SUBJECT: DoH/TRR Comments
FROM: "Livingood, Jason" <[redacted]
TO: "[redacted] <[redacted]
DATE: 19/11/2020 23:17
ATTACHMENTS (20201119-231731-0000014): [redacted]

Feedback follows below in response to your questions. These are my personal views and are not endorsed by my employer.

- Jason

1. Our current policy states that user data must not be retained for longer than 24 hours. A number of DNS providers, however, only keep data in ephemeral state and delete it almost immediately.
1. To what extent can our requirement be shortened further while allowing providers sufficient data to operate the service?

Comment: Do not shorten the requirement as it is already sufficiently stringent. Given the small number of TRRs I can't see how increasing requirements will help meet your goal of broad global deployment across a wider range of TRRs. You have more work to do instead in signing up more TRRs at the current requirement level.

4. Our current policy establishes that DoH resolvers in our program must maintain a transparency report providing public insight into the extent to which the resolver has been subject to government requests for data. How can this requirement be improved? What other mechanisms, processes, and governance tools may exist that could provide the public additional insight into such requests?

Comment: Corporate transparency reports are a significantly larger and more complex subject area than growing DoH & TRR deployment. I would leave this sort of work to the EFF, EPIC, and other groups and focus instead on more DoH & TRR deployment.

1. Our current policy states that the provider operating the resolver should not by default block or filter domains unless specifically required by law in the jurisdiction in which the resolver operates. How, if at all, should this requirement change to address legally required blocking in other jurisdictions?

Comment: The TRR policy & agreement should be amended to permit a TRR to block or filter when required to do so under national/local law/court order. Otherwise it would seem a great many operators in the EU may be excluded from the TRR program, as many of those countries already have such mandates. While we can certainly argue whether such tactics are effective at a technical level, it is certainly the case that organizations must comply with their local laws whether or not those laws have the intended effect.

2. What harmful outcomes can arise from filtering/blocking through the DNS?

Comment: Clearly citizens may be unable to access legitimate news sources, social media sites, and so on. But this appears as a risk only in the most authoritarian of countries. So I think one way to mitigate this may be to have a TRR policy that excludes some of those countries from participating as a local TRR.

4. How could we ensure effective transparency and accountability in

situations where TRRs engage in legally required blocking practices?
(For example: publicly available transparency reports with blocked
domain names by country.)

Comment: Listing blocked names will in some cases be illegal. For example, in the US you could not share/publish the list of sites in the NCMEC list and I believe the UK has similar protected lists. I think instead it is sufficient to ask a TRR to disclose in their policies that they must comply with such block orders and to specify the types of blocks (e.g. under code XXXX of law, due to court order, etc.).

3. What are the best ways to gain global adoption/support of the DoH
standard amongst ISPs and DNS providers?

Comment: Signup ISPs and DNS operators in countries such as Germany and the UK where government-mandated blocks are a fact of operational life. Do this by creating a reasonable carve out in the TRR policy to accommodate operators that are required to take blocking action but are not otherwise in the business of doing so. My perception is they are quite willing to become TRRs and that in doing so would make a range of pro-privacy improvements so the net result would be overwhelmingly positive & further Firefox's privacy and security goals.

<end of comments>