ETNO position on DNS over https (DoH)

1. Position

ETNO members have followed the definition of protocol “DNS over https” (also known as DoH) and are concerned about the development around its potential implementation ([1][2][3][4]) and in particular the operational impacts for the networks of operators and internet service providers.

Whilst ETNO agrees that DNS over https as a protocol may provide some improvement to currently deployed DNS technology, ETNO considers that the foreseen deployments (browsers, but also mobile applications etc.) raise a number of issues regarding policy, law enforcement, user privacy and governance and will significantly impact its members. ETNO therefore calls for more industry collaboration to address these issues prior to large-scale deployment of the technology.

In particular, ETNO encourages the technical community to work together to develop mechanisms to address the impacts identified in this position, and notably, a mechanism for DNS resolver selection. ETNO considers that automatic default updates of browsers to DoH – that would result in customers switching from operator cache servers to public resolvers – would have a detrimental impact on (the quality of) operators’ fixed and mobile Internet access services.

ETNO is also concerned that the ongoing work on DoH has been so far limited to a particular technical community, when this technology has a number of non-technical consequences including (but not limited to) data protection, regulation and law enforcement. ETNO therefore calls for policymakers to review DoH technology to consider the impacts of the technology on the policies identified in this position. ETNO is ready to contribute to this analysis.

The rest of this paper provides a high-level analysis of the risks already identified with this technology (e.g. [5] and [6]) and further elements on our position on this topic as to where ETNO considers future work is necessary. This future work could also include widening the scope of the discussion to cover the full range of Encrypted DNS options – DNSSEC, DNS over TLS and DNS over HTTPS.

2. Background

The Domain Name System (DNS) is a critical element of the Internet infrastructure. It consists of a hierarchical and distributed set of clients and servers that enables Internet users and platforms to convert domain names such as etno.eu into other “Internet identifiers”. For example, the DNS is most commonly used to convert domain names into IP addresses.

The DNS recursive resolver is an essential element for the operators and Internet Service Providers to provide access to the web for their customers. This resolver is also widely known in operator networks as a “DNS cache server”. The DNS recursive resolver serves as an intermediary to process the DNS request received from a client (a set-top box, the Operating System of a smartphone, etc.), sending it to the hierarchy of servers to “resolve” the domain name and re-channelling the response from these authoritative servers. Most users who access the Internet use the DNS recursive resolver that is provided by their Internet Service Provider.

Various models of managing the servers that provide this resolver function exist among operators. Some operators outsource the management of the servers through SLAs, but most operate the servers themselves, sometimes using open-source software suites. For all traffic, the DNS requests between the client and the servers are sent over UDP or TCP in “clear text” i.e. unencrypted. In addition to providing a basic name-to-identity conversion, the servers of operators are also used as a control point for a number of other functions such as access policy (e.g. parental control, blocking of illegal content), content distribution (e.g. CDN), and phishing and malware detection.

Concerns over user privacy and security on the Internet led the Internet Engineering Task Force (IETF) to define Request for Comments (RFC) 8484 “DNS Queries over HTTPS” (DoH), approved in October 2018 to prevent man-in-the-middle eavesdropping on the requests and/or exploiting the user’s personal data without prior consent. Other mechanisms to encrypt the DNS traffic also exist, for instance, RFC “Specification for DNS over Transport Layer Security (TLS)” (aka DoT). However, since DoH is based on the same port (443) as https, the associated (encrypted) messages cannot be distinguished from other https non-DNS traffic.

In addition to these developments of the DoH protocol, proponents of the technology such as the Mozilla Foundation and Google have unveiled plans to implement DoH on their respective browsers, Firefox and Chrome. This may ultimately result in transferring the DNS traffic, which is today processed by the recursive resolvers, to so-called Public Resolvers e.g. Mozilla’s partner Cloudflare (1.1.1.1 aka “quad 1”) and Google’s public DNS (8.8.8.8 aka “quad 8”). As the DNS traffic is sent encrypted, it would become impossible for the Internet service provider to use their servers for the purposes mentioned above.

ETNO also notes the positive changes in position indicated by Mozilla and Google. We take note that recently Mozilla ([13] and [13]) has stated that there are no plans at the moment to enable DoH by default in the UK. In the same vein, Google stated that Chrome will only enable DoH if the existing DNS provider (as per client settings) supports DoH.

3. Impact of DoH on operators and their customers

The following sections identify several areas, where ETNO sees an impact of the combined use of DoH and public resolvers, and elaborate on the position taken by the ETNO.

ETNO members consider that DNS resolver "selection" mechanism for customers accessing the web on their networks should have as default choice the DNS resolver provided by the ISP before trying other options. Likewise, and for the same reason of maintaining the same level of service, if the browser user chooses to use DoH, the DoH DNS resolver provided by the ISP should be the default choice. As highlighted below under the split DNS section, a large number of enterprise customers of ETNO members would need to continue using their corporate DNS resolvers, and the policy of migrating to DoH should be their choice and that of their ISP.

Operational implications for operators

Content filtering through DNS blocking

The encryption of HTTP traffic represents a major challenge for Law Enforcement Authorities (LEAs). The emergence of DNS over https protocol will only increase this challenge. Currently end users can

change their DNS settings on their computers, but the reality is that this does not happen for the vast majority of residential fixed broadband users. This option will radically change, thus making investigations and blocking against malicious domains by LEAs much more difficult. LEAs will have to opt for investigation and blocking mechanisms that will ultimately be more intrusive (and less privacy-aware) than the current ones based on DNS.

In addition, the combined use of DoH and public DNS makes it impossible for operators to apply content filtering based on a limited list of domain names unless they implement their own DoH servers.

The use of domain name list based DNS filtering to implement parental control, for example, is not uncommon as it provides an easy way of giving customers the option to restrict access to the Internet. The use of DoH and public resolvers makes such control ineffective.

For Internet service providers in Europe, larger systematic DNS blocking is only applied under regulatory/legal oversight to prevent access to a website that is deemed illegal e.g. in the context of child abuse, illegal hate speech or counterfeit goods. It may not be the only measure taken for this purpose, because ways of circumventing such filtering do exist (including the use of VPNs or moving to public resolvers), but the use of domain name blocking lists remains widely in use. Operators will no longer be able to comply with legal requests regarding the blocking/redirection of domain names as is foreseen by national legislation (e.g. applicable legislation by national regulatory bodies, requests from magistrates).

ETNO members apply national regulations applicable to DNS blocking, **ETNO therefore considers that the motivation of DoH for circumventing excessive access control is unfounded in countries where its members operate**. On the contrary, the combined use of DoH and public resolvers will facilitate access to such sites.

Single point of failure

The Internet and DNS resolvers in particular have historically been deployed as a highly distributed architecture. The distribution of recursive resolvers among all access service providers makes it a highly resilient function of the Internet.

ETNO considers that moving all DNS resolver traffic from European ISPs to a limited number of non-European operators can only increase the impact of a potential failure of these public resolver providers on operators' customers and services. ETNO appreciates that some public DNS resolver architectures are designed to provide high resilience and scalability, but also notes that authoritative DNS hosting service providers have made similar claims in the past and have fell short on their commitment. At the very least, DoH conditions Internet access to the reliability of a handful of players. In the event of a failure, customers of European operators will solicit their operator's helpdesk for support. Europeans operators, ISPs in general and their customers would be likely to incur significant financial consequences in such events.

Network security, protection and threat detection

DNS filtering is commonly used by Internet Service providers for malware protection and cyberattack threat detection to protect their customers and their own networks from viruses and intrusions. This is in part based on lists of domains that are known to be at risk. These lists also depend on local

security policy and are not replicable on a centralised DoH public resolver. For example, block-lists that help detect botnet infiltrations and remote controls are impossible to apply with such architectures, which makes operators' customers and devices and therefore the Internet at large more vulnerable to denial-of-service (DDoS) attacks and computing capacity abuse (e.g. illicit cryptomining). **ETNO is concerned that the combined use of DoH and public resolvers weakens operators' own protection measures and puts operators' networks at an increased risk of cyberattacks.**

Public Wi-Fi and so called "coffee shop" access network scenarios

In the "coffee shop" access network scenario, where ISP subscribers take their phone to a coffee shop and connect to its Wi-Fi network which may be engaged in practises that the ISP / individual may not necessarily agree with, ETNO sees some benefits with DNS encryption if it is consistent with the elements developed above. As a result, and for it to be consistent with the technical and policy impacts described in this section, **ETNO considers that the resolver selection process applied for ISP subscribers under public Wi-Fi networks should be such that the user would have the option to use the ISP DNS by default if enabled by prior user choice/consent**. If ISPs do not offer this support function, the next best option would be to use selected cloud DNS provider rather than the coffee shop resolver.

Policy impacts

Single point of control and accountability for privacy

The browser market worldwide is highly centralised: almost 80% of the market is covered by two vendors [9]. Default DoH setting enforced by browser vendors would likewise result in customer DNS data being sent to a handful of players and would lead to an unprecedented concentration of Internet user data in very few points of control.

ETNO is concerned that moving all DNS traffic to a limited number of players, who unlike operators are not/less accountable to national authorities, offers no guarantee that user DNS traffic will not be monitored and monetised. In contrast with the current model whereby user data of a country is distributed across the domestic DNS resolver operators, the combined use of DoH and public resolvers will concentrate user data to a very limited number of large Internet players that may not be accountable as it relates to protection of personal data.

It is worth distinguishing between what DoH as a protocol does to secure DNS resolver information from a technical point of view and what Mozilla and Google (at least originally) plan to implement. The issue is that the plan in its complete and unilateral form, and notwithstanding recent announcements of these players (see above), is to move a fundamental part of the network routing resolution – that is the translation between names and IP addresses in the network layer – to a resolution feature of the service layer. This means that a network capability normally provided by network providers (Internet Access Service and IP carriers) would be provided by Content and Application Service Providers (often referred to as CAPs). **ETNO sees this as not consistent with the role of CAPs.** BEREC considers CAPs as users of network services provided by ISPs through the IAS (see [6] and [6]).

Response time to content and access to local content caches

The architecture of operators' farm of DNS cache servers is dimensioned to meet the common demands of their own specific customer base to access content on the web. Although having resolvers "close" to the customer premises may not necessarily mean that response time is optimal, having DNS traffic centralised on a handful of public resolvers may make it difficult to address different and possibly conflicting user requirements, especially if this involves sharing user's information such as its location.

Local DNS mechanisms are also used to redirect customers to web content caches to optimise access. Using centralised public DNS resolvers may affect these mechanisms and have a detrimental impact on access to web content for customers of European operators.

When response time is unsatisfactory, customers will turn to operators' helpdesk to address the problem. **ETNO is concerned that the use of DoH on public resolvers will increase the number of customer complaints to their helpdesks for performance problems that they would not be in a position to solve**.

Split DNS

A number of enterprise/corporate networks use architectures called Split DNS, where DNS clients on enterprise networks are provided with DNS records that are different from records on the Internet DNS. **ETNO is concerned that the combined use of DoH and public resolvers is incompatible with such Split DNS architectures and this may have a major technical and financial impact on how enterprise intranets are designed**.

ETNO notes that in Mozilla's process of releasing DoH in the USA, Mozilla is considering options to support "split-horizon" DNS and some form of filtering.

Geographic diversity among public DNS resolvers

ETNO notes that all prominent DNS public resolvers, and in particular those associated with the major browser companies, are based in the US. **ETNO is concerned that this would pose an issue of governance in terms of data collection and technical sovereignty of European players**.

Internet governance and fragmentation of the Internet namespace

In terms of access to the broader Internet namespace, ETNO operator members provide a uniform access to all top-level domain (TLD) names. Operators provide access to TLD names through their DNS cache servers relying on the IANA root [12] on the public Internet. Most Internet Service Providers use the same approach. In this respect, ETNO considers that the distributed nature of the DNS in general and how user requests are handled by ISP cache servers today are indeed a guarantee of stability for the Internet namespace.

Generally speaking, ETNO has been a long-time supporter of the ICANN multi-stakeholder model [13], whereby the management of the root zone file and the generic policies that govern how generic top-level domains are added or removed from the root zone file are perfectly transparent.

Although using DoH as a justification to centralise user DNS requests on a limited number of players is not directly aimed at fragmenting the Internet namespace, it is clear that a company which would collect 60% of DNS requests will be in a position to provide DNS responses that differ from those of the authoritative servers or, worse, to unilaterally decide to add or remove access to some TLDs to a large number of Internet users. **ETNO considers that the use of DoH as a justification for migrating the Internet user DNS requests to a very limited number of public resolvers raises serious concerns as to whether the Internet root zone would continue to be recognised by these players in the future.**

Transparency for Internet users

It is unclear at this stage whether the change of resolvers from the operator networks to centralised public resolvers will happen without the user's full "enlightened" consent, and whether using DoH on a public DNS resolver will be based on opt-in, opt-out, or made mandatory for all users. ETNO believes that the technical analysis of the use of DoH so far has given too little consideration to the overall consequences for the Internet user beyond the expected benefits of encrypting DNS requests. In ETNO's view, the consequences for users should be perfectly transparent both in terms of benefits and drawbacks. With the exception of small number of savvy Internet users, most users are unaware of how DNS works and what this change would mean for them. **ETNO considers that any such change cannot be made without the user's full consent and understanding of its impact in terms of where the DNS requests will be sent to, used for and what services may no longer be available.**

4. References

[1] RFC 8484 DNS Queries over HTTPS (DoH) https://tools.ietf.org/html/rfc8484
[2] CENTR Issue Paper on DNS over HTTPs https://www.centr.org/news/news/centr-publishes-issue-paper-on-doh.html
[3] ICANN 65, Policy Aspects of DNS over HTTPS (DoH), DNS over TLS (DoT) and Related Issues, Jun 25, 2019 https://65.schedule.icann.org/meetings/1058184
[4] ICANN 64, Emerging Identifiers Technology, Mar 12, 2019 https://64.schedule.icann.org/meetings/961998
[5] DNS over HTTPS (DoH) Considerations for Operator Networks https://datatracker.ietf.org/doc/draft-reid-doh-operator/
[6] Centralized DNS over HTTPS (DoH) Implementation Issues and Risks https://datatracker.ietf.org/doc/draft-livingood-doh-implementation-risks-issues/
[7] https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/
[8] https://www.theguardian.com/technology/2019/sep/24/firefox-no-uk-plans-to-make-encrypted-browser-tool-its-default
[9] statcounter.com Browser market share, https://gs.statcounter.com/browser-market-share
[10] BEREC's assessment of IP interconnection in the context of Net Neutrality BoR (12) 130 https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/1130-an-assessment-of-ip-interconnection-in-the-context-of-net-neutrality
[11] BEREC's Net Neutrality Guidelines BoR (16) 127https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules
[12] IANA root zone management https://www.iana.org/domains/root
[13] ETNO Reflection Document in Response to the Notice of Inquiry from the United States Department of Commerce on the Midterm Review of the Joint Project Agreement with ICANN https://etno.eu/datas/positions-papers/2008/rd278-nani-igv-ntia-jpa-etno-reply.pdf