SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Mozilla Corporation
331 East Evelyn Avenue
Mountain View, CA 94041
Via e-mail to:
[redacted]

SWITCH-CERT
[redacted]
E-mail: [redacted]

Zurich, 20. January 2021

Comments on Mozilla's Comment Period on DNS-over-HTTPS Implementation

Dear Mozilla Corporation

SWITCH is a Swiss not for profit foundation that runs the Swiss National Research and Education Network (NREN). In the context of the questions for comment, we act as a Network Operator, as the DNS competence center for Switzerland, as a national CSIRT, as an operator of a recursive resolver and as a Managed Security Provider (MSP) providing RPZ feeds and DNS monitoring services to our customers.

SWITCH welcomes the continuous improvements in DNS security and privacy through new standards. We appreciate the efforts of the Mozilla Corporation to build a better ecosystem with more online security and privacy for Internet users. But we also see some difficult challenges in the implementation of these new security and privacy standards. That's why we want to support this implementation through our comments on Mozilla's "Questions for Comment" on DNS-over-HTTPS Implementation. (https://blog.mozilla.org/netpolicy/files/2020/11/DoH-Public-Comment-Period-Question-for-Comment.pdf.pdf)

General comments regarding Mozilla's TRR Policies

Comment SWITCH-CERT:

We welcome Mozilla's TRR policy requirements and strict conditions regarding the handling of DNS data. One thing to keep in mind is that Internet access providers, that traditionally operate recursive DNS servers in Switzerland are regulated by federal laws, in particular the Telecommunications Act (FMG and FDV Art 80) and are restricted in their use of traffic information. Operators of recursive resolvers that are not Internet access providers are not subject to regulation by the FMG and FDV. So any efforts that shift users from ISP run resolvers to cloud based resolvers, should take into account a compensation for the loss of regulation and data protection.

Respecting privacy and security

Question 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?

2. What operational constraints, if any, are created by this maximum 24-hour retention time?

Comment SWITCH-CERT: no comments

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).

Comment SWITCH-CERT: no comments

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?

Comment SWITCH-CERT: no comments

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?

Comment SWITCH-CERT: no comments

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?

Comment SWITCH-CERT:

Switzerland has a network neutrality law. For Internet access providers, domain name blocking is legal for domains that are on a list of a national agency authorized

by law, to protect infrastructure or with the consent of the user. Blocking domains that are legally required to block by another jurisdiction, but not by Swiss law, would conflict with the required net neutrality in Switzerland.

Some Swiss ISPs block by default domain name resolution for known malicious domain names (e.g. malware, phishing) on their ISP DNS resolvers. One of the reasons is that it reduces the number of ISP helpdesk calls because end customer computers work better (e.g. less malware infections). This reduces the overall costs for the ISP. Taking away the DNS and in this case, the control plane, will increase helpdesk calls and the cost of providing ISP services. Mozilla should either allow these ISPs to demand a blocking resolver for their users or Mozilla should provide a mechanism so that ISPs can opt-out their end users from using a TRR.

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

Comment SWITCH-CERT:

Overblocking is a risk, that can be managed with a quick response from DNS resolver operators, if they can set and correct the policy themselves.

We see a general risk, that users do not agree to filtering/blocking by their ISP and change their resolver. This may result in a loss of protection from filtering and other security and privacy features.

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

Comment SWITCH-CERT:

Blocking harmful content directly in the browser or the operating system is a good complement, but not a substitute for filtering harmful content on the DNS level by network operators. DNS filtering with RPZ allows a near real-time response to specific and local threats that are unlikely to be integrated in the global safe browsing list.

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.)

Comment SWITCH-CERT:

Transparency is the key acceptance of any filtering/blocking. Users currently cannot see what filters are in place by their DNS resolver. Mozilla should work towards a standardization to make DNS filtering transparent and, if possible, display that information in the browser.

4 1. 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?

Comment SWITCH-CERT:

For non-legal mandatory blocking it should be visible to the user that the domain name is blocked by his DNS resolver and why. It should be easy to request a review and TRRs should regularly report the number of complaints and actions taken to the public.

4.2. What challenges weigh against a requirement to publish block lists?

Comment SWITCH-CERT:

Whenever it is possible to show whether and why a domain name is blocked, this should be published. However, publishing the filter/block lists in full and in real time is subject to operational and legal constraints. Some of the reasons are:

- National law doesn't allow the publication of CA or other blocklists
- Agreements with commercial feed providers don't allow the publication of the threat intel information
- Publishing block lists for specific threats would give threat actors the possibility to see in real time, what detection mechanisms are in place and how effective they are. This could weaken the defense against phishing, malware and other threats that require a timely response.

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

Comment SWITCH-CERT:

Users should see, and be able to understand the effects of any opt-in and lawful blocking.

Building a better ecosystem

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

Comment SWITCH-CERT:

A secure and private DNS resolution is essential for trust in the Internet. Unfortunately, DNS resolution is not visible to most end users and DoH doesn't resolve all of the issues of the DNS. More visibility and promotion of secure DNS standards are needed.

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

Comment SWITCH-CERT:

For Switzerland, we see a risk in the use of public WIFI networks. The usage exposes user's unencrypted DNS traffic to eavesdropping and DNS hijacking. DoH can help protect against this.

So far, the availability of DoH hasn't stopped the implementation of mandatory lawful filtering. The use of alternative resolvers that don't have to implement Switzerland's lawful filtering via DoH is a possibility for users to access services that are not licensed in Switzerland.

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

Comment SWITCH-CERT:

Awareness regarding the risks of unencrypted DNS and promotion of encrypted DNS standards are essential. Visibility to the end user of DNS security features used in the browser could help increase demand.

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)?

Comment SWITCH-CERT: no comments

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)?

Comment SWITCH-CERT:

Browsers should bypass the system stub resolver and send DNS requests directly via DoH to the resolver configured in the operating system, only if they detect that the resolver offers DoH and the operating system doesn't use DoH or DoT or another encrypted channel for DNS resolving.

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

The Swiss NREN is a heterogenous network, recursive DNS resolvers are operated by the universities, departments and research projects. As network operator it is not possible to signal that enterprise policies are in place. We therefore urge Mozilla to respect the choice of the network operator, university or user regarding the recursive DNS resolver. Changes to the resolver, other than a protocol upgrade to DoH, must not be done without the explicit consent of the user or network operator.

The DNS resolution path was not subject of instability, configuration errors and other issues from the WebPKI. Encrypted DNS based on TLS will increase the number of potential issues and reduce the availability for end users.

Thank you for the consideration,
kind regards

SWITCH-CERT