Status: 2021-01-17

ISPCP Comment on Mozilla DoH questions

This response is based on the ICANN ISPCP (Internet Service Providers and Connectivity Providers Constituency) May 2020 policy paper. The paper was developed prior to Mozilla's consultation. This paper reproduces the full questions of the "**Mozilla Comment Period on DNS-over-HTTPS Implementation"** and wherever appropriate offers a tentative mapping onto the elements developed in the ICANN ISPCP policy paper, or notes that "The ISPCP policy paper did not address this question" otherwise. Other elements are developed in the paper which can be found at https://www.ispcp.info/assets/docs/PolicyStatements/2020_PolicyStatements/2020_05%20May%20DoH%20statement%20clean%20v2.0.pdf

Mozilla Comment Period on DNS-over-HTTPS Implementation

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.
   - 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?
   - ➢ **The ISPCP policy paper did not address this question.**

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 ISPCP policy paper did not address this question.**

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 ISPCP policy paper did not address this question.**

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?

   ➢ **The ISPCP policy paper did not address this question.**

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

- **The models of deployments for the protocol have generated concerns notably on the impact for DNS resolvers provided by ISPs [ETNO, Open-xchange, CENTR, Centralized DNS over HTTPS (DoH) Implementation Issues and Risks, DoH Considerations for Operator Networks (https://datatracker.ietf.org/doc/draft-livingood-doh-implementation-risks-issues/)]. Concerns are mostly related to**
    - **the consequences of the joint use of DoH and public resolvers**
    - **and in particular the fact that some deployments of DoH may be used to enforce a change in browser's settings to use an alternative resolver to the currently defined (unencrypted) DNS resolver**

  In particular, the following consequences have been documented by ISPs and are largely described in the papers referenced above:

    - **technical impacts: CDN selection, DNS query logging, load balancing, DNS-based address mapping for IPv4/IPv6 coexistence, joint use of NAT and stub resolvers, malware detection, enterprise/split DNS**
    - **Regulatory and Policy Considerations: administrative block-lists of domain names associated with hate speech or child pornography, parental control, data privacy**

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

- **The ISPCP policy paper did not address this question.**

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.)
    a. 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?
    b. 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)?

- **The ISPCP policy paper did not address these questions.**

Building a better ecosystem

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

- **The ISPCP policy paper did not address this question.**

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

- **The ISPCP policy paper did not address this question.**

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

- **Regarding the policy that determines the choice of the DNS resolver, the ISPCP supports the approach that the upgrade to DoH should not change the user's DNS resolver choice, i.e.:**
    - **-selection policy**
        - **use DoH when it is available on the DNS resolver configured in the browser/Operating System**
        - **remain unencrypted if DoH is not available on this resolver –unless the user has explicitly chosen to do otherwise**
            - **in particular not redirect user DNS traffic to a DoH compliant resolver owned by/partnered with the browser/OS maker by changing the user's DNS resolver provider**
    - **maintain/define a long term mechanism to opt-out of DoH deployment (e.g.,"canary domain name")**

  The rationale is the following:-A well-functioning DNS resolver is a condition for Internet connectivity:

    - **ISPs have direct relationship with their customers who would turn to the ISP support if Internet access –the above maintain some control from the ISP**
    - **ISPs are evaluated (or have regulatory constraints) on access to content conditioned by the performance of their DNS resolvers**

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)?

- **The ISPCP policy paper did not address this question.**

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)?

- **See Question 2.**