ERLEBEN, WAS VERBINDET.

DEUTSCHE TELEKOM AG
Postfach 20 00, 53113Bonn

Deutsche Telekom AG Response to the Mozilla Consultation on DNS over HTTPS Implementation

We welcome the opportunity to share the Deutsche Telekom AG view on questions in the context of DoH implementation. We fully support the position paper submitted by the European Telecommunications Network Operators' Association (ETNO) and wanted to provide our company answers to your specific questions as a complement to the association's position paper.

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?
>
> Deutsche Telekom AG has no requirements regarding the storage of user data. In our own DNS implementations, we do not store user data at all. In order to build trust, we recommend to not store user data at all.
>
> 2. What operational constraints, if any, are created by this maximum 24-hour retention time?
>
> We do not see any operational constraints here.

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).
We do not see emergency circumstances in the context of DNS resolution that could be resolved or mitigated by collecting additional data.

3. Our existing agreements stipulate that providers in our TRR program shall undergo third-party audits to confirm compliance with our TRR policies; are there particular criteria (e.g., auditor qualifications) or considerations (e.g., cost) that we should take under advisement?

N/A

4. Our current policy establishes that DoH resolvers in our program must maintain a transparency report providing public insight into the extent to which the resolver has been subject to government requests for data. How can this requirement be improved? What other mechanisms, processes, and governance tools may exist that could provide the public additional insight into such requests?

The current policy is perfectly acceptable.

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?

From the Deutsche Telekom perspective, the current policy does not require any changes regarding legally required blocking.

2. What harmful outcomes can arise from filtering/blocking through the DNS?

Given Net Neutrality rules and Open Internet policies, blocking and filtering is not allowed in the jurisdictions we operate in. Hence, blocking and filtering will not occur unless it is legally required. When a court orders the DNS blocking the effects are fully intended and should not be harmful to the general public.

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

There is a wide variety of client-based solutions when it comes to protecting users from illegal and harmful content, like malware and phishing.

4. How could we ensure effective transparency and accountability in situations where TRRs engage in legally required blocking practices? (For example: publicly available transparency reports with blocked domain names by country.)

> 1. What governance, process, or audit requirements should be required of parties that maintain and create block lists? For example, what complaint and redress processes should exist?
>
> N/A
>
> 2. What challenges weigh against a requirement to publish block lists?
>
> N/A

5. How can we best present information about opt-in filtering endpoints to end users (e.g., for malware blocking or family-friendly blocking)?

It would be great to first implement a visual indication in the browser, that Do Hist active. For example, an icon similar to the lock icon for encrypted websites. Once that is done adding variations that indicate active malware blocking etc. would be a sensible next step.

Building a better ecosystem

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

For Europe it is safe to say that encryption in general is likely to increase trust. Under the condition that it is implemented with full transparency and as long as the user is asked for explicit consent before changing existing setups.

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

N/A

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

To gain the support of Internet Service Providers it is all important to ensure that their own deployments of DoH are discovered and used by applications.

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)?

ISPs' networks in general have high standards in terms of security and privacy. In open networks (e.g. public unencrypted WiFi, Internet Cafes, Hotels etc.) DoH might add security/privacy. Nevertheless, this should be indicated by the application to the end users (for example with an icon, as described above). Otherwise we see the risk that the end user will make wrong assumptions about encrypted DNS communication, especially when applications fall back to unencrypted DNS.

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)?

Other examples include:

- DNS64/NAT64 in mobile networks
- DNS based load balancing mechanisms, e.g. for CDNs or other applications such as voice
- Redirection mechanisms in mobile networks to certain landing pages
- Zero-Rating plans on mobile networks