DNS-over-HTTPS: a freedom of expression perspective

I. DNS-over-HTTPS: protocol innovation for the 21st century

ARTICLE19 monitors human rights compliance in technical standards bodies through direct intervention. As such, we are on the ground in standards development organizations where decisions are made with respect to future internet infrastructures.

DNS-over-HTTPS (DoH) is a new protocol for DNS provisioning which may guarantee stronger security and privacy for end-users, as well as more transparent choices on who to trust for an end-user. It is motivated by increasing concern over public and private censorship of end-user communications, and it means to bring transparency to DNS provisioning, where currently there is no transparency. In many cases DoH is also more efficient, resulting in websites loading faster for users.

> Domain name system (DNS):
>
> Also called the "telephone book of the Internet", DNS is a public decentralized database which links a unique name to the IP address (a virtual location) of a server.

It was developed at the Internet Engineering Task Force (IETF), the leading internet standards development organization since the 1990s. ARTICLE19 participates regularly in IETF meetings, and is co-leading the organization's research group on human rights.

II. What problem does it solve?

Today, DNS services are bundled with internet service provision. That is, the commercial entity responsible for looking up the virtual location of a server in the DNS database on behalf of the end-user is normally the internet service provider (ISP).

The ISP may be a residential ISP, a mobile operator, or a WiFi network at a café, railway station, airport or in the public library. Effectively, the end-user has a different DNS service provider every time they change the network, and in practice non-expert end-users cannot verify who provides their DNS at any given time.

DoH opens the possibility for end-users to more easily choose the DNS provider, for instance a web company or an independent company. It makes it possible to choose a trusted provider and keep that provider over many different networks in a way that is resistant to being overridden by the ISP.

In addition, it limits the vulnerability of the user to surveillance of their Internet usage by encrypting their DNS lookup requests. Specifically, it makes it harder for third parties other than the DNS provider to discover the websites or other Internet services the user is accessing.

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA

T +44 20 7324 2500 F +44 20 7490 0566
E expression@ARTICLE 19.org W www.ARTICLE19.org
Registered in England and Wales 2097222,
Reg.Charity nr 327421
O Free Word Centre, 60 Farringdon Road, London EC1R 3GA, UK

T +1 415 650 2557
E jeremy@prostasia.org W www.prostasia.org
S.501(c)(3) Non-Profit Public Benefit Corporation, California
EIN 82-4969920
O 18 Bartol Street #995, San Francisco CA 94133, US

III. Does it cause problems?

One consequence of DoH is that an end-user who chooses to trust a DNS provider other than their internet service provider (ISP) or mobile operator (MO), may end up with a DNS provider who is not covered by internet filtering obligations that ISPs and MOs are subject to under UK law.

We are aware that concerns have been raised, including in the House of Lords,[i] relating to a possible disruption of existing internet filtering and blocking schemes in the UK that aim to protect children, the most vulnerable members of our society, from harms.

The reality however is that DNS-based blocking has always been a fragile technique for Internet filtering. Even without DoH, users can and do easily circumvent DNS blocks using methods like Virtual Private Networks (VPNs), the Tor browser, or even simply manually changing their computer's network settings.

If DoH became widely adopted in the UK, this would merely hasten the natural obsolescence of DNS-based blocking, which was never fit for purpose to begin with. Given the inadequacy of DNS blocking the UK's reliance on this technique has created a false sense of security. DoH exposes this inadequacy, but it has existed all along. Children deserve better.

A more robust method for the elimination of illegal content uses a combination of hash-based filtering controlled by the Internet content host (which prevents the most egregious illegal material), in conjunction with more fine-grained, customisable filtering at the level of the Internet access device (using parental control software).

Both of these measures are already in place in the United Kingdom. All major Internet companies (including 140 who are members of the Internet Watch Foundation) already use hash-based filtering to prevent unlawful content. Parental control software is already widely and freely available. In combination, these are far better suited to the task at hand than DNS-based filtering.

But ultimately, we cannot rely on technology alone to solve the problem of exposure to illegal or unwanted sexual content online. In this context, we wish to highlight that recent child protection efforts turn away from internet filtering and blocking as a sustainable solution for child welfare. Through robust research and interaction with real children, it has been demonstrated that trust relations between adults and children and pro-active communication strategies instead work best to prepare children for the digital world.

The Swedish Prince Carl Philip and Princess Sofia's Foundation together with BRIS (Children's Rights in Society) recent *Parents' Guide To Kids Online* is a good example.[ii] The guide presents itself in this way:

> Kids and teens worry about things online they feel parents don't have a clue about. They might also fear getting blamed for things that have happened, especially if they have done something they know their parents are concerned about. Parents, on the other hand, often feel they are lacking in knowledge about new apps or trends. This gap between kids and grown-ups is the biggest hurdle to conversation. And that's what we want this book to change.

The goal of the book is to give parents tools to address difficult topics with their children on the children's own terms.

In addition, more attention needs to be given to changing the behavior of adults who seek out unlawful material online—not by throwing technical roadblocks in their way (which can inevitably be circumvented), but by educating them about the impacts of their behaviour, and providing them with the resources and support that they need to avoid offending.

Prostasia Foundation supports and works with several UK-based charities that are engaged in this important endeavour. One of them, StopSO, reports that 16% of the clients who contacted it for support for their troubling thoughts did so *before* offending or looking at child abuse images. If the UK government acted to reduce the stigma that surrounds seeking help, and provided additional prevention resources, many more children could be saved from harm.

We believe it is in the UK governments' interests to pursue more child-oriented child protection policies such as these, rather than placing stock in an obsolete method for website blocking that has long stopped being fit for purpose.

VI. On content filtering broadly

ARTICLE19 has long argued that internet filtering is not a good route forward to deal with unlawful content in the online environment. In 2016, ARTICLE19 presented the following observations:[iii]

1. Technical restrictions on access to content are prima facie an interference with the fundamental right of every person to exchange information and ideas;
2. Blocking measures in particular are notoriously ineffective, carrying the risks of both over-blocking and under-blocking and as such are a violation of the right to freedom of expression;
3. Blocking/filtering decisions usually lack transparency and are rarely ordered by a court. Very often, they are adopted by either administrative authorities or through so-called 'voluntary' cooperation with service providers. As a result, many governments are now in breach of their obligations under international human rights law through their use of blocking/filtering technologies. Even more disturbingly, vast swathes of information are disappearing from the Internet without users even noticing.

In fact, ARTICLE19 noted already in 2011 that "[c]ontent filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression."[iv]

Prostasia Foundation shares these views, with the proviso that it considers the voluntary hash-based filtering of verified unlawful images by commercial service providers to be an industry best practice, provided that it is disclosed to the end-user and that any hash list employed is maintained using a transparent and accountable process.

We hope the UK government **will take the opportunity presented by DoH to re-assess its previous strategies for child protection**, and that the UK government will work to ensure that the most vulnerable members in our society get the help they want and need, while at the same time new technical developments that have the potential to bring trust and security benefits to billions of people around the world are not needlessly cast aside.

ABOUT ARTICLE19

ARTICLE 19 is an international human rights organisation, founded in 1987, which defends and promotes freedom of expression and right to information worldwide. It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information.

ABOUT PROSTASIA FOUNDATION

We are a child protection organization that combines our zero tolerance of child sexual abuse with our commitment to human and civil rights and sex positivity. Our mission is to ensure that the elimination of child sexual abuse is achieved consistently with the highest values of the society that we would like our children to grow up in.

i House of Lords Hansard, Internet Encryption, 14 May 2019 Volume 797, Available online: https://hansard.parliament.uk/Lords/2019-05-14/debates/E84CBBAE-E005-46E0-B7E5-845882DB1ED8/InternetEncryption [accessed: 2019-08-06] and,

House of Commons, Tom Watson MP, Internet: Cryptography: Written question - 281658, and

House of Commons, Tom Watson MP, Internet: Cryptography: Written question - 281657, Available online: https://www.parliament.uk/business/publications/written-questions-answers-statements/written-questions-answers/?page=1&max=20&questiontype=AllQuestions&house=commons&member=1463

[accessed: 2019-08-06]

ii BRIS (Children´s Rights in Society) and Prince Carl Philip and Princess Sofia's Foundation, *KIDS ONLINE: A PARENT'S GUIDE*, February 2019. Available online: https://www.natforaldrar.se/#english [accessed: 2019-08-06]

iii ARTICLE19 Policy brief: *Freedom of Expression Unfiltered: How blocking and filtering affect free speech*, December 2016. Available online: https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf [accessed: 2019-08-06]

iv ARTICLE19, Global Campaign for Free Expression and the Centre for Law and Democracy, *Joint declaration on freedom of expression and the internet,* May 2011. Available online: https://www.article19.org/resources/joint-declaration-freedom-expression-internet/ [accessed: 2019-08-06]