

©2013 Bloomberg Finance L.P. Originally published by Bloomberg Finance L.P. Reprinted with permission.

The Opinions expressed are those of the author.

**COOKIES**

The author reviews recent moves by browser manufacturers to limit third-party cookies, asking whether the changes are truly disinterested and pro-consumer. The author cautions those in the online advertising space to be wary of the competitive consequences these changes may render.

**Is Web ‘Transparency’ Good for Competition?**

BY ALLISON SHEEDY

Earlier this year, Mozilla, the open source software foundation, announced plans to block automatically certain types of Internet “cookies” in an upcoming version of its Firefox browser.<sup>1</sup> The target of Mozilla’s blocking efforts is cookies from “third parties”—cookies set by a website other than the one a user is currently visiting.<sup>2</sup> Third-party cookies are a fundamental part of the online infrastructure used to deliver targeted advertising to Internet users when they visit websites.

Is the move to limit cookies a disinterested pro-consumer move? Maybe not. Industry reports suggest

that Mozilla may be entering the targeted advertising business itself.<sup>3</sup>

Google, architect of the Chrome browser, also has announced plans to replace third-party cookies with its own brand of unique identifier.<sup>4</sup> Microsoft similarly has publicized a proposal to replace third-party cookies with its own tracking technology that can track users across multiple devices.<sup>5</sup> Apple, for its part, has longed

<sup>1</sup> Alex Fowler, *Firefox Getting Smarter About Third Party Cookies*, MOZILLA PRIVACY BLOG, Feb. 25, 2013, <https://blog.mozilla.org/privacy/2013/02/25/firefox-getting-smarter-about-third-party-cookies/>

<sup>2</sup> Mozilla Support, <http://support.mozilla.org/en-US/kb/disable-third-party-cookies> (last visited Dec. 11, 2013).

Allison F. Sheedy is an attorney in the Washington, DC office of Constantine Cannon. Ms. Sheedy’s practice focuses on civil antitrust litigation, government antitrust investigations involving potentially anticompetitive business practices, and consumer protection matters.

<sup>3</sup> See Kate Kaye, *Mozilla Tool Could Turn Firefox into Ad Data System*, ADAGE, July 25, 2013, <http://adage.com/article/datadriven-marketing/mozilla-tool-turn-firefox-ad-data-system/243315/> (reporting that Mozilla is experimenting with system that targets content based on web browsing activity);

Zach Rodgers, *Mozilla Hires Digital Ad Star Darren Herman To Lead New Content Unit*, ADEXCHANGER, NOV.26, 2013, at

<http://www.adexchanger.com/platforms/mozilla-hires-digital-ad-star-darren-herman-to-lead-new-content-unit/> (announcing Mozilla’s hiring of digital advertising executive to head new content unit, to add additional forms of content “including but not limited to advertising”).

<sup>4</sup> Alistair Barr, *Google May Ditch ‘Cookies’ As Online Ad Tracker*, USA TODAY, Sept. 17, 2013, available at <http://www.usatoday.com/story/tech/2013/09/17/google-cookies-advertising/2823183/>.

<sup>5</sup> Tim Peterson, *Bye, Bye Cookie: Microsoft Plots Its Own Tracking Technology to Span Desktop, Mobile, Xbox*, ADAGE, Oct. 9, 2013,

<http://adage.com/article/digital/microsoft-cookie-replacement-span-desktop-mobile-xbox/244638/>.

blocked third-party cookies in its Safari browser by default.<sup>6</sup>

The presumptive reason presented for these anti-cookie policies is the enhancement of consumer privacy.<sup>7</sup> Yet when viewed from a competitive framework, the privacy debate surrounding third party cookie blocking may be pretextual. Replacing the third-party cookie with other proprietary tracking technologies will not eliminate the collection and use of personal information. Instead, it simply may consolidate market power in the hands of only a few, powerful, technology companies. If that happens, both consumers and small, entrepreneurial companies that rely upon online advertising revenue will be harmed.

## What Are Third-Party Cookies?

A “cookie” is a file saved by a user’s web browser that is used to identify an Internet user as a discrete person through their computer’s unique online identifier.<sup>8</sup> Cookies function to recognize a user’s specific browser/computer combination.

Cookies placed on a browser by the website a user is viewing are relatively uncontroversial. They are known as “first party” cookies because the user is seen to have a first-party relationship with a website voluntarily visited.

Cookies may also be used by “third-party” companies other than the website being visited by an Internet user. These cookies store and share information about a consumer’s online activities across websites. Their most fundamental use is to collect anonymous-user information to deliver targeted or “interest based” advertisements and understand consumer behavior.<sup>9</sup> Tar-

geted advertisements make advertising more relevant, for, by example, limiting the number of times the same advertisement is shown to a particular user, or providing information about products connected to the user’s demographic or other browsing behavior.<sup>10</sup>

Notably, however, cookies cannot be used to identify *individuals*—only machines—so consumer data remains anonymous.

## Are Third-Party Cookies Anti-Privacy?

Third-party cookies have become the subject of an intense debate about consumer privacy. Privacy advocates criticize the use of third-party cookies for data collection as non-transparent in nature, citing lack of consent by consumers to have their personal—albeit de-identified—information used by others. They note that an unknown, but large number, of third parties collect data about Internet users using cookies.<sup>11</sup>

As a result, the idea of a “do not track” mechanism for the Internet has become an important public policy concern.<sup>12</sup> The Federal Trade Commission, for example, which operates the telemarketing Do-Not-Call registry, has been exploring the possibility of creating an online version of a Do Not Call list to allow consumers to opt out of anonymous online data collection.<sup>13</sup> There have also been efforts by lawmakers to introduce legislation granting greater authority to the FTC to regulate directly online tracking.<sup>14</sup>

## Will Proposed Limits Harm Consumers?

Some in the online-advertising industry claim, however, that doing away with third-party cookies by the dominant browsers is merely a way to capture advertising dollars. Simply put, online advertising is a multi-

<sup>6</sup> See Apple Safari Homepage, <http://www.apple.com/safari/#security> (last visited Dec. 16, 2013). However, as discussed below, Google was accused of manipulating the Safari browser to circumvent Apple’s default cookie-blocking policy and recently settled allegations by 37 states and the District of Columbia that it placed unauthorized cookies on Web browsers in 2011 and 2012. Rolfe Winkler, *Google Settles Privacy Case*, WALL ST. J., B7, Nov. 19, 2013.

<sup>7</sup> See Fowler, *supra* note 1 (describing rationale for third party cookie blocking fostering greater transparency, trust and accountability related to privacy); Apple Safari Homepage, *supra* note 7 (marketing Safari browser as having “advanced” privacy features and being “the first browser to block [third party] cookies by default”).

<sup>8</sup> Federal Trade Commission, *Cookies: Leaving a Trail on the Web*, <https://www.consumer.ftc.gov/articles/0042-cookies-leaving-trail-web>

<sup>9</sup> Notably, large first-party websites like Google, Facebook, and Amazon collect and use their visitor’s personal information in many of the same ways as do third parties—for example, to send targeted advertising. See, e.g., Google Ads Display Network Webpage, *Targeting Tools* (“Keyword Contextual Targeting delivers relevant messages to users based on the type of content they consume.”), <http://www.google.com/ads/displaynetwork/manage-your-ads/targeting-tools.html> (last visited Dec. 16, 2013); Facebook for Business Webpage, *Advertising*, <https://www.facebook.com/help/433385333434831> (last

visited Dec. 16, 2013); Amazon.com Webpage, *Interest Based Ads* (“On both Amazon-owned and operated sites and unaffiliated sites, Amazon displays interest-based advertising using information you make available to us when you interact with our sites, content, or services.”), <http://www.amazon.com/b?ie=UTF8&node=5160028011> (last visited Dec. 16, 2013).

<sup>10</sup> See Randall Rothenberg, *Why We Love the Cookie Monster*, INTERACTIVE ADVERTISING BUREAU BLOG, Dec. 22, 2010, <http://www.iab.net/iablog/public-policy/>

<sup>11</sup> A browser tool called Ghostery is available to scan websites a user visits and provide notification of the companies whose code is present on the webpage. See <https://www.ghostery.com/> (last visited Dec. 16, 2013).

<sup>12</sup> See generally Jonathan Mayer, WebPolicy Blog, <http://webpolicy.org/category/privacy/do-not-track/>

<sup>13</sup> Julia Angwin & Jennifer Valentino-Devries, *FTC Backs Do-Not-Track-System for Web*, WALL ST. J., Dec. 12, 2010, at <http://online.wsj.com/news/articles/SB10001424052748704594804575648670826747094>

<sup>14</sup> Earlier this year, Senator Jay Rockefeller reintroduced proposed legislation that would require the FTC to establish standardized mechanisms to give consumers control over online tracking activity. See Natasha Singer, *Senator Seeks More Data Rights for Online Consumers*, NY TIMES, Feb. 28, 2013.

To request permission to reuse or share this document, please contact [permissions@bna.com](mailto:permissions@bna.com). In your request, be sure to include the following information: (1) your name, company, mailing address, email and telephone number; (2) name of the document and/or a link to the document PDF; (3) reason for request (what you want to do with the document); and (4) the approximate number of copies to be made or URL address (if posting to a website).

billion dollar business. And much of the Internet's free content exists because of advertising. Even large publishers, for example, have struggled to find revenue models that make publication on the Internet viable without the support of advertising.<sup>15</sup> And even ubiquitous services like search functionality rely heavily on advertising dollars: Google's 2012 SEC filings, for example, reveal that online advertising accounts for 95% of its revenue.<sup>16</sup> The value in online advertising lies in the ability to make advertising relevant, i.e., target users with ads.<sup>17</sup>

Independent advertisers argue that the end of third-party cookies will be the downfall of small Internet publishers who depend upon advertising revenue to survive.<sup>18</sup> Their business models depend upon the ubiquity of third-party cookies. They claim it will harm consumers, who may no longer have free access to ad-supported online content, either because the sites will be forced to charge subscriptions for access or because the content will disappear entirely.<sup>19</sup>

They also argue that consumer tracking will not disappear even if third-party cookies are inhibited or eliminated. Mozilla, Google, and Microsoft are all said to be developing a competing tracking technology to cookies that would have the ability to function in an integrated fashion on multiple user devices (e.g., mobile phones and tablets) and interfaces.<sup>20</sup> The proposed changes would allow any one of these companies—as a first party—to track a unique person across multiple devices and multiple websites. At the same time, these companies are rumored to be considering blocking third-party cookies on their browser platforms. This change could eliminate the ability of third parties to collect information about Internet users who browse the web using Firefox, Chrome, or Internet Explorer. And because the browser manufacturers intend to collect user data themselves—and presumably sell it to advertisers—they

stand as current or future horizontal rivals to the third parties who currently perform that function.

As a result, the elimination of third-party cookies simply may concentrate the power and ability to collect valuable consumer data into the hands of a smaller number of first-party firms. This change undoubtedly will make their first-party data more valuable.<sup>21</sup> On the privacy side, however, the fact that fewer companies have access to personal information does not mean that information is more protected. Indeed, because first parties like Mozilla, Google, Microsoft and Apple can track users over a variety of devices and interfaces, the consumer data that they collect stands to be more comprehensive than anything collected by a third party. Hence, the proposed browser cookie policies could heighten, rather than alleviate, privacy concerns.

## A Monopoly in Online Advertising?

Denials of access like blocking the ability of third parties to obtain data may be anticompetitive where they function to create or maintain a monopoly.<sup>22</sup> Indeed, research suggests that Google and Facebook already control 95 percent of online advertising revenue.<sup>23</sup> If new anti-cookie policies change the landscape of the current market,<sup>24</sup> permit first parties to raise prices for access to consumer information, or restrict the ability of new entrants to gain access to consumer information, it starts to look like classic monopolistic behavior under Sherman ActSection 2.<sup>25</sup> If there is a coordinated effort by browser manufacturers or other first parties to render these changes, it could be an agreement to monopolize under Sherman ActSection 2.<sup>26</sup>

## Regulators and the Courts

The collusion between privacy concerns and competition is destined to play out at the both regulatory and litigation levels. Regulators in Europe are already voicing concerns about the potential anticompetitive effects related to the concentration of access to personal data. Joaquin Almunia, the Vice President of the European Commission, has cautioned that “exclusive access to

<sup>15</sup> See Tom Rosenstiel, Mark Jurkowitz, & Hong Ji, *The Search for a New Business Model*,

Pew Research Journalism Project, Mar. 5, 2012, at <http://www.journalism.org/2012/03/05/search-new-business-model/>

<sup>16</sup> Google, Inc. Form 10-K for the Fiscal Year ended Dec. 31, 2013, at <http://www.sec.gov/Archives/edgar/data/1288776/000119312513028362/d452134d10k.htm>

<sup>17</sup> Howard Beales, *The Value of Behavioral Advertising*, Study by the National Advertising Initiative, at 11,

[http://www.networkadvertising.org/pdfs/Beales\\_NAI\\_Study.pdf](http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf) (2010).

<sup>18</sup> See generally, Interactive Advertising Bureau, *FAQ On Mozilla's Intent To Block Third Party Cookies*, <http://www.iab.net/mozilla> (last visited Dec. 16, 2013) (arguing small publishers will not be able to get fair price for publishing advertisements absent third party cookies); Interactive Advertising Bureau, *IAB President & CEO Randall Rothenberg's Statement Opposing Mozilla's Intention to Block Third-Party Cookies* [http://www.iab.net/mozilla\\_rothenberg](http://www.iab.net/mozilla_rothenberg) (last visited Dec. 16, 2013); see also Kenny Katzgrau, *Mozilla to Block Third-Party Cookies: What Does It Mean for Small, Online Publishers?*, *BroadStreet*, Mar. 18, 2013

<http://broadstreetads.com/blog/mozilla-blocks-third-party-cookies-what-does-it-mean/> (reporting that “publishers who depend on remnant ads can probably expect a 20% drop in remnant display income over time”).

<sup>19</sup> See, e.g., *IAB President & CEO Randall Rothenberg's Statement Opposing Mozilla's Intention to Block Third-Party Cookies*, *supra* note 16 (“All users, no matter the browser they're using, will lose access to independent websites produced by small businesses.”).

<sup>20</sup> See notes 3, 5, & 6 *supra*.

<sup>21</sup> Mitch Weinstein, *Why Blocking Third-Party Cookies Is Good For Google And Facebook*, *AdEXCHANGER*, June 20, 2013, at

<http://www.adexchanger.com/data-driven-thinking/why-blocking-third-party-cookies-is-good-for-google-and-facebook/>

<sup>22</sup> See *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 605 (1985) (“The question whether conduct may properly be characterized as exclusionary” must take into account “whether it has impaired competition in an unnecessarily restrictive way.”).

<sup>23</sup> Claire Atkinson, *Google, Facebook Dominate Ad Dollars*, *NEW YORK POST*, Sept. 22, 2013, at <http://nypost.com/2013/09/22/google-facebook-dominate-digital-advertising-dollars/>

<sup>24</sup> See *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 604 (citing “a decision by a monopolist to make an important change in the character of the market” as indicia of monopolistic behavior).

<sup>25</sup> See *United States v. E.I. DuPont de Nemours & Co.*, 351 U.S. 377, 391 (1956) (defining monopoly power as “the power to control prices or exclude competition”).

<sup>26</sup> See *Biovail Corp. v. Hoechst AG*, 49 F. Supp. 2d 750, 767 (D.N.J. 1999) (recognizing claim for agreement to monopolize).

personal data in a given market could give rise to concentration concerns.<sup>27</sup>

While there has been virtually no publically expressed antitrust interest yet by U.S. regulators surrounding the collection of personal data, a recent case on the privacy side portends how courts might examine some of the issues.

In October 2013, a federal district court in Delaware dismissed plaintiffs' challenges to Google's alleged circumvention of the default blocking technology in Safari, so that third-party cookies were surreptitiously allowed.<sup>28</sup> Bringing claims under several federal and state laws related to computer fraud, plaintiffs claimed to have suffered injury to "the value,

privacy and confidentiality of their Personally Identifiable Information" as a result of Google's alleged conduct.<sup>29</sup>

However, the court found that plaintiffs lacked Article III standing to bring their challenge because they had not adequately alleged any actual injury.<sup>30</sup> The court concluded that while personal identifiable information ("PII") has some "modicum" of identifiable value to an individual plaintiff, plaintiffs had not alleged that the ability to monetize PII was diminished by any practice of Google.<sup>31</sup> Hence, the court called into question the ability of certain plaintiffs to bring antitrust challenges related to data collection.<sup>32</sup>

A related question is how, under the antitrust laws, a relevant product-market might be alleged in the event of a challenge to the elimination of third-party cookies by browser manufacturers. A relevant product-market is the group of products and suppliers that compete, de-

termined, at a basic level, by how substitutable one product is for another.<sup>33</sup>

In 2012, online advertising in the United States was reported to be a \$36.6 billion business. Competition authorities apparently consider online display advertising to be a distinct market from online search-based advertising (the small text advertisements that appear next to search page results).<sup>34</sup> While it is likely that changes to browser cookie policies will affect online advertising, the product the really appears to be at stake is the collection of consumer data that can be gleaned from a user's internet activity. This information is sometimes characterized as "big data" and has been deemed to be the "new oil" of the information economy.<sup>35</sup> Indeed, at least one FTC commissioner has conceptualized big data as a possible product market.<sup>36</sup> The myriad and interconnected web of companies, products, and services that relate to targeted online advertising present challenges in determining the actual competitive landscape, and therefore, in defining a relevant product market.<sup>37</sup>

Because of the potential elimination of third-party cookies, there appears to be a situation in the making where a small number of first parties will have control over the ability to collect meaningful consumer data based on Internet activity. If a small number of firms control access to this information, they will potentially have the ability to control the cost of big data and exclude competitors, no matter how the relevant product market is defined.

The elimination of third-party cookies stands on the horizon for 2014. But the proffered privacy gains appear to be limited, and those involved in the online advertising space should be wary of the competitive consequences these changes may render.

<sup>27</sup> Joaquin Almunia, *Competition and personal data protection Privacy Platform event: Competition and Privacy in Markets of Data*, Nov. 26, 2012, at [http://europa.eu/rapid/press-release\\_SPEECH-12-860\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm)

<sup>28</sup> *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, MDL Civ No. 12-2358. Google settled similar allegations brought by the FTC in 2012 for \$22.5 million, and settled last month with 37 states and the District of Columbia for \$17.5 million related to the same practices. See FTC Press Release: *Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, Aug. 9, 2012, at <http://www.ftc.gov/opa/2012/08/google.shtm>.

<sup>29</sup> See *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, MDL Civ No. 12-2358, (D. Del.), Am. Compl., filed Dec. 19, 2012, at 70.

<sup>30</sup> See *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, MDL Civ No. 12-2358, Mem., Op. at 7, Oct. 9, 2013, <http://www.ded.uscourts.gov/sites/default/files/opinions/slr/2013/october/12-2358.pdf>

<sup>31</sup> *Id.* at 6.

<sup>32</sup> The requirement of injury in fact is equally applicable under the antitrust laws. See, e.g., *Story Parchment Co. v. Pater-son Parchment Paper Co.*, 282 U.S. 555, 563 (1931).

<sup>33</sup> See *Brown Show Co. v. United States*, 370 U.S. 294, 325 (1962) ("The outer boundaries of a product market are determined by the reasonable interchangeability of use or the cross-elasticity of demand between the product itself and substitutes for it.")

<sup>34</sup> See, e.g., *Statement of the Federal Trade Commission Concerning Google/DoubleClick*, FTC File No. 071-0170, at \_\_\_\_\_. The online advertising industry similarly distinguishes between display advertising and search advertising. See IAB Internet Advertising Revenue Report, Apr. 2012, at \_\_\_\_.

<sup>35</sup> Perry Rotella, *Is Data the New Oil?*, FORBES, Apr. 2, 2012, at \_\_\_\_.

<sup>36</sup> See *In the matter of Google/DoubleClick*, F.T.C. File No. 071-0170, Dissenting Statement of Commissioner Pamela Jones Harbour, at 9, [http://www.ftc.gov/sites/default/files/documents/public\\_statements/statement-matter-google/doubleclick/071220harbour\\_0.pdf](http://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf) ("In this case, for example, it might have been possible to define a putative relevant product market comprising data that may be useful to advertisers and publishers who wish to engage in behavioral targeting.")

<sup>37</sup> See *AdExchanger*, *Display Advertising Technology Landscape*, at <http://www.adexchanger.com/wp-content/uploads/2010/09/LUMA-Display-Ad-Tech-Landscape-for-AdExchanger.jpg>