SUBJECT: Comment on DoH
FROM: V Parla <[redacted]
TO: [redacted]
DATE: 19/11/2020 20:36

Hi,

Regarding #5 in your list - 'opt-in' filtering.

DoH has resulted in substantial fragmentation of controls for Enterprises wishing to provide simple and effective DNS Security functions on their networks.

Previously, a network operator could provide DNS Security (my-network-my-rules model) to enforce enterprise policies. In some cases, such as the edu sector, these requirements are mandated.

DoH has changed the entire ecosystem where-in a network operator must also be a device manager (often this is not the case - think Guest Wifi). What this has resulted in is a situation where all well-known DoH servers are being blocked at the network level in a whack-a-mole approach. While some network mechanisms like canary domains exist today, they are not widely supported across vendor solutions (fragmentation) and don't inform the user clearly as to the outcome.

Even in cases where a network operator and a device owner are the same entity, the controls to enforce DoH policies across OSes, Browsers and Apps is entirely fragmented. There is no single 'Setting' to disable or configure DoH across these components that an ITA can use. As such they must have many settings to manage which could be solved by standardization of endpoint controls if vendors were able to collaborate on such a mechanism.

Similarly, end users are besieged with the same problems as an administrator. There is no single place to configure DoH settings for both the device, Browsers and apps. They are all fragmented an seperate. While in some cases, an App or Browser might use the OS resolver, the ability to override this makes it difficult for and results in a bad user.experience.

Two areas that could be improved at the ecosystem:
1) *Automatic Discovery at Network Join with a Mutual Agreement* - Where-in a Network Operator and a Device Owner can have a clear agreement to Use or Not User a Network if the Network-Advertised DoH/DNS service will not be enforced on the device.
Similar to a Captive Portal workflow, that exists today, for devices joining a network. When the two entities disagree on the required settings, a Network Connection would not continue and the user would be presented with an option to comply with the settings or not join.
This would solve most, if not all, of the use cases around Network Enforcement requirements, including Jurisdictional policies an ISP or Network Operator must enforce as well as all Enterprise use cases where the device owner and network operator are not the same entity.
It gives the user clear feedback and a choice to join the network and accept the network DoH / DNS settings - or alternatively an opportunity to opt out of using the network. As such it preserves choice and privacy for the user while solving network operator needs.

2) *Simplified and Unified Endpoint Configuration and Settings* that are system-wide and can be set in one place. This reduces the complexities and improves overall user experience for both the end user and a device administrator (enterprise) to set policies for DNS on the device and know that all components (including Browsers and Apps) will honor and respect those singular settings.