SUBJECT: Mozilla DoH implementation comment period
FROM: Matthijs Tijink <[redacted]
TO: [redacted]
DATE: 19/11/2020 23:55

Dear Sir/Madam,

I'm writing regarding the DoH implementation.

= Respecting privacy and security =

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?

A: I cannot think of a reasonable reason to keep data for such a long period. Also, it's clearly possible to operate with ephemeral state, since some providers already do so. To me, this is a clear indicator to shorten this period significantly, to perhaps minutes.

2. Are there exemptions that should be allowed by the policy for additional data collection in emergency circumstances? Please specify (e.g., the relevant circumstances as well as transparency and reporting requirements).

A: Yes, for law enforcement purposes, with a suitable warrant. This should only happen on case-by-case basis, not for large-scale monitoring. This should be transparent, except if that conflicts with the goal of this monitoring.

= Online safety =

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?

A: A resolver should respect the law of the user's restriction. If the operator does not want to comply with restrictions of an user's jurisdiction, it should not serve the user at all.
Ideally, the operator should block *only* the domains not allowed by the users' jurisdiction. This might be impossible, if the provider falls under another jurisdiction. How that should be handled is unclear to me.

3. What more rights-protective and technically effective means of protecting users from illegal and harmful content exist beyond DNS-based blocking?

Blocking based on ip-addresses.

= Building a better ecosystem =

1. How can deployment of DoH help to increase trust in Internet technologies in your region?

A: As far as I can tell, it only helps for protecting against snooping/ MitM'ing local network users.

2. What exploitations of the DNS in your region could DoH protect against?

A: As far as I can tell, such "exploitations" are against the law (here in the Netherlands), and ISP providers don't engage in them. So none.

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

A: Provide ways for non-browsers to seamlessly upgrade to DoH, without switching between DNS providers in the process. Implement DoH in common DNS servers, like BIND. E.g. try to connect with DoH to the configured DNS server, instead of some other DoH server.

4. Are there specific DNS use cases for which you think DoH would provide particular security and privacy value (e.g., when users connect over free public WiFi hotspots)?

A: Yes, in cases where the connection to the DNS server isn't trusted. Usually, that's in WiFi networks.

5. Although Firefox disables DoH when it detects that enterprise policies are in place, are there other situations in which deployment of DoH might cause technical or operational challenges (e.g., mobile networks, NAT64 and DNS64)?

A: Yes. DNS should follow user configuration (e.g. custom DNS on a device or local network level), and follow the user's jurisdiction's laws. If this is not possible (e.g. the operator's jurisdiction requires blocking additional domains), then DoH shouldn't be used automatically. Putting the user first is essential.

Kind regards,

Matthijs Tijink