Respecting privacy and security
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

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?

> The issue of auditing is very fundamental. However, the auditors shall have to be free from conflict of interest to ensure that the end-users' security decisions are respected. For instance, they shall not take advantage of access to TRR data to their advantage. At a bare minimum, the auditor shall be conversant with the operations of DNS and have working experience of security (i.e. usable security, cryptography, system security e.tc.)

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?

> Much as I agree to this policy, I feel that the end-users should be protected from malware and phishing attacks by default. Most of the users in Africa, regardless of their computing skills level, are not conversant with security configuration. These users could benefit from filtering at the TRR level.

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

> DNS filtering/blocking has got both disadvantages and advantages depending on where it is implemented. Recently we have witnessed DoH providers operating different instances of TRR performing various filters. This could be the right approach. Talking from the novice African Internet end-user's point of view, they could benefit from security filtering by default. There ought to be an easy-to-configure way for the ads and family filters to enable users opt-in (From the results of a user study we conducted in 35 African Countries). Making wholesale filtering may infringe the rights of some users. Also may not necessarily completely solve the problem; harmful content should be dealt with from the source, i.e. shutting down the server in question. DNS filtering/blocking may break several other good services originating from the same address raising human rights questions.

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

> The purest method of all is to eliminate the harmful content from the source. This is not a technical question only, but also a legal question. For example, laws that work in one jurisdiction may not work in another jurisdiction. International law on Internet governance is required to allow inter-jurisdiction dispute handling to deal with harmful content from the source.

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.)

> To ensure end-users are educated on cyberattacks and harmful domains online, It will be necessary for the TRR provider to provide transparency reports to their users. These reports will be in addition to Mozilla's efforts to publish transparency reports. These will, by and large, enable users to have insights on the dark side of the Internet and be able to defend themselves even when using unfiltered DNS provider.

4.2. What challenges weigh against a requirement to publish blocklists?

> I am pro publishing. However, care has to be taken to avoid blocking domains as a result of false positives.

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

> We recently conducted a user study to understand users' ability to configure security/privacy in browsers. The results show that even the tech-savvy do not know where the config tool is. One of the options to implement best opt-in would be having the config screen on the browser's home tab to enhance visibility. Another way could be nudging users at browser startup or other regular intervals. An educative nudge could help to reinforce cybersecurity culture. This is one of the questions my PhD research seeks to answer.

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?

> DoH deployment will reassure Intenet users of their privacy online and help them regain trust in Internet technologies. The only challenge in Africa is high latency caused by suboptimal routing and offshore hosting.

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

> In one of our user studies, users complained of unwanted ads and phishing pop-ups. DoH is better placed to counter these attacks.

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

> The best way is to enable DoH by default. Furthermore, TRRs should be replicated to increase resilience and trust. It is imperative to distribute TRRs towards the edges as well to improve Quality of Experience. We conducted measurements in Africa under 3G, 4G, Community network and campus networks. The result indicated more unsatisfactory performance (DNS response time and page load time) for DoH than for DoT under deteriorating network conditions. The closer TRRs are to the users, the lower the latency and the better the QoE. It would also be very useful if DoH configuration is integrated in the mobile Oss just like DoT. This way it could be easier since most of the Internet users nowadays use mobile devices.

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)?

> DoH has potential to protect users from various attacks under different Internet access networks. The only thing users are not comfortable with is the centralisation of 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)?

> Our measurements studies from South Africa indicate lowest DoH resolution success rates under a Community network which uses a captive portal to serve the Internet to the network users. We are still looking into possible causes for this. This is in comparison to DoT and regular measurements.