20.01.2021

Nominet response to Mozilla DNS over HTTPS (DoH) Comment Period

This is Nominet's response to Mozilla's call for comment on its proposed rollout of DNS over HTTPS (DoH) beyond the United States.

Nominet, responsible for running the UK's country code top level domain (ccTLD) takes a considerable interest in these discussions, and ensuring the best outcomes are secured for all internet citizens. For over twenty years Nominet has been working to maintain the relevance, stability, security, and safety of the .UK domain. We keep pace with criminal abuse, stay ahead of trends and ensure everyone understands the benefits of being part of the UK's namespace.

Responsible adoption of DoH technologies can be compatible with all these objectives, while bolstering the privacy of end users.

However, there are questions as to how Mozilla and others can implement these in a way that includes users, while ensuring online safety and privacy. The most significant of these relate to who would be recognised as trusted resolvers and on what basis. Our response sets out four main principles we ask Mozilla to place at the heart of any global deployment of DoH and recognition of Trusted Recursive Resolver (TRR).

These are each set out in turn below.

1. Users should be able to make informed choices

Mozilla must place user safety and choice at the heart of DoH deployment. This means users must a have clear and informed choice to either enable to disable DoH. While we acknowledge that the proposed 'default on' model will invite the user to make a choice, we do have three concerns as to how users will interact with this in practice:

i. It is crucial that DoH is not simply turned on by default. The implications of DoH are significant for a user's data and privacy on the web at large, and users should have informed choice about where their data is routed. A 'default-on' recommendation discourages users from properly engaging with the question and obfuscates the many reasons a user might prefer not to use DoH if informed.

ii. On a similar note, it is essential changes are widely understood by users opting into them. Nominet has produced explainers to this effect, and more widely there needs to be information in clear, simple and impartial language at the point the user makes a choice.

iii. This also requires a consistent user experience. We would welcome greater collaboration and standardisation between browser providers in order that impartial information on DoH genuinely accessible. Using standardised terminology and user interface presentation of choices will ensure a level playing field so users can make informed choices, regardless of provider.

These will be critical to establishing user trust. We also have concerns regarding linkability between DoH HTTPS sessions, and whether this may enable user tracking. We would ask Mozilla for greater clarity around how long an HTTPS session would persist - and therefore be able to link a particular user and application.

2. DoH rollout must ensure equal or improved online safety

Some of the internet safety and security measures that have been built over the years involve the DNS. Parental controls, for example, generally rely on the ISP blocking domains for their end users. The Internet Watch Foundation (IWF) also ask ISPs to block certain domains because they are hosting child sexual abuse material. The basis for these practices exits not only through the policies of ISPs, but through local laws and regulations. We believe that DoH, if implemented responsibly, can be compatible with all of these.

However, Mozilla must place these obligations to the security and safety of end users front and centre in approving an TRR. We would welcome clarification from Mozilla on what basis it will approve TRRs and if support for this level of filtering would be included in the criteria. To note as well, publishing filtering lists – in many jurisdictions – is likely to prove unlawful for some content and have unintended consequences (for example providing a directory for those seeking out unlawful content).

3. Local jurisdiction and accountability

Mozilla should also clarify by what means it will ensure compliance with local Law Enforcement Agencies (LEAs) can be met with confidence by approved TRRs. The rollout of DoH in the UK and the rest of Europe will also raise several issues related to General Data Protection Regulation (GDPR). Nominet believes a one-size-fits-all approach to these challenges is unlikely to work.

Our preference would be for Mozilla to recognise a local TRR located within the UK, that can be genuinely subject to UK laws and GDPR. Doing so will ensure confidence and accountability for UK citizens for the rights they have under law. We believe this will be essential to long-term confidence in DoH in general and securing Mozilla's own objectives for user trust and privacy.

There is need for greater maturity in the TRR landscape to support safe adoption of DoH. Today, there is a possibility that large volumes of traffic could be centralised into just a few components of recursive infrastructure. This has implications for resilience, and we would urge Mozilla to assess prospective TRRs on the basis of genuine transparency and accountability, while also ensuring choice rather than further consoldation.

We would also ask Mozilla to clarify by what means it would address any misconduct on the part of a TRR, as we believe this is unclear as proposed. While we welcome Mozilla's proposal for third-party audit

in principle, we also ask for clarity as to how an auditor would be chosen, and paid, and whether their findings would be made public.

4. Security controls in enterprise and public services

Nominet is also concerned about potential implications for cyber security in enterprise settings. Many organisations currently use the DNS to secure their networks, by blocking domains known to contain malware. All these measures could be undermined by a flawed introduction of DoH. We would therefore welcome Mozilla's comment on what measures it can take to allow organisations to properly configure use of DOH in their workplaces and work devices.

Annex 1 - Nominet response to specific questions

1. General comments regarding our TRR policies
On Mozilla's proposed Blocking & Modification Prohibitions, Mozilla must also recognise resolvers that offer the ability to block or filter where appropriate. A user or administrator of a device should have a full and wide choice as to the protocol and resolution service they choose to select or use. The approach taken to recommended providers is currently based on an assessment criterion that is limiting choice and is to the exclusion of resolution service providers that may offer alternative TTR with regards to criteria a user deems trusted. This is not providing consumers with clear and open informed choice. In addition, many current security controls, or postures that maybe in place could well be weakened with the current approach as documented. We also note that publishing documentation to include all blocked domains is not a viable or supportable approach. This would be the case for a number of the more illicit categories including IWF lists regarding filtering of child sexual abuse material online. The exclusion of filtered DoH DNS service providers is not providing consumers with an informed and open choice. In addition, many current security controls or security postures in place may well be weakened with the current approach as documented

2. 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. i. To what extent can our requirement be shortened further while allowing providers sufficient data to operate the service? ii. What operational constraints, if any, are created by this maximum 24-hour retention time?	The 24 hour retention requirement will restrict DNS providers ability to provide cyber security and filtering, as we do not believe this time period is sufficient to identify malware in a great many cases.
2. Are there exemptions that should be allowed by the policy for additional data collection in emergency circumstances? Please specify (e.g., the relevant	N/A

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?	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?	N/A

3. 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?	N/A
2. What harmful outcomes can arise from filtering/blocking through the DNS?	N/A
3. What more rights-protective and technically effective means of protecting users from illegal and harmful content exist beyond DNS based blocking?	N/A
4. How could we ensure effective transparency and accountability in	We also note that publishing documentation to include all blocked

situations where TRRs engage in legally required blocking practices? (For example: publicly available transparency reports with blocked domain names by country.) i. 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? ii. What challenges weigh against a requirement to publish block lists?	domains is not a viable or supportable approach. This would be the case for a number of the more illicit categories including IWF lists regarding filtering of child sexual abuse material online.
5. How can we best present information about opt-in filtering endpoints to end users (e.g., for malware blocking or family-friendly blocking)?	N/A

4. Building a better ecosystem	
1. How can deployment of DoH help to increase trust in Internet technologies in your region?	DoH offers increased privacy for end devices regarding network and MITM visibility of DNS lookups and responses. A clear and informed choice in use of DoH resolution, and in the selection of the server/provider, will help in achieving a level of trust. Trust is directly aligned with who the end device owner chooses to select with knowing the details of the requesting end device seeking resolution.
2. What exploitations of the DNS in your region could DoH protect against?	DoH can provide improved protection from MITM attacks and malicious snooping. It reduces visibility of DNS on the network and outside of the client and the selected end resolver. DoH however also provides an attack surface for exploitation with potential to

	bypass many current deployed security controls. Exploitations already observed include C2 and malware that has taken advantage of the increased privacy offered and inability to easily detect and block its use. This brings challenges and potential increased infrastructure and overhead costs for achieving or retaining visibility and management of DNS resolution.
3. What are the best ways to gain global adoption/support of the DoH standard amongst ISPs and DNS providers?	This can be delivered through a consistent and clear end device user experience. Greater collaboration and standardisation between OS, browser providers and DoH service providers, so information on DoH is genuinely accessible. Using standardised terminology and presentation of choices will ensure a level playing field so users can make informed choices, regardless of provider.
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 offers increased privacy for end devices regarding network and MITM visibility of DNS lookups and responses. DoH though also offers the potential to bypass security controls put in place.
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)?	Where DNS translations may be being deployed or where infrastructure is not capable of supporting DOH. In addition, where current security controls and monitoring including DNS Filtering are in place and are then potentially bypassed. This may also result in increased overhead for recursive DNS provider infrastructure.