SUBJECT: DoH public comment
FROM: Martin Millnert <[redacted]
TO: [redacted]
DATE: 20/11/2020 03:19
ATTACHMENTS (20201120-031946-0000022): [redacted]

Dear Mozilla Corporation,

first, a thank you for your open source products which I use, both for Email and Web Browsing.

I have two comments, regarding Privacy in the European Union in general, and safety risks to people under jurisdiction where use of e.g. non-state controlled DoH infrastructure is illegal.

First, regarding Privacy in the European Union:

A) It is without a question that the Domain Name System handles Personally Identifiable Information. My very own domain name is such an example.
B) In the European Union as per a recent verdict in the European Court of Justice, it is not legal to transfer PII to 3rd countries not meeting the standards of the European Union on citizens lawful right to privacy.
C) The USA, and corporations under its jurisdiction, notwithstanding where the physical infrastructure is geographically located (due to among other the US Cloud Act), are examples of 3rd countries where transfers of PII as would be the case with a browsers resolver traffic, is not allowed.
D) It would therefore be strictly legally necessary that no such provider is made available to citizens of the European Union, including but not limited to Cloudflare. The European Union law is extremely clear on this.

Secondly, regarding safety risks offline rather than online:

A) It is clear that different jurisdiction on Earth have different laws.
B) Certain jurisdictions have laws with varying degrees of punishments for circumventing e.g. state-controlled block lists.
C) There's also a non-state variant of this, for example enterprises with IT-policies governing e.g. acceptable use and so on, where using a non-enterprise approved resolver infrastructure might lead to violations of the IT-policy and therefore, wittingly or unwittingly, risk termination or worse.
D) In order to avoid causing unwitting harm to individuals who are using Mozilla Firefox, care must be taken as:
i. Users could wittingly or unwittingly enable DoH in an unapproved/illegal manner, exposing them to potential harm,
ii. Mozilla definitely need to take an enormous amount of care if ever considering enabling DoH by default, due to the risks that:
1. Users wittingly or unwittingly obtain a binary package with DoH enabled, rather than disabled,
2. Users could obtain the intended binary package, and in

violation of legal or contractual compliance have DoH enabled,
3. An automated Geo-IP-infrastructer is used to control Opt-In vs Opt-Out behaviour and the errors from this infrastructure can cause harm to users.

Some mitigations to these two problems might be:
- Distribute an EU-version of Mozilla Firefox with only fully GDPR-compliant TRR's, necessarily excluding any US-based corporations.
- Design a very considerate wizard and require users to actively opt-in to using DoH.
- Implement multiple layers of controls that must pass before DoH becomes activated.

In closing, moving the world towards more transparency on block-lists, especially when done for purely commercial reasons, is a worthwhile goal. But undervaluing or not properly understanding the challenges posed by the total sum of the world's jurisdictions risks causing actual physical harm to users of your products, an harm for which utimately Mozilla bears liability. For this reason, the safest option is to allow users to opt-in to using DoH, and make this an active choice for users.

Best regards,
Martin Millnert, Sweden