



**Mozilla Corporation**

331 East Evelyn Avenue  
Mountain View, CA 94041

## Questions for Comment

# Mozilla Comment Period on DNS-over-HTTPS Implementation

We are [seeking comments](#) in four areas. Firstly, we seek general feedback with respect to our TRR policy and its relation to different regions. We also seek to crowdsource helpful input in three specific areas related to product roll-out in new regions, which will help us maximise the security- and privacy-enhancing benefits of default-on DoH for more users.

### General comments regarding our TRR policies

DNS over HTTPS (DoH) brings the benefits of transport-level security to DNS queries and responses. Building on this foundation, Mozilla partners with selected DNS providers who join our Trusted Recursive Resolver (TRR) program to ensure even stronger privacy and security guarantees for Firefox users. This means that DoH look-ups in Firefox are routed to DNS providers who have made binding legal commitments to adopt extra protections for user data. Our [TRR policy](#) sets strict conditions regarding the handling of DNS data; in particular it establishes limits on data collection, use, and retention, limits on filtering and blocking without user consent, and transparency regarding data handling.

Consistent with the transparent practices and commitment to openness that Mozilla is known for, **we welcome general feedback on our TRR policy and its relevance for particular regions in different parts of the globe** - what benefits it may bring in terms of privacy and security, and what local considerations we should be conscious of in different regional contexts.

**Mozilla Corporation**

331 East Evelyn Avenue  
Mountain View, CA 94041

## Respecting privacy and security

We believe that privacy and security should never be optional on the Internet, and that as the developers of Firefox we have an important role to play in protecting our users from privacy and security risks. With that in mind, we have drafted our TRR policies with strict privacy requirements to minimize the potential that DNS data will be used for building user profiles.

**We are interested in feedback on these privacy requirements, whether they can be tightened further, and what if any operational constraints they create.**

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?
  2. What operational constraints, if any, are created by this maximum 24-hour retention time?
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).
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?
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?

**Mozilla Corporation**

331 East Evelyn Avenue  
Mountain View, CA 94041

## Online safety

Numerous ISPs today provide opt-in filtering control services, and our deployment of DoH is designed to respect those controls where users have opted into them. We take very seriously the challenges presented by the breath of malicious, harmful, and illegal content present across the web today (indeed, Firefox uses Google's Safe Browsing service to protect Firefox users from malware and phishing websites). At the same time, we do not consider broad filtering and blocking through the DNS to be an appropriate means for ensuring online safety, since it entails significant risks to fundamental rights and is easily circumventable.

With this in mind, we're interested in general feedback as to how **online safety goals can be met in ways that respect the technical architecture of the Internet and individuals' fundamental rights.**

More specifically, we welcome comments on the following technical questions related to 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?
2. What harmful outcomes can arise from filtering/blocking through the DNS?
3. What more rights-protective and technically effective means of protecting users from illegal and harmful content exist beyond DNS-based blocking?
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.)

**Mozilla Corporation**

331 East Evelyn Avenue  
Mountain View, CA 94041

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?
2. What challenges weigh against a requirement to publish block lists?
5. How can we best present information about opt-in filtering endpoints to end users (e.g., for malware blocking or family-friendly blocking)?

## Building a better ecosystem

Privacy and security issues differ across regions. As we seek to bring the protections of DoH to Firefox users in different regions, we're interested in general feedback as to **whether there are unique local considerations that we should be designing for in given jurisdictions.**

More specifically, we welcome comments on the following technical questions related to localisation:

1. How can deployment of DoH help to increase trust in Internet technologies in your region?
2. What exploitations of the DNS in your region could DoH protect against?
3. What are the best ways to gain global adoption/support of the DoH standard amongst ISPs and DNS providers?
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)?
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)?



**Mozilla Corporation**

331 East Evelyn Avenue  
Mountain View, CA 94041

## How to respond

All responses should be submitted in the form of an accessible pdf or via email to the following address before 4 January 2021:

[doh-comment-period-2020@mozilla.com](mailto:doh-comment-period-2020@mozilla.com)

**\*NOTE: All genuine responses will be made available publicly on this Open Policy & Advocacy blog. If you wish for your submission to remain confidential, please explicitly indicate when submitting your comments by email.**

Submissions that violate our [Community Participation Guidelines](#) will not be published.