Local and Internet Policy Implications of Encrypted DNS

ICANN Office of the Chief Technology Officer

Paul Hoffman
OCTO-003v2
25 February 2020

TABLE OF CONTENTS

This document is part of the OCTO document series. Please see https://www.icann.org/resources/pages/octo-publications-2019-05-24-en for a list of documents in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

This revision contains updates from many people who read OCTO-003v1. ICANN greatly appreciates the reviews sent to us.

1 Executive Summary

Since the creation of the Domain Name System (DNS), DNS traffic has been sent between computers and recursive resolvers in cleartext, meaning in-path observers could read the requests and responses. Recently, new technologies have been standardized to allow this DNS traffic to be encrypted, so that observers cannot see the information in the requests and responses. Deployment of these new technologies, particularly in browsers, is increasing.

The use of encryption for DNS traffic has numerous implications that are now being discussed in earnest in many different forums. Adding privacy to DNS traffic prevents eavesdroppers from gaining valuable information, but it can also prevent network administrators from using DNS as a way to enforce content, access, and other control policies. Recent discussions have shown that the way that DNS encryption is deployed has significant effects on enforcement of local policy. This paper discusses the ramifications of various proposed deployment strategies for encrypted DNS between end user computers and recursive resolvers.

2 Introduction

This document first gives a brief technical description of the two major standards for encrypted DNS. It then gives an overview of the major issues that have been discussed as encryption has been added to the DNS protocol, and also lists many of the most interested parties. These issues fall under the general topic of “policy,” even though that term is not well defined. In this document, “policy” can mean “local policy,” such as rules that a system administrator wants to put on their users, and it can also mean “Internet policy,” such as the guidelines that are commonly expected across the Internet. However, for the purposes of this document, it does not mean “ICANN policy,” because ICANN has no community-approved policies that relate to how resolvers and authoritative servers use encryption.

There is no attempt in this document to go into depth about the policy issues that are listed, because each interested party has a different take on those issues, even when they agree. These issues are being discussed in many places; a list of some of those venues is given in Appendix A.

Individuals in many parts of the ICANN community have different (and often strongly-held) views on the topic of encrypted DNS, but there has not been any consensus about which positions might be more important than others, or even how to implement the various policies that have been proposed.

2.1 Adding Encryption to DNS

The DNS protocol was designed well before there was any thought that Internet communication protocols should always have encryption and authentication built-in. “Classic” DNS, which is still by far the most used method for sending and receiving DNS messages, has no encryption or authentication. That is, the data in the DNS messages are not encrypted, and the transport of those messages between the parties in the classical DNS protocol adds no encryption; nor are the endpoints of communication authenticated. Even when DNSSEC is used by both parties, doing so does not add any privacy.

During the ensuing decades since the DNS was created, there have been a few proposals for how to add encryption and authentication to DNS, although none of those caught on before the Internet Engineering Task Force (IETF) standardized *DNS over TLS* (often abbreviated as "DoT") in RFC 7858 in May 2016.[1] DoT uses the same message structure as classic DNS, but adds encryption with Transport Layer Security (TLS) to DNS packet exchanges. TLS is the protocol that adds privacy and communications integrity to many other protocols, most notably to HTTP. Currently, DoT only defines how to encrypt DNS traffic between end users' computers and recursive resolvers, not between recursive resolvers and authoritative servers, and not between authoritative servers.

The IETF later standardized a second method for encrypting and authenticating DNS: *DNS over HTTPS* (often called "DoH") in RFC 8484 in October 2018.[2] Whereas DoT is "DNS messages transported over TLS," DoH is "DNS messages wrapped in HTTP messages, transported over HTTP over TLS". The extra wrapping in DoH may seem superfluous and/or inefficient, but browsers deal with this sort of encapsulation all the time and it has some operational and security properties that made DoH significantly more attractive to browser vendors than DoT, such as allowing servers to push DNS responses before being requested. DoH is primarily designed to encrypt DNS traffic for applications, such as web browsers on end users' computers, whereas DoT is primarily designed to be an alternative, more private, transport for DNS messages for operating systems.

During the effort that led to DoT, there was little discussion of the local policy implications of encrypting DNS traffic from end users to resolvers. However, as a result of DoH increasing the complexity of monitoring and filtering DNS traffic, after the first implementation plans for DoH were announced by browser vendors, a number of policy discussions have been taking place in many forums, often with very diverse groups of participants. Many of those discussions are on how a computer or application chooses which resolver it will use for encrypted DNS, although resolver selection is not inherently part of encrypted DNS.

This document focuses exclusively on encryption of the transport channel between devices such as end user computers and recursive resolvers. The IETF has not standardized an encryption protocol to secure the transport channel between recursive resolvers and authoritative name servers, nor for between authoritative servers. If the IETF does so, it is likely there will be different local and Internet policy implications than those created by encrypting the client to recursive resolver communication.

2.2 Definitions

This section defines some terms that are used throughout the document. Note that there is no universal agreement on the definitions given here because the terms can have very different meanings in different contexts.

For an overview of other terminology that is used when discussing the DNS, see RFC 8499, *DNS Terminology*.[3] In specific, Section 6 of RFC 8499 defines the roles of recursive resolvers and authoritative servers, both of which are important for understanding where encrypting DNS takes place. (In short, DNS resolution typically starts on end user computers with queries sent to

[1] See https://datatracker.ietf.org/doc/rfc7858/
[2] See https://datatracker.ietf.org/doc/rfc8484/
[3] See https://datatracker.ietf.org/doc/rfc8499/

recursive resolvers; recursive resolvers send different queries to authoritative servers to formulate answers that can be sent to the end user computers.)

DNS messages – DNS is a query/response protocol in which every transaction is started by a DNS query from a client and is finished by a DNS response from a resolver or authoritative server. Each DNS query and each DNS response is a DNS message.

Middlebox – A system in the network between a client and a server that observes and possibly modifies traffic. In this document, middleboxes are usually firewalls that are operated by network managers to protect users and system assets in their network.

Enterprise – An organization, such as a company or a school, that offers network services to the people who are part of the organization. The enterprise's network or networks may be managed by professional managers or outsourced administration services. Enterprise networks usually provide either recursive resolution of DNS queries or forward such queries to other enterprises for resolution.

Home network – A small network of computers in a home. Home networks are usually unmanaged, although they can sometimes act as very small enterprises.

Internet Service Provider (ISP) – A company or organization that provides commercial network connectivity to a variety of clients. Historically, ISPs almost always provide recursive resolution for DNS queries, often using their own recursive resolvers. ISPs sometimes offer other DNS services, such as providing or managing middleboxes for home and enterprise clients.

Government – An organization that is recognized to have authority to make and enforce laws.

Throughout this document, the word "computer" refers to any system or device that can request DNS resolution. These include any system that is connected to the Internet, such as mobile phones, laptops, desktop computers, and even devices such as smart televisions.

3 Filtering and Monitoring DNS

Some enterprises, ISPs, and home networks filter DNS messages. Some filter in the provided DNS resolver; others do it using middleboxes. Filtering and monitoring of DNS traffic are known to be imperfect methods to achieve goals such as blocking objectionable content and preventing malware, but they are often considered good practices for networks. SAC 050, "DNS Blocking: Benefits Versus Harms," has an in-depth examination of DNS filtering.[4]

There are diverse reasons for filtering, such as reducing the risk of phishing/malware infection, "parental controls," and "government mandates," but the filtering itself usually consists of either:

- intercepting DNS *queries* for domain names related to suspected undesired content and preventing a DNS response for those queries, or

[4] See https://www.icann.org/en/system/files/files/sac-050-en.pdf

- intercepting DNS *responses* for domain names related to suspected undesired content and changing the answers to point to either non-working servers or servers that have different content.

Some middleboxes and resolvers that do not actively filter DNS messages will at least monitor those messages for later analysis. Monitoring DNS traffic can be useful for finding attempts to exfiltrate information that is meant to stay within the network or on a particular computer, for detecting malware that gets installed despite the best efforts of network administrators, and many other purposes.

Encrypted DNS messages cannot be read by middleboxes that filter or monitor, so that filtering/monitoring becomes impossible by those middleboxes, unless a middlebox and the associated computers are configured in such a way as to provide the middlebox with the key to decrypt TLS traffic. Filtering and monitoring can be done on resolvers because those resolvers are an endpoint for the encrypted DNS traffic and thus the traffic would be unencrypted by the resolver.

When filtering is integrated with the DNS resolver, the choice of resolver directly affects the choice of filters imposed and the monitoring conducted. When middleboxes provide this filtering or monitoring, they typically intercept the DNS traffic when it is sent to or from a resolver. For unencrypted traffic, it is difficult for the DNS client to detect the filtering and monitoring. For encrypted traffic, an intercepting proxy can be detected during the exchange of credentials. Thus, it must present credentials which will be accepted by the DNS client.

4 Primary Local and Internet Policy Issues for Encrypted DNS

This section gives an overview of the local and Internet policy issues of encrypted DNS that are most often cited in public discussions. The text here does not attempt to assign a value judgement on how important each issue is, or assess which of the interested parties listed in Section 5 appear to have the most stake in any particular policy issue. Some of the arguments that are made about encrypted DNS cover multiple policy points at the same time. Again, this discussion is only about local and Internet policy, not ICANN policy.

4.1 Increased Privacy for Users' DNS Traffic

Any Internet traffic that is not encrypted can be easily viewed by third parties that are between the two ends of the traffic. For the DNS, this means all of a user's unencrypted DNS messages can be seen by anyone who has access to the network between them and the resolver they are using. The more routers or middleboxes that are between a user and the resolver, the more places that someone can observe the DNS traffic.

4.2 Increased Assurance for Users' DNS Traffic

Applications that are concerned that the resolver being used by a computer may be giving responses to DNS queries that reveal information about the user or otherwise act in ways the application developers felt were inappropriate, might choose to instead use a resolver more

preferred or trusted by the application. Middleboxes that are watching unencrypted DNS traffic might block access to such resolvers, and one way to prevent them from doing so is by encrypting the DNS traffic and mixing it with other encrypted traffic going to the same destination.

4.3 Circumvention of DNS Filtering for Security

One frequent reason for DNS filtering is to prevent malicious actors from attacking network users. Some attacks that can be prevented, or at least thwarted, using DNS filtering include:

- Visiting websites that install malware
- Getting email from servers that typically send malware
- Communicating with malware servers after being infected
- Exfiltration of sensitive data

However, some users may feel that such filtering is redundant or blocks their use of the network in some way. They may choose to circumvent that filtering by encrypting their DNS queries, typically by using different servers than the one provided by their network operator.

4.4 Circumvention of DNS Filtering for Local Policy

Some networks filter DNS traffic to enforce local policy that is not related to user or organizational security. There are many types of local policy which can be at least partially enforced with DNS filtering, such as:

- Preventing users from seeing particular types of content, such as hate material
- Reducing the chance of tracking users by unauthorized websites
- Enforcing limits on the use of some sites to particular hours

More common than circumvention of DNS filtering for security, circumvention of DNS filtering for local policy by encrypted DNS is frequently performed to bypass limitations on access to services or content on the Internet.

Encrypting Internet traffic with DoH prevents middleboxes from knowing whether that traffic contains DNS traffic, or at least hides that traffic even if it is clear that it is DoH traffic because the host is known to be a DoH server. Thus, if a network has a local policy of requiring particular DNS resolvers be used, the middlebox cannot detect whether a different DNS resolver is being used during any encrypted sessions.

Note that a middlebox still knows the endpoints of the traffic. For example, if a resolver that supports DoH and/or DoT has one or more known IP addresses, a middlebox can assume that encrypted traffic to those addresses is DNS traffic and can enforce local policy, such as blocking encrypted traffic to those addresses.

4.5 Circumvention of DNS Filtering that is Mandated by Governments

Some governments have laws and regulations that require some entities to filter DNS for particular types of content. If, due to encryption, the DNS messages cannot be seen by those who are required to perform filtering, the filtering becomes impossible.

Note that different laws from different jurisdictions apply to different parties. Some laws apply to ISPs, but they do not define whether enterprises count as ISPs, or whether homes with middleboxes count as ISPs.

4.6 Unwanted Centralization of DNS Resolution Cannot Be Detected

Centralization of DNS resolution can have both positive and negative effects. Some of the positive effects include ease of configuration, having just a single set of DNS policies to understand, and larger caches leading to some faster responses. Some of the negative effects include making the resolver a more interesting target for those who want to surveil DNS traffic, making the resolver a more interesting target for denial of service, unnoticed malicious actions by the resolver operators, and slower web traffic due to geographic misidentification.

The rapid rise in voluntary use of Google Public DNS (also known by one if its IP addresses, 8.8.8.8) and similar services shows that some network administrators and users feel that the balance is more positive than negative. At the same time, however, many systems have begun to use Google DNS and other centralized DNS resolvers without users' knowledge.

Some applications that can do encrypted DNS (such as Firefox) currently have configuration options that can change the resolver that is used for DNS resolution. Other applications and operating systems (such as Chrome and Android) currently only upgrade a classic DNS session to encrypted DNS using the same resolver. In the former case, DNS resolution will become more centralized towards the default resolvers chosen by the application.

4.7 Speed of DNS Responses

ISPs and content providers often care a great deal about the perceived speed of their services. Because DNS is the first step for many Internet connections, slower DNS resolution can add perceivable latency to an ISP's service. DoT and DoH inherently have a slower startup than classic DNS, and can easily have greater latency even after a DoT or DoH session is started, depending on networking setting either on the client or the resolver.

5 Interested Parties

Encrypted DNS is of interest to many organizations and people. Initial interest was only in the DNS technical community, followed by the security community, but then interest widened when it became clear that there were significant issues when encrypted DNS was deployed. This

section briefly lists some of the many groups who have already expressed interest in the local and Internet policy aspects of encrypted DNS.

5.1 Browser Developers

Both Mozilla and Google have announced plans to deploy DoH in their browsers (Firefox and Chrome, respectively). In February 2019, Firefox began shipping with DoH visible to users but not enabled by default. The developers of these browsers are actively involved in discussions of the implications of DoH deployment. Developers of some other browsers have also expressed interest in deploying encrypted DNS, but have not been nearly as active in the public discussions.

The following information about the plans for encrypted DNS in popular browsers is believed to be true at the time of publication (October 2019), but will likely change in the future. This document will be updated when there are significant changes in the DNS ecosystem that affect the implications of encrypted DNS.

5.1.1 Mozilla Firefox

A recent blog post from Mozilla gives their rollout of encrypted DNS.[5]

Firefox ships with the capability to enable DoH in its preferences command, with the feature turned off. The “Enable DNS over HTTPS” option has a “Use Provider” option that allows the user to choose from a short list of providers or enter a custom URL for a different DoH service provider. The values for these options can be modified by site administrators who are using Firefox for Enterprise.

At the time this document is published, Cloudflare and NextDNS are the only DoH service providers listed by default because they have agreed to the requirements to be considered as a potential partner for Mozilla’s Trusted Recursive Resolver (TRR) program[6].

Other resolver operators are in discussions with Mozilla to be added to Mozilla’s TRR list. If they are accepted, they may appear in the “Use Provider” list, based on considerations such as the countries in which they are located. Mozilla expects the initial set of providers to be small but to grow over time. Mozilla has not specified how a default provider will be selected if there is more than one provider in the list.

Firefox checks whether the user’s computer and/or the user’s network uses opt-in parental controls and disables DoH if it detects those controls. Mozilla is working with companies that offer such controls in order to make them visible to Firefox. Firefox also checks for a signal that the local DNS resolver implements special features that make the network unsuitable for DoH.[7] This mechanism may change in the future.

[5] See https://blog.mozilla.org/blog/2020/02/25/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/
[6] See https://wiki.mozilla.org/Security/DOH-resolver-policy
[7] See https://support.mozilla.org/en-US/kb/canary-domain-use-application-dnsnet

If the DoH server fails during resolution or gives an NXDOMAIN response, Firefox will also send the queries to the resolver that the computer is using.

Mozilla has enabled DoH automatically in Firefox for many users in the United States. When DoH is enabled for a user, that user is alerted and have the opportunity to opt-out of its use.

5.1.2 Google Chrome

A blog post from Google in September 2019 outlined their plans for testing encrypted DNS using DoH in Chrome.[8] In December 2019, Google indicated that the results so far had been encouraging, and gave tentative plans for the next steps if the experiment is successful.[9]

During the fall of 2019, Google conducted an experiment to validate their implementation of DoH. This experiment was done in collaboration with DNS providers who already support DoH by upgrading users to DoH on their current DNS service. Under that plan, if DoH fails, Chrome will revert to the provider's regular DNS service. The providers included in the list are selected for their privacy and security policies, as well as the readiness of their DoH services. Google has not said how it will add to that list of providers. Enterprise administrators are able to opt-out of the experiment.

End-users have the ability to control and configure the feature to match their needs. Enterprise administrators are able control enabling, disabling, or configuring a specific DoH service.

Google is interested in future protocols that would give the browser more details about the network, in particular which ISP is providing the service and which DNS resolvers are involved beyond the first hop (typically, the home router).

5.2 Operating System Developers

To date, browsers have been getting the most publicity for their deployment of encrypted DNS. However, some operating systems also have deployed encrypted DNS, and thus the developers of operating systems may also be interested in discussions around encrypted DNS.

5.2.1 Android

Google's Android operating system, which is popular on many cell phones and tablets, was the first to support automatic encryption of DNS traffic. Beginning in 2018, the stub resolver in Android automatically upgraded to DoT if the recursive resolver it was using supported DoT at the same address.

5.2.2 Microsoft Windows

[8] See https://blog.chromium.org/2019/09/experimenting-with-same-provider-dns.html
[9] See https://groups.google.com/a/chromium.org/forum/#!msg/net-dev/IIm9esAFjQ0/vJ93oMbAAgAJ

In November 2019, Microsoft announced plans to start supporting automatic encryption in the Windows operating system using DoH.[10] The Windows DNS client in Windows Core networking will use DoH for any DNS servers that Windows is already configured to use, although no date was given for when this feature will appear in Windows. The intended policy, which is still under development, is that failures in DoH will cause DNS lookup failures.

5.3 Governments

Governments have begun taking an interest in encrypted DNS. Some of these governments are concerned about the impact that encrypted DNS might have on existing requirements in their jurisdictions to filter or monitor DNS traffic. Some are also concerned about the potential anticompetitive effects that centralization of DNS lookup suggested by certain deployment models might have on their local markets. Recent examples of governmental interest in encrypted DNS include inquiries by the US Congress into the practices of some providers of encrypted DNS services[11] and legislative hearings in the UK Parliament.[12]

5.4 Network Administrators

The network administrators of ISPs and enterprises (and, to a much smaller extent, home networks) often care about the DNS traffic in their networks, particularly if they cannot view or filter that traffic. Some browser and operating system vendors who are adding encrypted DNS capabilities are adding features to allow network administrators to change where encrypted DNS is performed or to prevent it from being automatically configured.

5.5 DNS Developers

The companies and people who create the software that runs in various parts of the network often care about the larger implications of that software. In the case of DNS, some of the software developers were active in discussions about encrypted DNS well before other parties, and continue to be concerned with how the features and configuration options of their software will affect policy made by others.

6 ICANN Position

The ICANN community has not developed a consensus on encrypted DNS. As such, ICANN organization's position, if any, on the deployment of encrypted DNS has not been informed by community input. However, there are some basic principles in the context of the secure and stable operation of the DNS upon which ICANN's Office of the CTO does have a position.

To be clear, the following principles are not intended to be prescriptive or identify areas in which ICANN has specific responsibilities. Rather, they aim to be supportive of efforts to ensure a

[10] See https://techcommunity.microsoft.com/t5/Networking-Blog/Windows-will-improve-user-privacy-with-DNS-over-HTTPS/ba-p/1014229
[11] See https://crsreports.congress.gov/product/pdf/IN/IN11182
[12] See https://hansard.parliament.uk/Lords/2019-05-14/debates/E84CBBAE-E005-46E0-B7E5-845882DB1ED8/InternetEncryption

single, stable, secure, and globally interoperable DNS by increasing the trust end users can place on the DNS.

6.1 Communication Privacy Is Good

Given the risks associated with on-path traffic eavesdropping, encrypting the communication between the computer and resolver should be considered a good practice. This is true even if the encryption is not authenticated (such as when using opportunistic encryption), even though unauthenticated communications are susceptible to on-path attackers intercepting traffic.

6.2 DNS Filtering Can Be Beneficial

DNS filtering, as a tool, can be helpful, particularly in the areas of reducing risk associated with phishing, malware distribution, spam, and other forms of abuse that leverage domain names. However, in most cases, this filtering should be done with the knowledge and acceptance (such as in the Terms of Service for the network operator) by the people impacted by the filtering.

6.3 Applications and Operating Systems Have Insufficient Information

Applications and operating systems typically don't know enough to make network control decisions such as split-horizon DNS, enforcement of legal mandates, and so on. It is thus important that the application or operating system obtain sufficient information, for example by operational heuristics or user interaction, before making decisions that may counteract network control decisions.

6.4 DNS Data Should Be Protected

DNS encryption, as discussed in this document, protects the communication channel between the computer and the recursive resolver. DNS encryption does not protect the data from the recursive resolver to the authoritative server, nor does it protect data resident in the recursive resolver. In order to protect the DNS data, DNSSEC validation should be deployed, ideally both at the recursive resolver (to protect data from the authoritative servers), as well as within the computer (to protect against data modification within the resolver's cache or between the resolver and the computer).

Appendix A. Further Discussion of Encrypted DNS

The following are places outside of ICANN where there are active conversations about the implications of encrypted DNS.

The DNS Privacy Project[13] publishes a great deal of information on DNS encryption and the issues related to it. The project is maintained by many experts in the DNS technical community.

The Encrypted DNS Deployment Initiative[14] focuses on large-scale adoption and operation of encrypted DNS. Its initial members include service providers, hardware and software vendors, and other organizations.

DNS encryption is discussed in many parts of the IETF. Because encryption technology is often implemented for local policy reasons, the technical discussions of how to encrypt DNS are often mixed with discussions of local and Internet policy. The discussions move from mailing list to mailing list over time, but the following are the primary lists at the time this is published:

- DNS Private Exchange (dprive)[15] – This working group standardized DoT. It is currently discussing operational aspects of DoT, as well as investigating using DNS encryption for communication between resolvers and authoritative servers.
- Adaptive DNS Discovery (add)[16] – This new IETF working group will deal with discovering servers that offer encrypted DNS resolution.
- DNS Over HTTPS (doh)[17] – This working group standardized DoH. It is still open, but is not actively discussing any work.

[13] See https://dnsprivacy.org/
[14] See https://www.encrypted-dns.org/
[15] See https://datatracker.ietf.org/wg/dprive/about/
[16] See https://datatracker.ietf.org/wg/add/about/
[17] See https://datatracker.ietf.org/wg/doh/about/