SUBJECT: Input on DoH
FROM: "Penris, SJ (Bas)" <[redacted]
TO: "[redacted] <[redacted]
DATE: 20/11/2020 20:46

L.S.,

We've been following the gradual rollout of DoH and we are absolutely stumped that Mozilla has jumpe
and think it's an absolutely terrible idea.

- The addition of all the HTTP headers and information to DNS queries and having them sit with jus
  providers is a giant privacy issue because it enables continuous tracking of end users. More than
  that our local laws do not apply to these US tech giants. If I fly to Teheran the US authorities can e
  of me if I use DoH for example, which is impossible with unencrypted DNS or DNSoverTLS.
- We agree that DNS needs to be encrypted, but we want the current standard to be encrypted an
  least in no way should a browser ever make a choice for a user about this. Your argument will be
  way because you currently give your users a choice, i.e. you ask them if it's okay.
- I don't think I have to explain to you that users do not understand the question you ask them, wh
  they're unable to make a proper and informed choice. This also doesn't excuse the fact that in a f
  will just be turned on without this question being asked, as this is the way things work and that is
  depressing reality.
- We provide corporate VPN services with split DNS to many thousands of users, which will be grea
  by this.
- DNS resolving is ***not*** a task of the browser but of the operating system.
- Your TRR programme is far too restrictive and blocks smaller DNS providers from participating in
  you require insight into all information requests done on DoH which in many jurisdictions like The
  illegal. This is anti-competitive and shuts down innovation that normally comes from small newcc
  solidifies the market for the giants without the opportunity to ever open it up again.
- Lastly, you argue that we, corporate network admins, have the possibility to control access using
  as per https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https, but I d
  mechanism as it is a client application configuration setting and not an actual policy that forces b
  same way that we're used to. It's not transparent and the wrong way to address this. As there is r
  in the US, what is stopping all major providers from just implementing this so they can keep hijac
  queries? This means that your entire reasoning is fallacious.

I will now answer the questions from the PDF:

Privacy and Security

1. **No user information should ever be retained or stored**
2. **Again: There is no reason for DNS servers which aren't mine to store any user data**
3. **Your TRR program has a wrong design to begin with, so no, there are no considerations until yo
   program.**
4. **These requirements are broken by design and therefore the question is invalid**

Online Safety

1. **It's not a workable requirement. In our situation for example, we have no legal obligation to bl
   pornography or known sites that spread malware. As we're a giant institution for secondary ed
   we do block a certain minimum. Your proposal will decrease security and increase threats to ou
   network**
2. **Not relevant in our situation, we don't have any issues as it's working as designed and it's not a
   country faces to begin with**
3. **Decrypting all traffic at the firewall level and inspecting it, which we do not want to do**
4. **You can never ensure this as for example the US could easily pass a law that would require non
   an operation like this and no one would know**

are the US President and his AG Bill Barr, who considers the office of the president to be Omnip any regard for basic democratic and judicial principles.

2. **There is no exploitation of DNS here.**
3. **There should not be a push for DoH period.**
4. **No, as DoH will expose more of the user's information to certain parties than a simple and trad query**
5. **Corporate VPNs with split DNS but again, I don't want a browser in control of resolving, that is definition and end of discussion.**

Honestly, if you want to protect people that live under certain regimes, offer them free or heavily discou services but this does not solve any problems, it will just create dozens more for IT admins. Google's hes it out in Chrome, which is clearly due to them currently being investigated in multiple territories in antit be a major red flag to Mozilla. All efforts on DoH should be dropped *__immediately__* and attention shoul DoTLS.

Met vriendelijke groet,

Bas Penris

Stichting Carmelcollege

[redacted]