SUBJECT: TRR Comment Period Response
FROM: Matt Corallo <[redacted]
TO: [redacted]
DATE: 20/11/2020 04:10

First of all, thank you for running a comment period on DoH/TRR - there has been a lot of criticism of Mozilla's stance here and lack of acknowledgement of that came off incredibly tone-deaf to loyal Firefox users.

I'd like to focus only on the TRR program - indeed, DoH is "just a technology", and one that can be used well or poorly, providing increased security and privacy when used well. Mozilla's continued mixing of terminology between DoH and its own TRR policy has significantly confused the public discussion, and reads as if the marketing department is trying hide the issues with TRR by incorrectly claiming that "everyone else is doing the same thing". Indeed, no other browser vendor has a DoH policy remotely similar to TRR as it stands today.

As many have pointed out, the net effect of the current TRR deployment has been that Firefox, by default, shares the full list of websites visited directly with Cloudflare, a third party which has a mixed history of user-first decisions and which users naturally have very diverse views on. While some users may be fine with this, others are, very vocally, not.

This is done with the claim that sending Cloudflare user browsing information will improve user privacy. However, the reality is, even with TLS 1.3, a network-level attacker (or a users' ISP) can see the full list of every website which a user visits, with or without DoH/TRR. Thus, the TRR default-on behavior not only does not change a users' privacy from network-level attackers (or their ISP), but only strictly reduces user privacy by sending the same data to an additional third-party without any active user consent. The Mozilla marketing department's claim that this clear degredation in privacy somehow *improves* user privacy makes the situation all the more absurd - almost to the point of maliciousness.

Consider the outrage if Google were to silently opt all Chrome users into sending the full list of websites they visit directly to Google in unencrypted form, with or without a statement that users need "not worry and that their privacy will be respected" - this is what Mozilla has done.

The world Mozilla (and Cloudflare) envision is one where ESNI/ECH is ubiquitous, where some claim that network-level attackers will no longer learn any useful information. However, not only is such a world a very long ways off (indeed, ECH does not exist in production *anywhere* yet, as its design isn't finalized!), but it also requires assuming the internet consists only of perfectly spherical cows. Even in a world where ECH is ubiquitous, network-level attackers still learn the IP addresses with which data is being exchanged, as well as the quanitity and "shape" of such data.

Back in the real world, this data is likely to enable motivated network-level attackers to make strongly educated guesses as to which websites are being visited. Even if every website switches to using Cloudflare (what a great outcome for the internet!), reducing user privacy *now* in anticipation of some perfect future later seems incredibly dubious.

As the world of Chrome-based browsers continues to ensure that users can be tracked broadly online, Mozilla's stance of sharing the list of sites their users visit with a large, multi-national, trusted third party, subject to regulations and court orders in many countries around the world puts Mozilla at the back of the crowd. At a time when users crave protection from pervasive online monitoring, Mozilla is squandering its reputation, with many, myself included, recommending users find other browsers that protect their privacy.

Despite the massive blunder that is TRR deployment to date, the motivation is sound - migrating users to obtaining DNS information over an encrypted channel is great. Chrome's approach has been to work with ISPs (which see the sites users visit even with DoH) to offer such an encrypted channel to as many users as possible - strictly improving user privacy from other network attackers without introducing TRR's additional privacy leak. Further, using the TRR program to do the same while extracting privacy-preservation commitments from ISPs, as Mozilla has done with Comcast, is a fantastic outcome! Even better, because such changes do not impact where user data flows or carry significant tradeoffs, users can be freely be opted-into such changes without nagging dialog boxes or the outrage we've seen around TRR.

Instead of moving forward with TRR deployment as-is, Mozilla needs to carefully ensure that it is encouraging its users to share their browsing data with additional third-parties only as a last resort. This must focus only on users with well-known privacy-hostile ISPs, ensuring users on small/medium ISPs across the globe are not impacted, especially as many small/medium ISPs already work hard to protect user privacy.

Mozilla's lack of communication and unwillingness to admit the technical realities and tradeoffs the TRR program makes has been embarassing to a fault - more accurate communication is a must. The reality is privacy is hard, and trying to sugar-coat tradeoffs by claiming everything is just dandy is misleading to the extreme.

Finally, Mozilla should take a strong stance that active user consent is a *must* when providing the full list of websites users visit to third-parties. Users on large ISPs which refuse to provide privacy protection for DNS queries would likely welcome a notification and happily "switch to using Cloudflare for to provide privacy from your ISP," without burying our head in the sand to pretend such decisions are best for all users.

Thank you for your consideration,

Matt Corallo
Long-Time Firefox User