



The Honorable Jon Leibowitz
Chairman
US Federal Trade Commission
600 Pennsylvania Ave
Washington DC 20580

February 17, 2012

Re: Request for declaration regarding unfair and deceptive browser circumvention methods and investigation into Google, Vibrant Media, Media Innovation Group, and Pointroll for compliance with Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1).

Dear Chairman Leibowitz and Commissioners:

The World Privacy Forum¹ writes respectfully to you today to request that the Federal Trade Commission (FTC) investigate Google,² Vibrant Media,³ Media Innovation Group,⁴ and Pointroll⁵ for potential violations of Section 5 of the FTC Act.⁶ These companies willfully override users' privacy preferences as expressly stated by the users in their browser settings. Overriding privacy preferences and doing so without notice are both unfair and deceptive business practices. We request the Commission take action. We also request that the Commission declare circumvention of users' chosen browser privacy settings without notice as a deceptive and unfair practice.

Further, Google, Vibrant Media, and Media Innovation Group are active members of the FTC-approved self-regulatory program, the Network Advertising Initiative.⁷ Pointroll does not appear to be a member of the NAI, but nevertheless links to the NAI policies and appears to offer an NAI opt out.⁸ These companies in overriding users' expressly stated privacy preferences have likely also violated the NAI agreement,⁹ and we request

¹ The World Privacy Forum is a non-profit public interest research and consumer education group based in San Diego, California. We focus on a range of privacy issues, including online privacy.

<http://www.worldprivacyforum.org>.

² <http://www.google.com/>

³ <http://www.vibrantmedia.com/>

⁴ <http://www.themig.com/en-us/>

⁵ <http://www.pointroll.com/>

⁶ Section 5 of the FTC Act states: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful." 15 U.S. C. § 45(a)(1).

⁷ <http://networkadvertising.org/>

⁸ <http://www.pointroll.com/privacy.php>

⁹ See 2008 NAI Principles: *b) Each member directly engaging in OBA and/or multi-site advertising shall*

the Commission investigate these companies for this violation. Finally, we request that the Commission investigate Google for failure to comply with the Commission's consent agreement regarding Google Buzz.

On February 17, 2012, Jonathan Mayer of Stanford released a study documenting that several companies were overriding Safari users' browser privacy settings.¹⁰ Specifically, the companies overrode the setting that specified no cookies would be accepted from third parties. By doing so, these companies broke good faith and trust with consumers. The companies did not disclose their plans or actions to consumers in their privacy policies. Consumers who were Safari users had no reasonable way of knowing this was occurring, and no reasonable way to avoid the harm if they used this browser. The number of consumers affected is significant: Safari browser appears on iPads, iPhones, iPods, and Apple computers. The Wall Street Journal reported on Mayer's findings independently.¹¹

We note that Google, Vibrant Media, and Media Innovation Group are active members of the NAI.¹² These companies have likely broken the NAI self-regulatory agreement in circumventing user choice. The World Privacy Forum believes all of the companies involved merit equal investigation. However, we believe that the impact of Google's action in overriding consumer choice, with its large DoubleClick ad network, will be more substantial.

In Google's case, Google noted on its web site that "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." Google then advised consumers step by step how to make sure this setting was correct so that Safari users could opt out of Google's DoubleClick cookies. (See Figure 1, below.)

require that a website with which it contracts for OBA and/ or multi-site advertising services shall clearly and conspicuously post notice—or ensure, that such notice be made available on the website where data are collected for OBA and/or multi-site advertising purposes—that contains:

- i. A statement of the fact that OBA and/or multi-site advertising is occurring;*
- ii. A description of types of data that are collected for OBA and/or multi-site advertising purposes;*
- iii. An explanation of how, and for what purpose, that data will be used or transferred to third parties; and*
- iv. A conspicuous link to the OBA choice mechanism (e.g., opt out link) provided by the NAI member, and/or a conspicuous link to the opt-out page on the NAI's consumer website. Full principles available at: <http://www.networkadvertising.org/principles.pdf>.*

¹⁰ Jonathan Mayer, *Safari Web Trackers*, <http://webpolicy.org/2012/02/17/safari-trackers/>

¹¹ Julia Angwin, Jennifer Valentino-Devries, *Google's iPhone Tracking: Web giant, others bypassed Apple browser settings for guarding privacy*. Wall Street Journal, Feb. 17, 2012. http://online.wsj.com/article_email/SB10001424052970204880404577225380456599176-1MyQjAxMTAyMDEwNjExNDYyWj.html

¹² <http://networkadvertising.org/participating/>

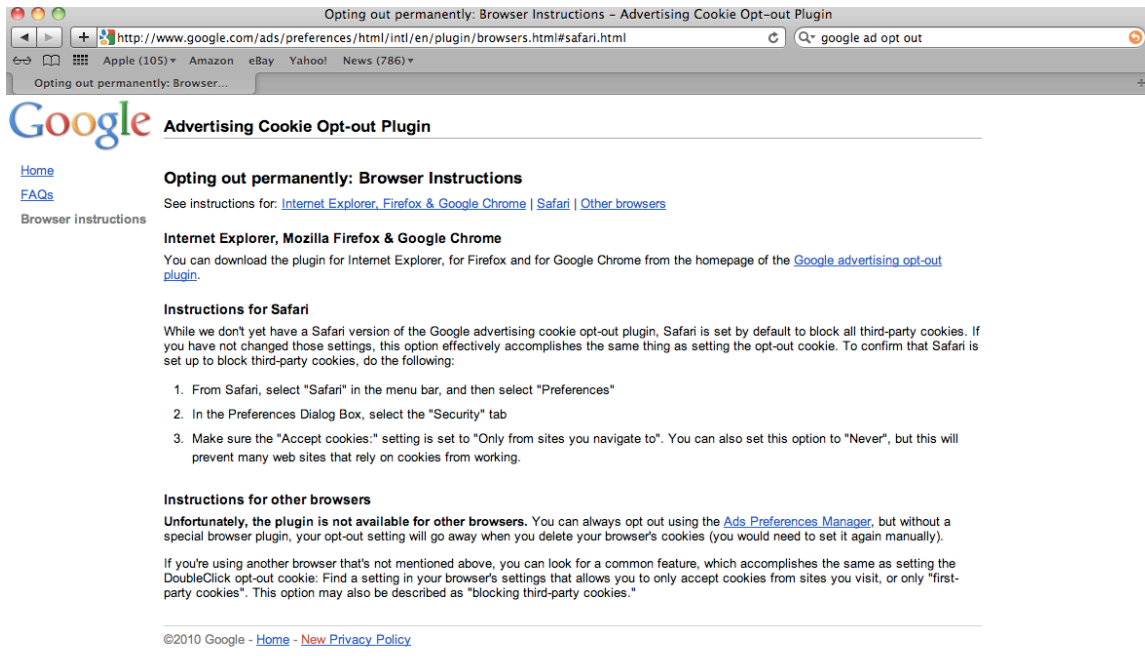


Fig. 1. A screenshot of Google's browser instruction page prior to Feb. 17, 2012. The page is no longer available on Google.

Mayer's technical analysis found that Google's Doubleclick.net ID cookie was fully functioning in Safari despite users' settings to block all third party cookies. Google's characterization of its DoubleClick cookie settings and activities for Safari users was not true, and as such is a deceptive business practice. The Commission should take note that Google owns DoubleClick, effectively making Google the direct beneficiary of its unfair and deceptive practices in several ways.

In a statement sent to Ars Technica Feb. 17, 2012¹³, Google has issued further clarification of its decision to override consumers' choices:

"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.

Unlike other major browsers, Apple's Safari browser blocks third-party cookies by default. However, Safari enables many web features for its users

¹³ Jon Brodtkin, *Google hit with FTC complaint, says circumventing Safari privacy features accidental*, Ars Technica, Feb. 17, 2012. <http://arstechnica.com/tech-policy/news/2012/02/google-hit-with-ftc-complaint-says-circumventing-safari-privacy-features-accidental.ars>

that rely on third parties and third-party cookies, such as “Like” buttons. Last year, we began using this functionality to enable features for signed-in Google users on Safari who had opted to see personalized ads and other content--such as the ability to '+1' things that interest them.

To enable these features, we created a temporary communication link between Safari browsers and Google’s servers, so that we could ascertain whether Safari users were also signed into Google, and had opted for this type of personalization. But we designed this so that the information passing between the user’s Safari browser and Google’s servers was anonymous—effectively creating a barrier between their personal information and the web content they browse.

However, the Safari browser contained functionality that then enabled other Google advertising cookies to be set on the browser. We didn’t anticipate that this would happen, and we have now started removing these advertising cookies from Safari browsers. It’s important to stress that, just as on other browsers, these advertising cookies do not collect personal information.

Users of Internet Explorer, Firefox and Chrome were not affected. Nor were users of any browser (including Safari) who have opted out of our interest-based advertising program using Google’s Ads Preferences Manager."¹⁴

Google’s statement clarifies that its circumvention of consumer choice was intentional and not a coding error. Google claims that they did not anticipate the *full extent* the effect its tampering would have, in that Google *advertising* cookies would be set on the browser. This is something a privacy audit should have uncovered. Further, even if the extent of the tampering was unintentional, the issue of circumventing consumer choice and engaging in consumer “mind reading” is inappropriate by technology companies.

Was Google’s privacy staff consulted when these actions were taken? We do not know which answer to this question is more condemning. If Google failed to consider the privacy consequences of its actions, then its internal privacy function is irrelevant. If the privacy staff raised no objection, then the privacy staff did not comply with the Google Buzz consent agreement. If the privacy staff was consulted and ignored, then Google’s privacy function has no effect.

¹⁴ Statement of Google's Senior VP of Communications and Public Policy, Rachel Whetstone, to Ars Technica, published Feb. 17, 2012. <http://arstechnica.com/tech-policy/news/2012/02/google-hit-with-ftc-complaint-says-circumventing-safari-privacy-features-accidental.ars>.

The World Privacy Forum additionally objects to Google’s characterization of these circumvention activities as anonymous. As the Commission has robustly documented, cookies are a form of ID tags that link information. Even if no personal information is contained in the cookies themselves, the cookies can act to link information and can therefore act as de-facto identifiers. The cookies serve to treat a particular computer, browser, and user as distinct consumers and to serve content individually selected for that particular computer, browser, and user. The potential absence of a name or other overt identifier in this activity does not make the activity anonymous.

Google merits additional attention because of the Buzz consent agreement. Google has an active consent agreement with the Commission for its privacy failures in its Buzz product.¹⁵ The World Privacy Forum believes Google has violated its Buzz consent agreement with the Commission.

The Buzz consent order stated:

IT IS ORDERED that respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:

A. the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information.

B. the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any other entity, including, but not limited to, the U.S.-EU Safe Harbor Framework.

Google violated A by its misrepresentations of consumer choice and how much control users actually had. Google potentially violated B by its probable lack of compliance with the NAI agreement.

Additionally, Google underwent a compliance audit for the Buzz Consent Decree, and sent a statement regarding its compliance audit to the Federal Trade Commission. In the compliance audit sent to the Commission Google stated:

“Google’s comprehensive privacy program, described in greater detail and referred to as the “Privacy Effort” subsequently in this Report, reasonably assures that Google is acting in a manner consistent with its public representations regarding the privacy and confidentiality of covered information.”¹⁶

¹⁵ <http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf>

¹⁶ <http://epic.org/privacy/ftc/google/120210-FTC-Self-Assessment-012612.pdf>

Further, Google affirmed to the FTC:

“Google has implemented a privacy risk assessment process in order to identify foreseeable material risks, both internal and external, as well as key privacy processes including training, product design, development, and research that help to mitigate these risks.

.... The Google privacy risk assessment process evaluates potential privacy risks and the sufficiency of existing controls. At the end of each risks assessment cycle, the privacy risk assessment team identifies areas of risk which might warrant additional mitigation, suggests additional or alternative mitigating controls to improve the risk posture of covered information, and escalates these control recommendations as appropriate for evaluation and implementation.”

Google has reassured the Commission that it is acting in a manner consistent with its public representations regarding the privacy and confidentiality of covered information. We note that “covered information” in the Buzz consent agreement includes persistent identifiers. However, we now have express evidence that Google made an inconsistent privacy representation regarding its DoubleClick ad cookies for Safari users. Google has described its risk assessment program as a robust, thorough program. How did something as significant as circumventing browser controls slip through a risk assessment program?

The World Privacy Forum believes Google has violated the terms of its Buzz consent agreement. We also question the efficacy of the risk assessments it is using as described in its compliance audit, and the Commission needs to review the quality and independence of that risk assessment.

To conclude, the World Privacy Forum requests that the Commission investigate each of the companies that overrode Safari users’ browser privacy settings. We also request the Commission investigate NAI member violations of the NAI code. We further request that the Commission investigate whether Google violated the terms of the Buzz settlement in its actions and in its description of its activities in its compliance audit. And finally, the World Privacy Forum requests that the FTC make a declarative statement about the unfairness and deceptiveness of circumventing users’ privacy settings in browsers.

Thank you for your attention to this matter. Respectfully submitted,

s/

Pam Dixon
Executive Director, World Privacy Forum

CC: Commissioner Julie Brill; Commissioner Edith Ramirez; Commissioner J. Thomas Rosch; David Vladeck, Director Bureau of Consumer Protection; NAI Executive Director Marc Groman