said.

The coding also has a role in some Facebook games and "apps"—particularly if the app wants to store a user's login information or game scores. In fact, a corporate Facebook page for app developers called "Best Practices" includes a link to Mr. Garg's blog post.

"We work to educate our developers on how to deliver a consistent user experience across all browsers," said Facebook spokesman David Swain.

Mr. Mayer, who spotted Google using the code, also noticed variations of Mr. Garg's code at work in ads placed by Vibrant Media and WPP's Media Innovation Group. Mr. Soltani verified those findings, and also found code being used by Gannett's PointRoll. In a test, Mr. Soltani found the PointRoll code present in ads on 10 of the top 100 U.S. sites.

Write to Julia Angwin at julia.angwin@wsj.com and Jennifer Valentino-DeVries at Jennifer.Valentino-DeVries@wsj.com