PROSTASIA
FOUNDATION

Prostasia Foundation
18 Bartol Street, #995
San Francisco, CA 94133

info@prost.asia
Ofc:+1 415 650 2557
Mbl:+1 510 480 8449
https://prost.asia

DNS over HTTPS implementation

November 28, 2020

Thank you for the opportunity to comment on Mozilla's plans for the implementation of the DNS over HTTPS (DoH) standard.

Prostasia Foundation is a child protection organization that aims to ensure that the laws and policies that our society adopts to combat child sexual abuse are evidence-based and compliant with international human rights norms. As such, we have an interest in the implementation of DoH, since one of the most common objections to the implementation of this standard is that it will interfere with DNS-based blocking regimes for unlawful sexual images of minors (aka. child sexual abuse material or CSAM).

We disagree with these objections, and support the implementation of DoH as a way to improve the security and privacy of the Internet's infrastructure for all its users, including children. We believe that DNS blocking is not well adapted to the fight against CSAM online, because it is so easily circumvented and because it risks being both over-inclusive and under-inclusive. We set out our position in more detail in a joint submission with Article 19 from August 2019.

Here we respond more specifically to some of the consultation questions posed by Mozilla in the "Online safety" section of the consultation document.

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?*

It should not change. If blocking is legally required in a jurisdiction in which a given resolver operates, but not in other jurisdictions, then this is a question of is for those jurisdictions to sort out between themselves. If an international regime for the legal DNS blocking of websites is to be developed, then it should be developed by an international multi-stakeholder institution.

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

DNS based blocking is easy to circumvent, and it is not granular enough to effectively block content such as child abuse images. Isolated child abuse images are often found on image hosting websites that are intended only for lawful content, and these cannot be targeted with DNS blocking without causing over-censorship. Although it was one the case that entire websites were devoted to child abuse material, these have largely been driven off the clear web. In rare cases when such websites are still found, their removal at source by law enforcement should be prioritized.

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

Although it is a difficult pill to swallow, the simple fact is that censorship has failed as a solution to the dissemination of child sexual abuse material. This is because is it impossible to both uphold human rights online, and also to completely foreclose the technical possibility of child abuse images being sent over private communications channels.

It must be understood that child sexual abuse is not a technical problem, but a human one. Therefore, to make headway we need to place much more emphasis on the prevention of child sexual abuse before it is perpetrated, using an evidence-based, public health approach. Prostasia Foundation works with platforms and with leading experts in the field of child sexual abuse prevention to design interventions for prevention and early intervention that are based on these principles.

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.)*

    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?*

The Internet Watch Foundation (IWF) provides a good model, with a fairly robust system of accountability, audit, and review that includes an independent inspection of its hotline every two years by a team of law enforcement, forensic and academic professionals led by a retired High Court Judge. The international association of child abuse reporting hotlines, INHOPE, also audits its members, however we have concerns about INHOPE's audit process. In particular, INHOPE allows its members to include cartoon images on their child abuse blocklists, which we believe to be inappropriate.

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

The commonly expressed concern is that if a list of websites containing child abuse images is published, this may be misused for obvious illicit purposes. However, a block list itself contains no illegal material. As a compromise between full transparency and the (current) system of completely secrecy, it would be possible for such lists to be published, but for access to be restricted to those who can demonstrate a legitimate research, law enforcement, or other professional interest.

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 directory of opt-in filtering endpoints, with associated public information about each, should be made available through a configuration wizard that would be displayed when DoH is first enabled in the user's browser.