Mozilla Comment Period on DNS-over-HTTPS Implementation

General comments regarding:

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.

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

    Opt-in policy could be made available for both providers willing to hold data shorter than 24h, as well as for users requesting the same. This opt-in should be highlighted as an extra step accomplished by committed providers in their efforts for preserving user privacy, so as to make users aware of their better-than-average commitment without further restricting providers complying with the existing 24h retention policy.

    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).

    In case a user, I.e a corporate client, requests their DNS data to remain available for logs,audits, or analysis, or if explicitly requested by law-enforcement under the appropriate procedures and channels, a clearly written notice should be made publicly-available for those affected by this request, to enable them to pursue action as necessary.

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?

Particular criteria that must be added includes detailed Human Rights Impact assessments (HRIAs); the main reason for this sea of change is to ensure end-users and their data are protected. This cannot be fully accomplished if we fail to address the impact our organizations, technologies, and policies have in the human and digital rights we directly or indirectly protect or hinder. Third-party audits should, therefore, include a human and digital rights considerations section, transparency and accountability mechanisms for public scrutiny of the results as well as the employed audit methods, and undoubtedly, feedback cycles for both the provider to implement recommendations and for the auditors to refine their methods. Auditors should be impartial, with good knowledge of the background and technical area, a proven interest in helping build a better internet for all, and with a focus on feedback and transparency rather than costs.

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?

    Including this report as a section to be analised by third parties conducting HRIAs will improve the accountability and trust that can be built among different parties. This will increase visibility of the findings as well.

Online safety

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?

    Since the regulatory framework defaults to the location of the main DNS provider (controller of data) under the GDPR, and the CCPA is so far only concerned with the origin and destination of the encrypted data, without regards for the middle hops forwarding said encrypted data, ensuring compliance with RFC8914 on extended DNS errors would help address this question, and at the same time, it's an important step towards better transparency in the policy. Support for ongoing work, such as draft-reddy-dnsop-error-page which aims at targeting the DNS error information to the end-users as opposed to the operators and system administrators as is the case in RFC8914, is likewise important; even though the hops or middle connections between the resolver location and the location of the end-user add increased complexity, informed user choice over the content the end-users are having access to (or not), is a must; they must clearly know when illegal content is being blocked, and they must be assured that only illegal content is, in fact, being filtered based on their jurisdiction.

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

    Thinking of Freedom of Expression as defined in Article 19 of the ICCPR (International Covenant on Civil and Political Rights) regarding expression, opinion, and access to information, different types of censorship and blocking may impact a person's ability to express themselves while not affecting their ability to receive information, or the other way around, or limit both their Freedom of access to Information (FoI) and their Freedom of Expression (FoE) at the same time. This is why censorship, blocking, and filtering, remain a key issue concerning DNS and FoE/FoI; regulating bodies have employed different techniques over the years in order to filter, control, and regulate Internet traffic through the DNS, to profile and target specific sectors of the population, and to manipulate the content they have access to. These heavy oppressions are held in place through manipulation of unencrypted DNS data; pervasive surveillance, tracking, cross-referencing, profiling, are all further enabled through practices of blocking content without regulation, and fed with information gained through DNS filtering and inspection.

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

    There must be a distinction between 'illegal' and 'harmful' content. To preserve users' rights, providers must only concern themselves with the content which is Illegal. The impact of harmful content is tied to the users' right to seek it and express it, for which society as a whole must find ways to address the actions and behaviors that lead to such harmful content; thinking of child protection and related content, DNS based measures are not enough, nor will they ever be enough, as long as the conditions that enable the creation of related harmful content continue to be unregulated, and DNS filtering has already been proven as an insufficient approach since the problem's scope is well beyond DNS and what can be achieved through its control.

    Technical means need a strong legal framework that allows an efficient approach by Law Enforcement without hindering the rights of the population.

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.)

    Approaching CSOs will prove useful in this regard. A group such as IFF's DNS [1] could provide a platform for such discussion and modeling of documents/requirements.

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

A 2-layer approach can be recommending; starting with leaflets/discussions/information-materials prior to rolling out opt-in filtering options, followed by informed user choice in the settings through clear and concise wording. This can be aided by optional GUIs for better user experience.

Building a better ecosystem

1. How can deployment of DoH help to increase trust in Internet technologies in your region?

Jurisdictions lacking end-user protections can benefit greatly from DoH; in locations where monetisation of DNS data (without user knowledge or consent) has been the norm, the encryption of DNS data provides a strong base for increased transparency and accountability. The competition that this implies helps build a healthier ecosystem than we currently have; users now have a point of pressure to expect and demand better services from their local providers, with the option of using global/remote providers if their expectations are not met.

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

In my region, profiling users for the sake of filtering their content and/or stifling their dissent, has not been in practice.

However, DNS inspection for tracking and cross-referencing is heavily used; the current president (Costa Rica) was found last year to keep a large database of citizens' confidential data [2]. It is unclear yet the methods used for the data capture, but DNS encryption is likely to protect against similar initiatives in the future.

Monetization of users' data is prevalent in the region, which is thought to be linked to zero-rated access to content [3] and the success of certain applications/services in establishing market dominance through such regional programs.

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

Publicly addressing some of the most pressing concerns will help towards building trust and partnerships. A specific concern is that of Centralisation, and the power shift happening when the DNS data control moves from local providers to global providers. This can be addressed through:

- Initiatives to help local/smaller providers to implement and deploy their own encrypted services.
- Joint panels/discussions with service providers where their concerns are discussed, for example: support provided in the local language to customers that are now also using a global provider, for which the local ISP/provider retains ownership of their accounts and responsibility for their satisfaction.
- Initiatives to help educate the users on how their data has been exploited and how encrypted DNS helps against it.

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 will likely be overriden through captive portals and/or vpn connections. Informed user choice and consent are key in these scenarios.

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)?

> The current lack of sufficient test data on DoH deployments, specifically regarding performance, has a direct impact on the ability that many providers have in deploying DoH, either through global providers, or through their own implementations. Mozilla's support in this regard would help alleviate this specific challenge.

I hereby explicitly agree to the responses in this file being made available publicly on Mozilla's blog if necessary.

Joey Salazar
Digital Sr. Programme Officer
ARTICLE 19

[1]https://lists.ghserv.net/mailman/listinfo/dns
[2]https://cnnespanol.cnn.com/2020/02/28/alerta-costa-rica-fiscalia-de-costa-rica-investiga-al-presidente-alvarado-por-supuesto-uso-indebido-de-datos/
[3]https://www.telesemana.com/blog/2017/04/28/un-mes-despues-que-claro-movistar-aplica-zero-rating-en-costa-rica/