> 1Questions for CommentMozilla CommentPeriod on DNS-over-HTTPS ImplementationWe
> are seeking commentsin four areas. Firstly, we seek general feedback
> with respect to our TRR policy and its relation to different regions. We also
> seek to crowdsource helpfulinput 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 policysets 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.

- The TRR concept is a good one. It'll be fine to tweak the policies as
experience is gained. The direction of movement should be towards more
transparency and less concentration. A mozilla declaration/pledge as to those
directions could be useful.

- I would very much prefer to see there being a range of TRRs, in my case
including some local to me in terms of jurisdiction (Ireland). Were I from a
different place (even within the EU!), I might likely prefer a TRR that is not
local in terms of jurisdiction, so this isn't a simple matter. It might be
possible to follow some recommendation from an objective, respected third party
as to the jurisdictions in which TRRs are best located. (Note: in this comment,
I'm talking about the jurisdiction according to whose rules the organisation
responsible for the TRR operates, and not the locale of a specific anycast
resolver instance.)

> 2Respecting privacy and securityWe 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

[redacted]

> 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?

- A short-term limit on high-granularity logging is good. I'm not much
concerned with that being 24 hours or a week.

- I can't conceive of an "emergency" that requires breaching the TRR
policy that wouldn't eviscerate the goals of the TRR poicy.

- Transparency reports are good, require those be more and more detailed.

- WRT transparency, consider working with an organisation that can be
the "best of breed" in transparency terms and publicising what has been
found to work well. (That would likely require finding a non-profit TRR,
maybe ask GEANT/Internet2 or a set of NRENs or IXPs or similar.)

> 3Online safetyNumerous 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, weâ€™re interested in general feedback as to
> howonline safety goals can be met in ways that respect the technical
> architecture of the Internet and individualsâ€™ fundamental rights.More
> specifically, we welcome comments on the following technical
> questions related to online safety:1.Our current policy states that
> theprovider 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.)

- Do not change the TRR policy to cater for net-nanny approaches, except where

the browser user has specifically opted-in to that. If you allow any form of opt-out net-nanny/censor, other than what is legally enforced in a fully open manner then the TRR concept will die sooner or later. By a "fully open manner" I mean a situation where a court case or similar has resulted in a block being mandated for some domain (e.g. pirate bay in various places) and where the list of such domains is public. Accepting secret block lists (as the UK govt might prefer) would not be acceptable as the default for a TRR IMO.

> 41.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
> ecosystemPrivacy and security issues differ across regions. As we seek
> to bring the protections of DoH to Firefox users in different regions, weâ€™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 arein place, are there
> other situations in which deployment of DoH might cause technical or
> operational challenges (e.g., mobile networks, NAT64 and DNS64)?

- Generally, I'd be against changes in this respect that make censorship easier or more effective. (Highly centralised control over a TRR also does that btw.)

> 5How to respondAll responses should be submitted in the form of an
> accessible pdf or via email to the following address before4 January
> 2021: [redacted] 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 Guidelineswill not be published.

It's fine to publish my comments.

[redacted]