SUBJECT:
FROM: Joshua Hudson <[redacted]
TO: [redacted]
DATE: 20/11/2020 00:21

I find it unnecessary to comment on the policy regarding privacy and security because it is reasonably constructed already.

The main issue comes from the blocking policies. Flipping DoH on by default is liable to lead to regimes that currently block content via DNS blocks to switch to an attack on TLS itself such as mandatory TLS interception because the DNS blocks aren't working anymore. We note that just leaving DoH off by default is likely enough to discourage such moves as someone who's looking for a bypass will surely find one and they must know this.

I suppose it's possible to arrange for it to be easy for such a power that wants to continue to use DNS blocks to be able to trip the enterprise checks, but from the description I have it doesn't appear designed to do so.

What we have here is kind of an uneasy truce and it's unwise to break it.

Disclaimer: I had to turn DoH off within hours of it turning on for me because it messed with internal resolving too much.