

SUBJECT: Mozilla DNS over HTTPS (DoH) and Trusted Recursive Resolver (TRR)

FROM: Fernando Gont <[REDACTED]>

TO: [REDACTED]

DATE: 14/12/2020 12:54

Folks,

Here is my feedback:

By changing the default recursive DNS server, you are changing trust relationships without user consent.

There are many trade-offs involved, that I have documented at length in these two documents:

*

<https://www.internetsociety.org/wp-content/uploads/2019/03/deploy360-dns-privacy-faq-v1.1.pdf>

*

<https://www.internetsociety.org/wp-content/uploads/2019/02/Deploy360-DNS-Privacy-Introduction.pdf>

As a user, there is no reason I should trust any company more than my ISP. And, if that trust assumption were to change, it should do so under my consent.

One additional factor is that for many of us not based in the USA, changing the recursive resolver from that provider by our ISP to one provider by a third company might even change the legal jurisdiction of the folks providing the DNS resolver service.

So, to put it bluntly: enabling DoH by default, and overriding the ISP-provided recursive DNS server by one of your choice is a **really bad idea**. Please refrain from that.

Thanks,

--

Fernando Gont

SI6 Networks

e-mail: [REDACTED]

PGP Fingerprint: [REDACTED]