DNS-over-HTTPS
Public Policy Briefing

Open-Xchange

Vittorio Bertola

vittorio.bertola@open-xchange.com

Version 1

November 2018

Table of Contents

1. Document scope 3

2. Executive summary 3

3. Basic concepts and current state of consumer DNS 4

3.1. Current state of encryption in DNS 5

4. DNS-over-HTTPS 6

4.1. Encrypting the DNS exchange and hiding it inside Web traffic 6

4.2. Transforming DNS into an application-level service 7

4.3. Centralizing the DNS into the hands of a few over-the-top providers 7

5. Public policy impacts of DNS-over-HTTPS 8

5.1. Privacy 8

5.2. Network security and administration 8

5.3. Parental and productivity control mechanisms 10

5.4. Law-mandated content filtering, blocking and censorship 10

5.5. Law enforcement and lawful interception 12

5.6. DNS policies and Internet fragmentation 12

5.7. Network neutrality 13

5.8. Competition 13

5.9. Centralization of the Internet 14

5.10. National sovereignty 14

5.11. User control 15

6. Conclusions 15

1. Document scope

This document provides a briefing on the public policy concerns raised by the **DNS-over-HTTPS (DoH) protocol**, a new technical specification recently released by the **Internet Engineering Task Force (IETF)**. It is designed for a non-technical audience having a basic knowledge of how the Internet works and of its current security and policy issues.

The following executive summary provides a two-page outline of the problem, while the rest of the document explains the technical issues in a simple language and discusses each concern in detail.

2. Executive summary

If you are unfamiliar with the technical concepts and terms used in this summary, please read section 3 first.

The DNS is the Internet's directory, being called into play each and every time the user accesses any online service or content (Web, email etc.). It is used to "resolve", i.e. convert into an IP address, the name of the server that the user wants to connect to; this makes the DNS "name server" a key point of control for all Internet usage. The name server is usually provided by the Internet Service Provider (ISP) of the user and managed by the operating system of the device.

DNS-over-HTTPS (DoH) is a new protocol just released; it allows browsers and other applications to send DNS queries directly to their own name server via HTTPS (the protocol used for the Web). It introduces three main changes in the way domain names are resolved:

1. The communication between the user device and the name server is encrypted and hidden within normal Web traffic in a way that cannot be easily detected or blocked;
2. DNS resolution is not managed any more by the operating system according to user settings, but each individual application can use its own name server;
3. The application makers, and especially the four big browser makers, gain control over the choice of the name server used for resolution, and could thus lead users to use their own and centralize all DNS resolution globally into their hands, bypassing the local name servers supplied by the ISPs.

This last effect emerged with the first major deployment of DoH, by Mozilla in their Firefox browser: they announced that they plan to redirect by default all DNS queries via DoH to their own name server, run by their partner Cloudflare, rather than to the name server configured by the user on the device.

These changes would have many far-reaching consequences on non-technical matters, which are discussed in detail in section 5 of this document.

The most radical change derives from moving the DNS "point of control" from the local ISP and the associated government to the big "over-the-top" players (OTTs) located in the United States.

ISPs and network administrators use their local name server for important security services, to block malware, phishing and botnets, and for shaping and monitoring their network. They also supply users with content-related services such as parental control and productivity filters, which are also based on DNS. All of this would stop working if the user's browser were pointed to other name servers out of the local network, effectively violating the security perimeter for which the network administrator is responsible.

Governments mandate DNS-level content filtering and website blocking measures to enforce national legislation of all kinds (security, hate speech, competition, tax compliance…), especially on foreign players and foreign-hosted content. DoH, deployed like Mozilla is doing, would circumvent all these measures by having users adopt a name server which is outside of their country and thus not subject to these laws. On the other hand, as almost all consumer name servers would be managed by U.S. companies, the U.S. government would gain even more jurisdiction over Internet usage all over the world.

Even from the user's point of view, DoH's advantages are questionable. By encrypting the DNS communication, DoH provides more privacy on the connection; but it also puts the user's whole online activity history in the hands of the few operators of the new centralized name servers. These companies, aggregating DNS data from billions of global users, could make money by monetizing this information and could cross-match each individual's DNS data with personal information from other sources. By using Web connections to send DNS queries, the common Web tracking techniques can be used to this purpose.

The "anti-censorship" properties of DoH, which can be valuable to dissidents in authoritarian countries, come at the price of depriving a much bigger quantity of Internet users in Europe (and in many other democratic countries) of the privacy and freedom guarantees that their local jurisdiction offers, forcibly transferring DNS resolution to a different jurisdiction that may not offer equivalent protection.

Moreover, today a user can easily decide which name server to use by setting it once for all in the operating system; with DoH, the user will have to change the name server dozens of times in each and every application, and it's not even guaranteed that all applications will make this option available.

So DoH is actually disempowering users, and pretty much everyone else, in favour of the OTTs that dominate the Web. Such a concentrated control over the Internet's namespace could even make the multi-stakeholder model for global DNS policymaking irrelevant.

In the end, we argue that DoH is yet another step – claimed to be technical, but in fact motivated by business reasons and with deep political consequences – towards the destruction of the original federated and multi-layered architecture of the Internet and towards its centralization into the hands of a few companies.

Due to all these concerns, we are raising awareness on the problem and advocate freezing the deployment of the new standard while these concerns are discussed and addressed with the involvement of all stakeholders.

3. Basic concepts and current state of consumer DNS

You may skip to the next section if you are already familiar with how the DNS works, and especially with the difference between local and remote ("public") resolvers, and with the state of encryption in DNS.

The **Domain Name System (DNS)** is a fundamental element in the Internet's set of basic protocols; it allows to discover the IP address corresponding to a server's name embedded in a URL or provided to an application, thus making it possible to connect to it and retrieve content or obtain a service. This operation is called **DNS resolution** and is accomplished by sending a **DNS query** to a DNS **name server** (in this role, also called **resolver**), which in turn will contact other name servers that are responsible for the specific domain name that was requested, retrieve the IP address and pass it on to the user's application.

Except in a very limited number of cases, every operation on the Internet (send an email, retrieve a Web page, exchange instant messages…) starts with a DNS resolution. This gives name servers relevance on privacy, security and other public policy issues, as each name server can track which servers its users want to connect to, and could even block or redirect the connections by altering the response to the DNS queries.

In theory, each Internet-connected device could perform the DNS resolution on its own, acting as its own name server. However, for technical reasons, usually the device only incorporates a simplified library, called **stub resolver**, within its operating system. All applications on the device contact the stub resolver, which sends the DNS query over the Internet to an external name server, which performs the resolution and sends back the result.

Traditionally, the resolver is provided to ordinary Internet users by their Internet access provider (ISP), as part of the connectivity service; it is usually configured automatically by the ISP's router when the Internet connection is established, via a protocol called **DHCP**. We will call this **local resolution**, as the ISP's name server is topologically near to the end user, and normally located in the same country; this is the default that all end-users get.

However, operating systems generally offer to the user the possibility to override the automatic configuration and pick a different name server, by entering the name server's IP address in a configuration screen. Several companies have thus started to provide **public resolvers** that any Internet user can adopt, either for free or as a paid service; the most famous is Google's "8.8.8.8". These name servers are topologically far from the end user and often located in a different country, so we will call this case **remote resolution**.

We could not find any reliable statistics on how the market for consumer DNS resolution is subdivided between the two models and among the various resolvers[1], but the broad majority of the end-users still seems to use the local resolution model; remote resolution, requiring opt-in and a minimum of technical knowledge by the user, is chosen only when the user has a compelling reason not to use the ISP's service, for example because it does not work well, or because the user is roaming (e.g. with a laptop in an Internet café) and does not trust the local network, or because the user wants to bypass a local policy applied to the DNS by the ISP or by the government.

3.1. Current state of encryption in DNS

DNS connections have always been unencrypted. Part of the security features that in other protocols are offered through encryption, certificates and so on, are offered in DNS by the **DNSSEC** extension; DNSSEC allows the resolver to verify that the reply to its query was not altered while in transit, even if transmitted over an unencrypted channel. However, the

[1] We could find the report of an anecdotal experiment in the United States concluding that about one fourth of the users was using remote resolution, mostly by Google, while the rest was using their ISP's name server – however, this has no statistic relevance.

adoption of DNSSEC is still slow in most parts of the world. Also, DNSSEC prevents the alteration of the results and removes many security threats, but does not prevent the interception and monitoring of DNS queries over the network.

In recent years, there have been proposals to encrypt DNS traffic as well. The **DNS-over-TLS (DoT)** protocol, released by the IETF a few years ago, allows to encrypt DNS communications without changing any other element of the architecture. The uptake of this protocol has however been slow or even non-existent, for several reasons.

Mainly, encrypting communications requires additional load and technical resources, so it must be justified by value (DNSSEC was designed to provide data security without requiring encrypted communications). In the case of the local resolution model, the communication between the user's stub resolver and the name server only traverses a limited number of nodes, all belonging to the ISP's own network – so opportunities for interception are much smaller than with HTTP, where the communication often traverses continents and many different networks and operators. This is why encrypting these communications has not been seen as a priority in the DNS community, nor there has been any significant user demand for it.

4. DNS-over-HTTPS

DNS-over-HTTPS (DoH) is a new protocol authored by Paul Hoffman (ICANN staff) and Patrick McManus (Mozilla). It has been published by the IETF as proposed standard **RFC 8484**[2] in October 2018.

The standard allows a client to send its DNS queries to a Web server acting as name server, as part of an HTTPS exchange, using all the encryption and authentication features provided by HTTPS, and making DNS resolution simpler for browsers and in-browser Javascript applications. It is explicitly focused on the connection between the end-user device and the resolver, and not on that between the resolver and other name servers.

The protocol introduces three major changes in how DNS works, which can be summarized as follows. In section 5 we will then discuss the public policy impacts of these changes.

4.1. Encrypting the DNS exchange and hiding it inside Web traffic

In DoH, the DNS query and the corresponding reply are embedded inside ordinary encrypted Web communications, using the HTTPS protocol. This makes it impossible to intercept, monitor or alter the communication for anyone on the network path between client and server.

Moreover, any Web server that wants to do so can act as a DoH name server. While the application could contact a specific DoH server separately from the rest of the Web traffic, it could also embed the DNS queries in the Web communications with a very popular website (e.g. www.google.com) supporting DoH. This would make it impossible even to know that DNS requests are being exchanged, and would make it realistically unfeasible to block the DoH service by blocking the IP address of the server, as that would also block

[2] https://tools.ietf.org/html/rfc8484

the very popular website. This was explicitly mentioned by one of the authors as one of the design objectives and advantages of the protocol[3].

4.2. Transforming DNS into an application-level service

Until now, the DNS resolution service has been provided by the operating system to all the applications running on the device; applications had no easy way to perform DNS queries without going through the operating system's stub resolver, as that would have required implementing and maintaining another stub resolver inside the application.

DoH was explicitly designed to allow any application able to "speak" HTTPS, and first of all web browsers, to bypass completely the operating system and the name server configured in it by the user, be it local or remote. Thanks to DoH, browsers and other applications can now perform DNS queries directly, and each one can choose its own name server, different from that used by other applications and from the one configured in the operating system, as long as this name server is updated to support DoH.

4.3. Centralizing the DNS into the hands of a few over-the-top providers

While the previous two changes to the DNS architecture are inherent in the DoH protocol and unavoidable, the extent to which this third one will materialize depends on the policies that will be applied when deploying it.

In late May 2018, even before the final standard was released, Mozilla added a DoH implementation to the Firefox browser, and also announced an agreement with Cloudflare, a leading content delivery network (CDN) provider based in the United States, so that all the DNS queries by Firefox users will in the future, by default, be directed only to Cloudflare's public resolver "1.1.1.1" using DoH, completely bypassing the resolver configured in the operating system[4].

As of today, Firefox has activated the DoH service for the users of its test version, but only in parallel with the "traditional" DNS resolution via the operating system, and has not yet turned off the latter. However, the original announcement has not been withdrawn.

Moreover, Google has implemented DoH in Chrome but has not announced yet their deployment policy, though rumors are that they will not follow Mozilla and will rather use the local resolver if it supports DoH. However, an Alphabet-owned company has released an Android application to enable DoH for all the communications of a mobile device[5].

These developments show how DoH is centralizing the DNS resolution for the Web into the hands of a few companies, namely the four major browser makers (Google, Microsoft, Apple and Mozilla, all from the United States) that control over 90% of the browser market both on desktop and mobile devices, and that DoH empowers with the choice of the name server used for resolution. Most of these companies are among the five big over-the-top (OTT) service providers that already control a great part of the Internet. If all these browsers adopted Mozilla's deployment model, the DNS resolution for almost all the Web

[3] See this interview: https://www.theregister.co.uk/2017/12/14/protecting_dns_privacy/

[4] See https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/ , and also the *"What is the status?"* section in https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/ .

[5] https://www.zdnet.com/article/alphabets-intra-app-encrypts-dns-queries-to-help-users-bypass-online-censorship/

traffic on a global scale would go through only four servers, those provided by each of these companies.

In other words, DoH promotes a switch from the “local resolution” to the “remote resolution” model, transforming DNS into another over-the-top application, rather than a network service supplied by connectivity providers. This could be avoided only if browsers and other applications committed to always use the local name server when available, though nothing would stop them from changing their policy in the future.

5. Public policy impacts of DNS-over-HTTPS

5.1. Privacy

One of the alleged primary objectives of DoH is to increase the user’s privacy, by encrypting the communication between the user’s device and the resolver, making it impossible for anyone to eavesdrop on it and thus to gain a list of the hostnames that the user is contacting during their online activities. This is indeed a benefit, but it is of limited value in the local resolution model, where the connection is topologically short and only managed by the user’s ISP, which is receiving the DNS queries on its resolver anyway; on the other hand, it is a significant benefit if the user is using a remote resolver, preventing their ISP and any network operator or attacker on the path from monitoring the DNS traffic.

At the same time, the centralization of DNS queries into the hands of a few OTT providers creates a much bigger privacy risk, by entrusting the personal information of billions of Internet users to companies that, in many cases, already have plenty of individual profiling information that can be cross-matched with DNS queries, and have data monetization as a core component of their business models.

Additionally, by performing DNS queries via HTTPS, all the tracking mechanisms currently used for the Web, from cookies to device fingerprinting, become immediately applicable to DNS queries as well, making such cross-matching straightforward.

Even if, in Mozilla’s deployment, Cloudflare publicly committed not to monetize this information, it is hard to imagine that none of these companies will do so in the long term; it is unclear why for-profit companies should run expensive DNS resolution operations on an immense scale if they cannot extract revenues from them[6].

For Internet users outside of the United States, this also represents a massive export of personal information to a foreign country; in Europe, it is unlikely that this can be compliant with the GDPR.

5.2. Network security and administration

By encrypting the connection between the user’s device and the resolver, DoH also prevents attempts to intercept and alter its content. Again, this is of limited value in the local resolution model, but it is of much higher relevance in the remote resolution model.

[6] ISPs, on the other hand, provide DNS resolution as part of a paid Internet access service; even if they still wanted to monetize this kind of information as well, they have much smaller amounts of information and a much smaller business reason, and also in several countries they are strictly regulated to prevent this.

Specifically, some ISPs are checking or even altering the DNS queries of their users that adopted a remote resolver, to enforce local security and content filtering policies even in that case[7]; encrypting the connection makes this impossible, freeing the user from such policies.

However, ISPs and network administrators deploy security policies at the DNS level – on their local resolver, and, if possible, also on remote resolver queries – for good reasons.

For example, several ISPs retrieve from a specialized provider (and in some cases, as in Switzerland, from national cybersecurity initiatives) an updated list of malware-infected websites, phishing pages, botnet command-and-control centres and so on; whenever a device tries to connect to any of these destinations, the ISP will block the DNS query, and thus the connection, and show a warning message. In some cases, the ISP can even identify the users that are sending these queries and warn them that their computer is infected by a botnet or a virus.

These mechanisms are more and more necessary to preserve the overall security of the Internet; ISPs can even be held accountable if they do not take action. While these threats could also be countered by installing an antivirus/security application on each single device, not all users do so; as the number of connected devices grows, users cannot install and manage antiviruses everywhere, and many of these devices (e.g. the “dumb” IoT ones) are not even technically able to run them. This makes the Internet access point for the home network a perfect place to locate security checks.

However, if the ISP’s users start using remote resolvers via an encrypted DoH connection, the ISP will lose any chance to apply these safeguards. Even if the remote resolver supplied by the browser applied security filters, it is hard to imagine that a resolver operator in another continent can keep up with local and national threats as quickly as the local operators.

Moreover, even if remote resolver operators managed to implement locally relevant security measures, this would not solve a basic issue: if DoH’s deployment had the effect to make users switch to a remote resolver, the ISP or the corporate network operator would lose the ability to use the DNS to shape the network, monitor what is happening on it and to reply to support calls or proactively take care of the users[8].

For example, many networks increase their security by customizing the DNS replies of their local resolver depending on who the user is and where they come from (the so-called “split horizon” configurations). Also, the network administrator can examine the overall database of DNS queries to detect usage trends and discover new threats (this is called “passive DNS”). These practices will become impossible if remote encrypted resolvers are adopted.

Generally speaking, the DNS is a fundamental element of the way any network works at the technical level, and this is why it is important that it is kept inside the “security perimeter”, especially for corporate and governmental networks in which avoiding external

[7] See https://www.dnsleaktest.com/what-is-transparent-dns-proxy.html for a technical description of this mechanism.

[8] Even RFC 7258 (https://tools.ietf.org/html/rfc7258), the IETF’s document that promotes the encryption of all protocols, recognizes that *“Making networks unmanageable to mitigate PM [pervasive monitoring] is not an acceptable outcome”*, though this problem has not been addressed in the development of DoH.

penetration and data exfiltration is paramount. These networks today often disallow the use of remote resolvers, by policy and/or by technical measures. Introducing a mechanism through which a browser breaks this perimeter, and doing so in a way that cannot be controlled or disabled by the network administrator, endangers the security of these networks.

Finally, DoH does not just disrupt DNS-based security for users and network administrators – it makes life easier for malware applications themselves, providing them with a new great way to break security perimeters.

Botnets, for example, need to be able to connect to their command-and-control server for functioning, and they usually rely on the DNS for this; as any IP address hardcoded in the code would be easy to spot and block, they make DNS queries for algorithmically generated hostnames that can then be pointed to the current IP address of the control server, which then can be easily and quickly changed in case of need[9].

By applying smart filters on the local resolver, botnets can be stopped, but bots can now use DoH to connect in an encrypted and almost unstoppable manner to a name server outside of the local network, and even to one run by the botnet owners or by complacent technical partners; bots can even encode information and files directly in the DNS queries and replies. Several separate implementations of this idea already appeared[10].

5.3. Parental and productivity control mechanisms

ISPs and network administrators also use the DNS to offer their customers voluntary, opt-in services to control what can be accessed over the Internet. For example, several ISPs in Europe now offer their users a parental control service (sometimes requested by the local government) so that families with children can turn off access to unsuitable websites; also, several products are available to corporations that want to make certain websites (e.g. social networks) inaccessible from offices and corporate networks during work time, to increase the productivity of their employees or reduce opportunities for computer infections and data exfiltration.

Since most HTTP connections are now encrypted, the DNS resolution is the only point of control to implement these features; by moving browsers to use remote encrypted resolvers, DoH will break these services and make inappropriate content immediately accessible to any child or employee that installed a DoH-enabled browser using a remote resolver.

5.4. Law-mandated content filtering, blocking and censorship

Most countries of the world have laws that make some kind of Internet content illegal. In authoritarian regimes, these laws may focus on stifling political opposition and freedom of expression; in democratic countries, these laws are usually limited to very specific types of content that endanger safety, minorities and public order, such as hate speech, Nazi-fascist propaganda, child pornography, instructions for terrorists, counterfeit medicine shops and so on. Also, blocking is used as the only possible retribution against global Internet platforms making business in the country without having a local company, to

[9] See https://en.wikipedia.org/wiki/Domain_generation_algorithm for a longer discussion of this practice.

[10] E.g. https://sensepost.com/blog/2018/waiting-for-godoh/ or https://github.com/SpiderLabs/DoHC2 .

enforce on them any applicable local regulation, including consumer and worker protection rules (e.g. on gambling, or on “sharing/gig economy” jobs and services), and the payment of in-country taxes and license fees.

In fact, for any content or platform located outside the country, especially in other countries not cooperating with law enforcement or having different rules, applying some kind of content filtering at the Internet access level is the only realistic way to enforce any national law.

While certain countries implement these laws by filtering out entire networks and IP address ranges, countries that want to limit the blocks to the necessary minimum usually apply these filters at the DNS resolution level, as this enables them to block specific hostnames and still allow access to all the other sites and services hosted on the same server. Thus, national ISPs receive a list of blocked websites from a certain kind of due process (court orders, governmental agencies…) and implement it on their local resolvers.

Users have often switched to remote resolvers to bypass these filters, and this is why, in some cases, ISPs also enforce them upon users that configured a foreign remote resolver, thanks to the lack of encryption (see 5.2.). However, even in the absence of such additional enforcement, the low share of users adopting remote resolvers ensures that these filters can be considered effective enough.

As long as the user continues to use a local resolver in the country, even via DoH or other encrypted protocols, these filters and blocks will continue working. However, DoH-enabled browsers using a remote encrypted resolver make these filters immediately ineffective; and given that DoH itself was explicitly designed to be very hard or impossible to block, if this became the default that users get when they install or update their browser, pretty soon almost all the citizens of the country would not be subject to these blocks any more.

This is considered a desired positive effect by those, including DoH supporters, that think that any forced governmental control over Internet content is censorship and violates human rights; in fact, fighting “governmental censorship” is often mentioned as one of the main objectives of DoH[11]. However, this is instead a negative effect if you believe that, at least in democratic countries and under due legal process, blocking access to content that endangers peace, democracy and the safety and rights of some parts of society, or to platforms that do not meet the local regulations on how they should operate in the country, is an appropriate measure.

One could have a discussion on whether blocking this type of content is a useful and positive response to the threat it poses, or whether it can ever be implemented without stifling free expression rights excessively. However, a decision on this point, involving a balancing of personal and collective rights which is highly cultural and varies across the world, should be taken by each democratic country through its own political processes; we do not believe that it is appropriate for the IETF or for browser makers to take that decision in place of each country’s people and elected authorities.

[11] See again the interview in note 3, or the app in note 5, or this interview to Cloudflare’s CEO: https://www.geekwire.com/2018/need-speed-security-cloudflare-developed-new-dns-service-pcs-phones/ or this statement on Twitter by Mozilla’s engineer and IETF Area Director Adam Roach: https://twitter.com/adambroach/status/1055923832861704192

It can also be expected that governments that mandate DNS-based content blocking will not passively accept the disruption of these filters, and will resort to more invasive measures, for example filtering content at the IP address level, making encryption illegal or requiring backdoors in encryption mechanisms[12].

It is also unclear whether the browser makers and their resolver operators will stand up to the pressures and legal threats that may be brought up against them by these governments, or whether – not to lose the business opportunities they have in those countries – they will actually resort to country-specific deals, adopting DoH deployment policies and DNS data management practices that vary by country; in this case, it is yet to be seen whether these policies and practices will actually be in the interest of the users and will deliver them all the promises of freedom, privacy and security.

On the other hand, since the remote resolver operator will still be subject to the laws of its own country, its users will definitely be affected by content blocking measures (or "censorship") mandated in that country. For example, European citizens that only use Firefox's remote DoH server are immediately subject to any content blocking measure imposed by the government or courts of the United States.

5.5. Law enforcement and lawful interception

Access to a user's DNS query history is also sometimes used in investigations, by police and law enforcement agencies. Again, as long as the resolution continues to be local, even if encrypted, law enforcement will still be able to gain access to these data by appropriate judiciary requests to the ISP. However, if the person under investigation is using a DoH-enabled browser with a remote resolver, these data will be out of reach for national authorities, unless they can obtain international access from the remote resolver's operator. Again, similarly to the discussion in 5.4., this may be seen as positive or negative depending on the specific country and situation.

On the other hand, law enforcement authorities of the remote resolver's country will be able to gain access to the DNS query history of the affected user. It can also be noted that in the United States, where all the browser makers are located, privacy protections for foreign citizens in case of law enforcement activities are weaker than those for U.S. nationals.

5.6. DNS policies and Internet fragmentation

As DoH puts a few browser makers potentially in control of almost all the Web-related DNS resolutions of the planet, this would attribute to these few companies a gatekeeping role over DNS policies as well. In other words, at any point in the future, it would only take an agreement between these few operators to apply modifications to the global DNS namespace, such as creating or blocking new top-level domains, that would be immediately available to almost all Internet users, even if the root server system did not support such changes and if they were not recognized by ICANN.

This is even more troubling if you suppose that such modifications started to happen without an agreement among these companies: each of them could start to create their

[12] See for example the ongoing discussion in Australia: https://www.reuters.com/article/us-australia-security-data/australia-plans-law-for-tech-firms-to-hand-over-encrypted-private-data-idUSKBN1KZ0W5

own TLDs, alter DNS results, filter content and so on. This can also be done today by the ISPs on local resolvers, but none of them has such a global reach and influence over the whole Internet.

In fact, having DNS resolution performed by the operating system ensures that, at least on each single device, all applications receive the same reply to the same query. By moving this to the application level, potentially each application could use a different resolver and get different results, suiting the policy and business interests of each application maker – so the DNS namespace could start to become more and more fragmented.

5.7. Network neutrality

Another alleged benefit of DoH, according to its authors[13], is to defend network neutrality by disempowering the ISPs and preventing them from altering DNS replies to disadvantage certain applications or certain content providers.

However, as DNS manipulation can be done by any resolver, DoH also empowers the OTT companies that run the remote DoH resolvers with the same possibility to hamper network neutrality; and these OTTs also offer many services that could benefit from network neutrality breaches.

In the end, DoH simply moves the ability to break network neutrality from the ISPs to the OTTs; and for users that live in countries where local laws offer stronger network neutrality protection than the laws of the United States, this change actually worsens network neutrality protection.

Specifically, content delivery networks (CDNs) often use the DNS to direct the user to the topologically nearest copy of the content. As Firefox's server is run by Cloudflare, a CDN operator, one could wonder whether Cloudflare will use the resolver to make its own content faster, and the content hosted on competing CDNs slower. An anecdotal experiment in the Netherlands for www.whitehouse.gov showed that the address returned by Cloudflare/Mozilla's server was 20% slower than the one returned by the local ISP[14].

5.8. Competition

Consumer DNS resolution is also a market. Local resolvers are provided as part of a paid Internet access service, while remote resolvers are generally free, but some of them are instead supplied as part of paid services, like Cisco's OpenDNS.

By recommending or even forcing a specific resolver to their users, browser makers are exploiting their share of the browser market to gain control over a share of the consumer DNS resolution market; and this, also given the very limited number of significant players in the browser market, raises anti-trust concerns. Consumer DNS resolution on a global scale is currently provided by thousands of companies scattered around the globe; through DoH, the exploitation of the browser's market share now enables a few companies to gain almost full control over the resolution market and concentrate it tremendously.

This could be just one more of many instances in which OTT players have used their dominant position on the global Internet to gain control of a service which was previously

[13] Again, see the interview linked in note 3.

[14] See https://blog.powerdns.com/2018/09/04/on-firefox-moving-dns-to-a-third-party/ , "Neutrality" section.

provided by local ISPs and telcos, draining wealth from all over the world to a limited stretch of territory on the U.S. West Coast.

Moreover, as resolution has traditionally been provided as part of the Internet access service, users will continue calling their ISP whenever it does not work. In other word, this change, especially if effected almost silently by changing a default and just showing a confirmation popup, will create significant support costs for the ISPs while also depriving them of any revenue deriving from DNS-based consumer services.

In fact, some of the DNS-based services described before, such as network security filters or parental control products, are in many countries a growing revenue stream for the ISPs, which would be immediately taken away by the browsers if they led their users to stop using the local resolver.

Finally, we note that governments use their ability to make Internet content inaccessible as a possible enforcement tool when trying to regulate Internet-based services of any kind, especially those that affect established "offline" industries such as transportation and hospitality, ensuring that any global platform competes on a level field with new and established local players. If this ability were taken away, governments would be even less able than today to regulate the impact in their country of new globally disruptive platforms, as these platforms could simply ignore any national regulation and serve the country from abroad over the Internet. Thus DoH does not just affect competition on DNS services – it globally affects competition on any service provided through the Internet.

5.9. Centralization of the Internet

Centralization of key Internet services into a few hands is *per se* a growing concern. The Internet has flourished thanks to the ability of every user to deploy new content and new technologies, and to innovate freely; however, opportunities for innovation are hampered when dominant positions emerge. Such centralization also reduces cultural, service and business diversity.

The centralization also makes the Internet more fragile in terms of reliability and security. If most DNS resolutions went through a few global name servers, these servers would become a potential point of failure for the entire Internet. In fact, in 2016 there have been successful denial of service attacks against one of the major global DNS providers. This risk has been recently recognized even at the IETF, in a draft by several members of the Internet Architecture Board[15].

5.10. National sovereignty

The switch from the local to the remote resolution model, promoted or even forced by DoH, implies a change in the jurisdiction that applies to DNS resolution operations; many of the policy issues exposed in the previous sections derive from this change.

The countries that do not host the new global resolution providers will thus lose any jurisdiction over the DNS queries of their citizens, which in turn, as we have seen, implies losing control over issues that affect individual and collective rights, security and economic opportunities. This control is instead transferred to the countries that host the global

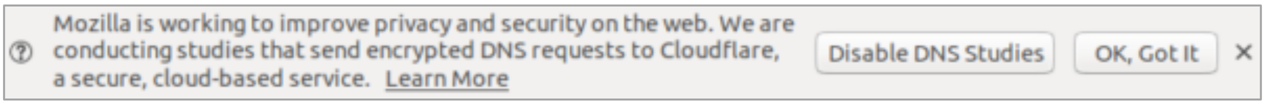
[15] https://tools.ietf.org/html/draft-arkko-iab-internet-consolidation-00

resolvers; and this arguably constitutes a loss of national sovereignty, which gets transferred to a different country.

5.11. User control

One of the advantages of DoH is to give the user more control over their DNS resolution when the user wants to use a remote name server, since it prevents any interference by governments and ISPs with the user's choice of giving all their DNS queries to Google, Cloudflare or other global providers.

At the same time, ignoring the name server configured by the user in the operating system and promoting the redirection of DNS queries to the browser's own server, like Mozilla is doing, does not look like an attempt to put the user in control. The user should be able to make a fully informed choice after understanding all the consequences, rather than just being offered more privacy and suggested to click *"OK"*. As an example, this is the message that Firefox showed to its users to get permission to activate Cloudflare's DoH server in parallel to the operating system's one:



Mozilla is working to improve privacy and security on the web. We are conducting studies that send encrypted DNS requests to Cloudflare, a secure, cloud-based service. Learn More

In terms of trust models, for the last thirty years, the default on any Internet-connected device has been to use the local resolver supplied by the Internet connectivity providers, with the possibility for the user to change it. Reversing this default, and using by default a remote resolver, betrays the expectations of the user, and should only be done after careful thought and appropriate communication.

Also, in the current situation, the user can choose the name server once for all applications on the same device, by setting it in the operating system. Under DoH's paradigm of resolution at the application level, the user would have to set it multiple times, in each application one by one; and even if all applications offered the user the ability to change their default DoH server, something which cannot be taken for granted, this change would still be inconvenient and cumbersome for the user.

There is thus a fundamental issue over who controls the setting of the resolver, and how to make it possible for users to make appropriate and informed choices. Without solving this issue properly, DoH could actually much reduce the control that individual Internet users have on their name server settings and on their DNS resolution process.

6. Conclusions

We have illustrated in this document the very long list of concerns that are raised by the introduction of DNS-over-HTTPS and by the way it is being deployed. We note that almost all these concerns are not related to the encryption of the DNS connection, but rather derive from the centralizing effects of DoH and from the switch from local to remote resolution. Almost all the privacy and security advantages of DoH could be obtained through other DNS encryption protocols as well, such as DNS-over-TLS, without generating all these adverse effects.

We note that most of these concerns have not been addressed or even mentioned by the IETF prior to the release of the new standard, which was conceived only in a small circle of engineers. The discussion at the IETF, though well intentioned, failed to address many of the architectural, policy, legal and business issues that this new protocol is creating, and that also intersect complex questions on sovereignty and jurisdiction. Several of these issues could also require further protocol work[16], which should be done before DoH is deployed at the consumer level.

Moreover, the main features of DoH seem to be very valuable in certain parts of the world, where users do not trust their ISP or their government, but of limited value or even damaging in others, where privacy, security and freedom of expression are well protected and would actually be reduced by the adoption of the remote resolution model and by its centralizing effects. We think that the needs and expectations of these other parts of the world, like Europe, have not been adequately considered yet.

We think that this issue deserves a full multi-stakeholder discussion, involving not just the IETF and the Web industry, but other parties like the DNS and security industries, ISPs and telcos, governments and even the final users. Thus we suggest that all involved parties should freeze the deployment of the protocol and agree on where and how to have that discussion.

[16] For example, even if an ISP wanted to provide a DoH server to its customers, it would have no way to announce its existence to user devices, because the IETF has not released an extension to the DHCP protocol or a similar alternative way for the ISP to do so, nor browsers have implemented it.