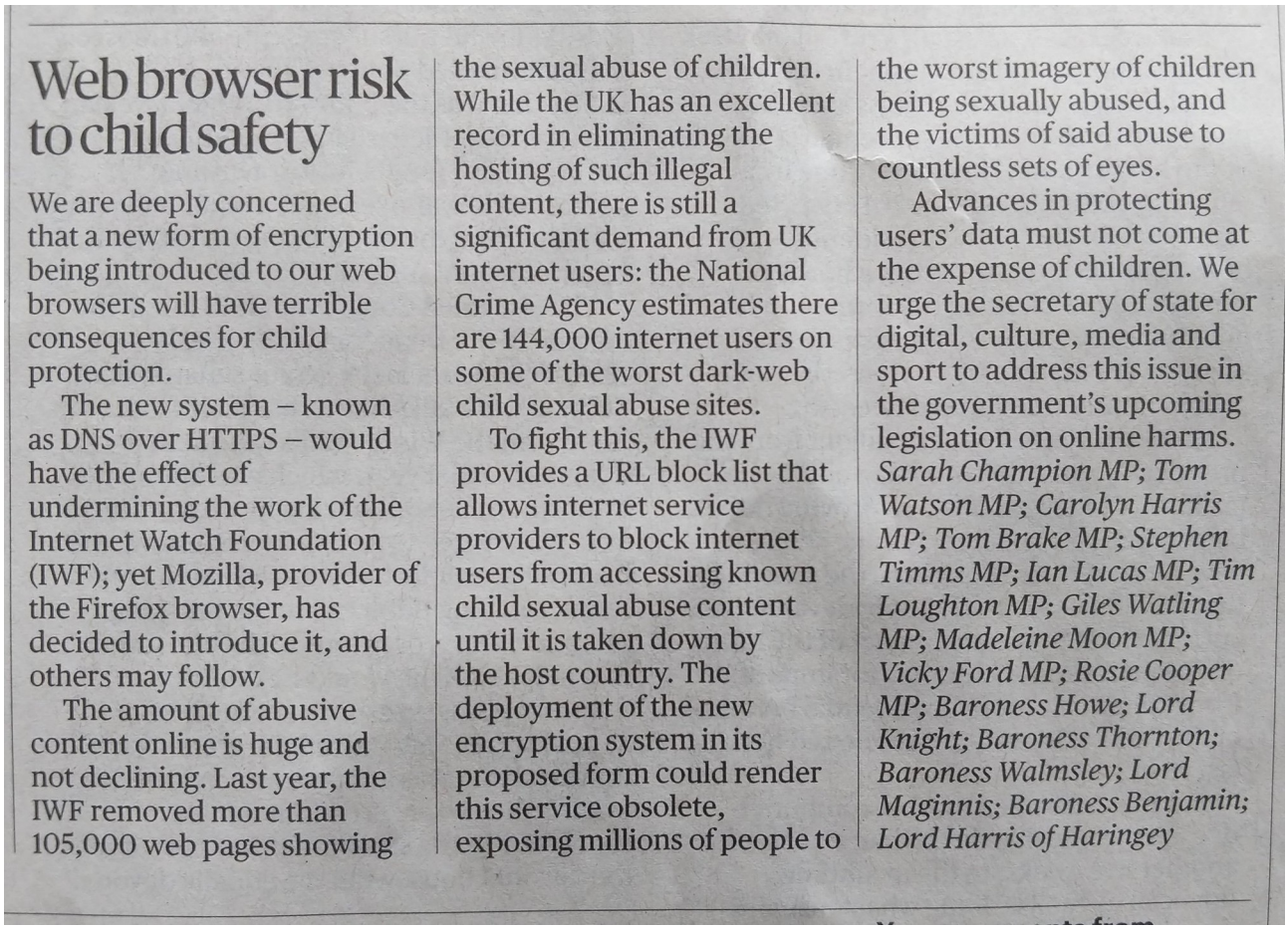
ORG Briefing for Mozilla: DNS over HTTPS comment period

January 2021

In June 2019, ORG published a paper, "DNS Security: Getting It Right", which laid out our recommendations for both policy and the technical rollout of DoH. We would like this paper[1] to act as the bulk of our submission.

While the paper remains current and accurate, the policy debate in the UK since its publication has tended to associate DoH with the online harms framework (see below image from August 2019).



Web browser risk to child safety

We are deeply concerned that a new form of encryption being introduced to our web browsers will have terrible consequences for child protection.

The new system – known as DNS over HTTPS – would have the effect of undermining the work of the Internet Watch Foundation (IWF); yet Mozilla, provider of the Firefox browser, has decided to introduce it, and others may follow.

The amount of abusive content online is huge and not declining. Last year, the IWF removed more than 105,000 web pages showing the sexual abuse of children. While the UK has an excellent record in eliminating the hosting of such illegal content, there is still a significant demand from UK internet users: the National Crime Agency estimates there are 144,000 internet users on some of the worst dark-web child sexual abuse sites.

To fight this, the IWF provides a URL block list that allows internet service providers to block internet users from accessing known child sexual abuse content until it is taken down by the host country. The deployment of the new encryption system in its proposed form could render this service obsolete, exposing millions of people to the worst imagery of children being sexually abused, and the victims of said abuse to countless sets of eyes.

Advances in protecting users' data must not come at the expense of children. We urge the secretary of state for digital, culture, media and sport to address this issue in the government's upcoming legislation on online harms.

Sarah Champion MP; Tom Watson MP; Carolyn Harris MP; Tom Brake MP; Stephen Timms MP; Ian Lucas MP; Tim Loughton MP; Giles Watling MP; Madeleine Moon MP; Vicky Ford MP; Rosie Cooper MP; Baroness Howe; Lord Knight; Baroness Thornton; Baroness Walmsley; Lord Maginnis; Baroness Benjamin; Lord Harris of Haringey

The full government response to the online harms white paper was released in December 2020[2] and did not explicitly discuss any technical aspects of the planned legislation. The paper did, however, state a commitment to continuing to work with multistakeholder initiatives on security-related issues. This may offer an opportunity for Mozilla, working with Open Rights Group, to engage with government in the future.

1 https://www.openrightsgroup.org/publications/dns-security-getting-it-right/

2 https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

We also respond to several of the questions presented in the consultation below.

B. Online Safety

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 is reasonable for a DoH provider to block according to national jurisdiction when that jurisdiction is law-abiding and has an accountable legal system. Where this is not present, blocking decisions may be egregious and to the detriment of people wishing to use DoH. DoH providers should be based in countries with a functioning and high level of legal accountability.

Likewise, application of national blocking policies should only ever follow a similar test by DoH providers. Currently, we are unaware that any national jurisdiction has required DNS blocking by DNS providers. If a country does, this should be considered in the light of that country's human rights record.

Mozilla should offer DoH providers that are explicit in their policy and explain how they ensure that they are complying with and reinforcing human rights standards in any blocking they may do.

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

Filters create many problems for website operators, who cannot reach all of their users when their site is incorrectly filtered. This is a common problem in the UK, where many homes use ISP filters, but awareness about the problems they create is very variable.

Users (with admin permissions for the device) should be able to choose DoH provider according to their own preference. While Mozilla defaults could use local ISP DoH providers, in order to alleviate concerns about bypassing filters, this should not be deterministic. A user may for instance want to have a network filter applied, but bypass it on their own device.

Regarding the IWF blocklist, it is not universally applied by UK ISPs, and so may legitimately not be applied universally to UK DoH providers for reasons of practicality. Instead, the IWF should work with DoH providers with a significant UK userbase to work out appropriate use of their or similar lists. Mozilla should consider how to ensure the IWF knows which providers it may wish to contact.

The situation is analogous to VPN users, for instance. Most VPNs are unlikely to apply IWF lists, but some may wish to, and no doubt the IWF is thinking about how to resolve this question with VPN providers.

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

Technologies that are focused on users are likely to be more effective and useful. Network level filters are rather a blunt instrument and can be easily improved on.

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

Any block that is presented should at a minimum explain how to resolve a complaint by complaining to the party who obtained a block, at the splash page where and when that block is encountered. At present, this is not done by UK ISPs, who instead offer that users may apply to the court, rather than explaining which party, eg the BPI or MPAA, is compiling and maintaining a list of sites to block under a particular injunction, and has the immediate power to easily check and remove that block.

We would welcome a conversation with UK ISPs and yourselves about what needs to be done with splash pages to make it easier to remove mistakes, of which there are several thousand regarding copyright blocks, mostly domains for sale, that are no longer in use for copyright infringement. Likewise, regarding the IWF, block pages should be present explaining how to contact the IWF to obtain a review.

These changes should be made as part of the process of enabling UK ISP DoH at Mozilla, in order that transparency requirements are at a higher and more appropriate level.

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

Information should be provided at the time of sign up to any service.