About ISPA

ISPA is the trade association for providers of internet services in the UK. ISPA has approximately 150 members, 90% of which are SMEs, as well as large multinational companies. We are proud to be an organisation which covers the whole Internet value chain, including companies that provide access, hosting and other online services. We represent the full ecosystem including communications providers that serve consumers and businesses, those that build their own networks and those that resell services via the fixed and wireless networks.

Introduction

ISPA welcomes the opportunity to respond to this public consultation on the Trusted Recursive Resolver (TRR) policy. We share Mozilla's aim that privacy and security should never be optional on the Internet but would go further and say that services should respect user choice and enhance online safety where possible. In liberal democracies, the implementation of DNS-over-HTTPS (DoH) and the drafting of policy documents such as the TRR should explicitly take account of and respect the wider ecosystem of general and specific legislation, as well as established user rights and expectations.[1]

DNS-over-HTTPS (DoH) is one of several standards in development which have a strong potential to enhance privacy but, if not implemented with care, risk undermining safety and security, and ignoring user choice.

With this in mind, we welcome efforts to mainstream DoH, but are concerned that:

- There are currently no agreed standards for DoH discovery;
- DNS resolution is being centralised within a smaller set of providers that are not necessarily subject to a user's domestic legal framework, and which will have greater visibility of global DNS records, thus potentially reducing privacy and undermining competition;
- For most non-technical users, using the Internet will become more complex than it is now; and
- There are several scenarios where current DoH rollout plans risk undermining rather than enhancing security, e.g. in many enterprise but also consumer environments.

Following a local upgrade path for DoH, where DNS resolution is switched over as soon as it becomes available from existing providers such as ISPs would help to mitigate some of these issues and our detailed response to the consultation questions is below.

Responding to the consultation questions

Respecting privacy and security

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

We are concerned that Mozilla's specific set of privacy features and requirements seems to take precedence over the privacy laws and regulations that apply in the jurisdiction from which a user accesses Mozilla's services.

[1] The response assumes rollout of DoH in liberal democracies and with established rule of law.

For example, the TRR does not explicitly commit to protecting the user's domestically guaranteed privacy rights such as rights to redress or grounds for processing.

Accordingly, we believe that Mozilla's TRR policy should explicitly require resolvers to respect the current and future privacy laws and regulations that apply to the jurisdiction from which the user accesses the services.

1.1 To what extent can our requirement be shortened further while allowing providers sufficient data to operate the service? & 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).

The TRR's data retention limits do not take account of the laws and regulations that apply to the jurisdiction from which a user accesses the service. This becomes particularly problematic where domestic law requires a longer retention period which precludes domestic providers from being considered as a TRR partner.

Furthermore, the explicit limitation to a 24-hour retention period undermines current customer service and security offerings by UK ISPs, as well as the anonymised use of DNS data for network capacity planning and content delivery.

The TRR remains silent on how these issues should be addressed and this becomes particularly relevant for non-technical users of Firefox who might not be aware that the mechanisms for DNS resolution have been changed. Those users are still likely to seek assistance for service issues from their local ISP which will no longer have the means to diagnose the relevant problems or answer relevant complaints for users of Firefox.

With this in mind, the TRR should:

- Explicitly allow partners to retain DNS data in line with domestic privacy laws, and including for purposes of providing customer support and cyber security services.
- Provide users with access to customer service support; this should include but is not limited to fault management (ticketing and inter-person handover/handoff, call/fault-resolution SLAs, and service quality reviews) in all languages spoken within the served territory.
- Support for fault-diagnosis and resolution between network provider, TRR and user, including customer data sharing, where required, and subject to the laws of the jurisdiction the user is based in.

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?

Costs of third-party audits are an important consideration and requiring extensive auditing could risk excluding smaller providers, including specialised UK ISPs, from becoming a TRR partner. As a result, there is a clear risk that third-party auditing requirements will lead to a further centralisation of DNS resolution.

There is also a question to what degree third-party auditing would deliver any meaningful benefits to users whose current providers already operate within the heavily regulated UK telecommunications and data protection framework.

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?

Any transparency requirements need to be compatible with domestic laws and regulations which can put in place reporting restrictions. Requiring a breach of UK regulations as a precondition to becoming a TRR partner would preclude domestic providers from applying and risk further centralising DNS resolution.

Online Safety

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.

A third consideration comes into play in this context – how can the rollout of DoH respect pre-existing choices that users have made regarding cyber security or online safety. For example, most UK Internet users have the option of using network-level tools that are offered by their ISP and can be configured to filter certain types of content or protect against malware or other threats.

Decisions about this are made by the account holder, e.g. a parent, and apply to all devices that are connected to that account, e.g. those used by children in the household. While all filtering solutions can be circumvented, it would be entirely reasonable for a parent to assume that simply using Firefox should not enable a child to negate the online safety and security settings that have been set for the household as a whole.

It is for that reason that we believe it is necessary that Firefox respects pre-existing user preferences and that changes to the DNS settings should be made by a person that can express the necessary consent, e.g. by the account holder. This would require providing clear and meaningful information to the user before DNS services are switched over, including an outline of the changes in plain English alongside case studies for how a typical home and small-business setup would be affected. These types of users typically do not currently engage with DNS and it is important that they make informed choices and are made aware of the consequences of enabling DoH.

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?

Many UK ISPs are members of the Internet Watch Foundation (IWF) and implement the IWF's watch list. This is not a legal requirement but the voluntary model underpinning this has built up and evolved over a 20-year period. We strongly believe that the TRR needs to take greater account of any domestic legal and regulatory frameworks, which in some instances can find expression in non-legislative conventions such as the IWF.

The UK also has an established non-legislative framework around providing parental control choices and this again should be more explicitly supported in the TRR policy for UK users.

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?
As with all types of blocking and filtering, there is the risk of over- (and under-) blocking. However, blocking at DNS-level can offer higher privacy standards than other mechanisms such as deep packet inspection. This privacy trade-off becomes particularly relevant if future regulatory or legal blocking requirements start mandating those more intrusive mechanisms in response to technical developments such as DoH.

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.)
&
4.2 What challenges weigh against a requirement to publish block lists?
Outside of court-based blocking orders, TRRs should outline the categories of content that might be blocked and, if a third-party service is used, TRR partners should also indicate this to their users. There should also be a point of contact to field queries regarding blocking or filtering decisions. However, we do not believe that it is feasible to require TRR to publish a list of blocked domains, especially if the content that is hosted on those domains is clearly illegal.

5. How can we best present information about opt-in filtering endpoints to end users (e.g., for malware blocking or family-friendly blocking)?
This should consider pre-existing decisions made at either device or account-level (e.g. flag existence and impact on ISP network-level control options) and ensure that decisions are made by a user that has sufficient competence (ideally the account holder or at least a person of the required legal age to make the relevant decisions).

Building a better eco system

1. How can deployment of DoH help to increase trust in Internet technologies in your region?
The best way to ensure that trust is enhanced through the deployment of DoH is by ensuring that the rollout is conscious of the established domestic laws, guidelines, norms, and customs that UK users expect to be met when they use the Internet.

2. What exploitations of the DNS in your region could DoH protect against?
EU and UK data protection standards and regulations provide strong safeguards, and we are not aware of ISPs exploiting DNS for commercial reasons such as advertising.

DNS can be exploited by malicious third-party actors but DoH, if not implemented carefully, risks increasing the potential for such malicious exploitation, especially in enterprise and small business contexts where account holders or managers might not be aware that existing network protection mechanisms might not be compatible with DoH.

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

We would strongly support a multilateral deployment process that is based on a universal standard for discovery and that preserves a decentralised model of DNS resolution.

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)?

Changing the provider of DNS resolution can cause many challenges, including DNS64 as you note. Furthermore, enterprises expect to be involved in the DNS resolution process to provide some security against attack, but we would strongly emphasise that the need for such security is not unique to enterprises. Home users also need security, and the need for this will grow over time as IoT devices proliferate. Accordingly, the challenge is to ensure that the upgrade to DoH does not involve a change of provider, or if it does, that the change in provider does not involve a weakening of any aspect of security.