Mozilla Says Enough is Enough

by Justin Brookman [1]
February 26, 2013

This weekend, the online advertising industry woke up to a bombshell that will fundamentally change their business: Mozilla's Firefox web browser will no longer let ad networks set cookies on user devices. As a result, ad networks will have a much harder time tracking users around the web, and developing profiles on those users in order to determine which ads to show them. In the short-term, this will result in less revenue to the ad networks, and also to the websites that rely on them. However, in understanding why Mozilla made this change — and why it makes sense — we need to examine the explosion of online tracking in recent years, and the failure to offer users meaningful control over their personal information.

For more than two years [2], Mozilla's Firefox web browser has included a "Do Not Track" setting that lets users signal to the world that they don't want to be tracked. When users turn on this feature, every single communication from the browser to a website includes an attached header stating that the user doesn't want to be tracked. In February of last year, industry representatives attended a White House privacy event and publicly committed [3] to respect browser headers like "Do Not Track," estimating it would be able to comply with users' browser preferences "within nine months."

Nonetheless, today, only a handful of ad networks [4] do anything at all when they see a user's "Do Not Track" header, and negotiations within the World Wide Web Consortium (W3C) over how to define "Do Not Track" have been stalled for several months. Many in the advertising industry continue to insist on excessively broad exceptions to "Do Not Track" instructions, as well as the right to reject "Do Not Track" signals where they believe the user is not sufficiently informed [5] about how tracking works. Indeed, representatives from the Direct Marketing Association recently proposed that "marketing" [6] and "advertising" [7] be recognized as exceptions to "Do Not Track" requests — which would effectively defeat the purpose for which "Do Not Track" was originally proposed [8].

At some point, something had to break the logjam. That may have happened last Friday, when Mozilla made the decision [9] to set its privacy default settings to block third parties from setting cookies to track users around the web. This means when you visit a website like NYTimes.com with the updated Firefox browser, the only cookies your browser will have set or modified will be either from NYTimes.com — the "first party" in your transaction — or from third parties you have already visited as a first-party (say Like buttons from Facebook.com). Ad networks that supply the banner ads for the site won't be able to place cookies, which could then be recognized on other websites where they also serve ads (thus letting them develop a behavioral profile on that user). Mozilla had debated this patch for weeks in its development forums [10], and ultimately decided that stopping third-party cookies reflects the wishes of their users. Given the continued lack of an agreement on a "Do Not Track" standard, we think they made the right call.

Self-Regulation Hasn't Kept Pace

CDT [11] and others [12] had predicted that if the ad industry didn't commit to a robust "Do Not Track" standard in short order, browser companies were going to take matters into their own hands to protect their users. Countless polls have shown that those users don't understand the value proposition for behavioral advertising, and object to a tracking ecosystem they don't understand. (Microsoft has cited the same rationale in support of their decision [13] to turn on "Do Not Track" for users who go with Internet Explorer 10's recommended settings.)

Industry to their credit has taken steps to ameliorate some user concerns. The revised code [14] for the Digital Advertising Alliance restricts the use or sale of behavioral data for particularly impactful uses like employment, insurance, or credit eligibility. And ad networks have committed to the laborious and no doubt expensive undertaking of putting an icon in all their ads (which users can

click on to learn to learn more about tracking, or opt out of behavioral advertising), though it's not clear [15] that average users have noticed or understood.

At the same time, despite these efforts, third party tracking has expanded dramatically in recent years. Sites that used to drop two or three third-party cookies are now dropping dozens (or 223 [16] in the case of Dictionary.com). Moreover, behavioral profiles that used to be "anonymous" (well, let's say pseudonymous) are increasingly linked to real name and off-line behavior [17] — crossing a line in the sand [18] that had been implicitly agreed upon for years [19]. In a compelling (and well-timed!) op-ed in MediaPost last week entitled "Suicide by Cookies," one long time industry player summarized [20]:

> "Self-regulation hasn't worked the way we'd promised Washington it would."

Of course, Mozilla's decision is just an interim step. Third party cookies are the most common tracking technology, but they certainly aren't the only way to track users on the web. Ad networks now face a brutal choice, at least in the short term: give up on tracking Firefox users, or use less transparent tracking technologies like browser fingerprinting, cookie syncing, Flash cookies, simulated first-party cookies, or history sniffing — potentially inviting regulatory scrutiny (the FTC has already brought Section 5 enforcement actions involving those last [21], three [22],options [23].)

A Way Forward?

But if this is now a war as one industry rep has suggested [24], and ad networks do decide to try to get around Firefox's settings, it's not clear this is a war they can win. Browsers have a direct relationship with the user. On the other hand, ad networks' relationship with the user is intermediated by those same browsers, as well as publishers who are also increasingly worried about user trust. (Yes, publishers may benefit from that tracking as well, but it's never been clear how much of the value from behavioral advertising flows back to the publishers, instead of just supporting the tracking middlemen.)

In drawing attention to the Mozilla update, privacy researcher Jonathan Mayer (who originally proposed the change [10] in December) did offer a potential olive branch [25]: perhaps the new cookie rules could be relaxed for sites that do eventually honor "Do Not Track." Fundamentally, most of the online tracking that occurs can be done in a minimally invasive way, with reasonable collection, use, and retention limitations. If there were clear and fair standards in place for the collection and use of personal information, perhaps it makes sense for behavioral tracking to be governed by a single opt out such as Do Not Track (at least in the United States; Europe with its e-Privacy Directive is a different matter). However, in the face of an ever-expanding third-party monitoring of their users' web browsing, it's understandable why Mozilla wanted to put the brakes on it. Industry can complain that this will kill innovation and the open web, but it's hard to deny that the web works pretty well on Apple's Safari browser — which has blocked third-party cookie setting for years.

CDT remains hopeful that we can reach accommodation on a reasonable opt-out regime [26] for third-party tracking in the W3C's Tracking Protection Working Group. For too long, delay favored the online advertising industry, who were understandably not thrilled at the prospect of spending money to reengineer their systems to monetize ads less effectively. With Firefox making third-party tracking a lot harder going forward, the ad networks have a lot more incentive to negotiate today.

Links:

[1] https://www.cdt.org/personnel/justin-brookman
[2] http://blog.mozilla.org/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/
[3] http://www.aboutads.info/resource/download/DAA_Commitment.pdf
[4] http://donottrack.us/implementations
[5] http://lists.w3.org/Archives/Public/public-tracking/2012May/0284.html
[6] http://www.w3.org/2011/tracking-protection/track/issues/178
[7] http://www.w3.org/2011/tracking-protection/track/issues/180
[8] https://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf
[9] https://blog.mozilla.org/privacy/2013/02/25/firefox-getting-smarter-about-third-party-cookies/
[10] https://bugzilla.mozilla.org/show_bug.cgi?id=818340
[11] http://www.huffingtonpost.com/leslie-harris/the-bizarre-belated-assau_b_1935668.html
[12] http://www.linkedin.com/today/post/article/20130124005038-258347-cookie-we-have-a-problem?trk=mp-author-card
[13] http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/10/26/privacy-and-technology-in-balance.aspx
[14] http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf
[15] http://www.mediapost.com/publications/article/187186/20-of-web-users-notice-behavioral-advertising-ico.html#axzz2LwqOCm64
[16] http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html
[17] http://online.wsj.com/article/SB10001424127887324784404578143144132736214.html
[18] https://www.cdt.org/blogs/justin-brookman/why-facebook-apps-story-problem-entire-web
[19] http://adage.com/article/news/abacus-deal-quaint-today-s-data-era/239154/
[20] http://www.mediapost.com/publications/article/194073/suicide-by-cookies.html#axzz2LsUVQ6Ny
[21] http://ftc.gov/opa/2011/11/scanscout.shtm
[22] http://ftc.gov/opa/2012/08/google.shtm
[23] http://www.ftc.gov/opa/2012/12/epic.shtm
[24] https://twitter.com/mikezaneis/status/305320662426324992
[25] http://webpolicy.org/2013/02/22/the-new-firefox-cookie-policy/
[26] http://lists.w3.org/Archives/Public/public-tracking/2012Apr/0078.html