DOH
Internet-Draft
Intended status: Informational
Expires: September 11, 2019

J. Livingood
Comcast
M. Antonakakis
Georgia Institute of Technology
B. Sleigh
BT Plc
A. Winfield
Sky

March 10, 2019

# Centralized DNS over HTTPS (DoH) Implementation Issues and Risks draft-livingood-doh-implementation-risks-issues-02

## Abstract

The DNS over HTTPS (DoH) protocol is specified in RFC8484. This document considers Centralized DoH deployment, which seems one likely way that DoH may be implemented, based on recent industry discussions and testing. This describes that implementation model, as well the potential associated risks and issues. The document also makes recommendations pertaining to the implementation of DoH, as well as recommendations for further study prior to widespread adoption.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 11, 2019.

## Copyright Notice

Table of Contents



## 1. Introduction

The DNS over HTTPS (DoH) protocol is specified in [RFC8484]. This document considers Centralized DoH deployment, which seems one likely way that DoH may be implemented, based on recent industry discussions and testing. This describes that implementation model, as well the potential associated risks and issues. The document also makes recommendations pertaining to the implementation of DoH, as well as recommendations for further study prior to widespread adoption.

## 2. Separating the Protocol from Implementation Issues

This document is not intended as a critique of the DoH protocol itself, which can be a valued addition to the Internet and appears to have many helpful uses. Rather, this document focuses solely on how DoH is now being implemented and/or might be implemented. Thus, in

no way should this document be read as critical of the DoH protocol itself, which can bring positive benefits to end user privacy.

In addition, conventional DNS generally uses UDP port 53, though in some cases TCP is used. DoH is still DNS but it uses an entirely different protocol to send and receive queries. This document does not delve into the particulars of the DoH protocol. For those details, please refer to [RFC8484].

## 3. Network Operators Are Interested in Deploying DoH

Network operators, ranging from ISPs to enterprises, schools, and others work hard to provide outstanding DNS and network performance, as well as to protect the security and privacy of users. In addition, most also provide DNS-based services such as opt-in parental controls for consumers or malware/security protection in enterprises, content filtering in schools, etc. These operators are also interested in adding support for DoH (as well as DNS over TLS, DoT). However, the current Centralized DoH implementation model does not appear to make it possible for these operators to continue to play a value added role in the delivery of network services, or to continue to provide DNS-related services, and may even cause problems beyond that.

In addition, the DoH resolvers that network operators might provide would likely not be open recursive resolvers but would instead mirror the current model whereby the resolver has an access control list (ACL) so that the servers only respond to clients on that network, which helps to reduce abuse (see the Open Resolver Project) [1]. This does not appear to be compatible with the current Centralized DoH implementation model that appears to assume that DoH resolvers are openly accessible from any network.

Finally, network operators also typically have a direct, trusted relationship with users, often bound by legal agreements including Terms of Service and a Privacy Policy. Depending upon the particular country/region there are laws and regulations, such as the General Data Protection Regulation (GDPR), that may also govern user privacy, data collection, and data handling. All of those things would apply to network operator DoH services as they do to conventional DNS services.

## 4. Centralized DoH Defined

DoH clients have been implemented in a number of platforms, including in the Mozilla Firefox web browser (see Mozilla blog) [2], and Google Chrome (Chromium) web browser (see Google Public DNS Developer web site) [3]. In deployments thus far, Mozilla has defaulted to

Cloudflare (see Mozilla blog) [4], and Google's Chrome browser have used Google Public DNS (see Google Public DNS Developer web site) [5].

Since directing DoH-based DNS traffic to a small number of commercial DNS providers represents a high degree of concentration and centralization of operation and control, this document describes this potential implementation model as "Centralized DoH".

## 5. Centralization vs. De-Centralization of Services

DNS is the most highly distributed global database on the Internet, with millions of people and organizations independently changing and adding to this database in a loosely coupled system. The web (HTTP/HTTPS) is also highly distributed, with countless parties creating and publishing content on the web. Both the DNS and HTTP protocols demonstrate the key architectural tenets of the Internet, such as loose coupling between systems and layers, loose coordination between different entities that use a particular protocol, and broadly de-centralized distribution of the protocol and associated systems.

But over the past decade, there has been a trend of most web traffic shifting towards a small number of very large web platforms. For example in 2009, Craig Labovitz described the rise of the so-called hyper-giants (see Arbor Networks report) [6], with 30 companies being responsible for 30% of global traffic. A subsequent paper from Harvard's Berkman Center [7] highlighted the security, independent media, and human rights implications of this development as a result of attacks against that small number of key platforms, among other issues. Many others have measured, studied, and debated this trend since 2009. A recent Sandvine paper [8] noted that Google's YouTube comprised 35% of mobile Internet traffic, and Netfix comprised 13.75% of global Internet traffic (see Sandvine blog) [9].

This trend towards centralization onto a small number of large platforms has given rise to efforts to "re-decentralize the web". Proponents of the effort to resist and reverse the further centralization of the web and the Internet more generally include Sir Tim Berners-Lee (see Ars Technica article [10], Gizmodo article [11], New York Times article [12]), Vint Cerf (see Archive.org blog [13]), Brewster Kahle (see IEEE Spectrum article [14]), MIT's Digital Currency Initiative [15], participants in the Decentralized Web summit [16], and others.

In addition, IETF contributors are also considering the challenges posed by consolidation, which in the DoH context is analogous to Centralized DoH. For example, the Internet Architecture Board (IAB) posted a draft entitled "Considerations on Internet Consolidation and

the Internet Architecture" [17] that delves into these issues, as also noted on the IETF blog [18]. The Internet Society also published their 2019 Global Internet Report on the Future of the Internet [19] that is primarily focused on consolidation.

While traffic to certain destinations is increasingly concentrated, at the same time the physical destinations (e.g. servers) are often highly distributed by these platforms in order to deliver good performance to users around the world. But while edge servers may remain relatively physically distributed, their control, administration, and operation is still centralized. But even if a Centralized DoH provider's physical servers are highly distributed it still would not come close to wide distribution of conventional DNS today, which is typically distributed down to the network level, ranging from a local region of an ISP's network (e.g. metropolitan London area) to a small business' local area network (LAN), enterprise network, school LAN, etc.

There are many potential implications to increased centralization and consolidation of the DNS. These can include technical, business, and other implications and risks that are explored later in this document in Section 8 and Section 9.

## 6. Centralized DoH Assumption: Enabled/Centralized by Default

This document assumes a potential Centralized DoH environment where a few large scale implementers have enabled DoH by default. This means that there are assumed to be a small number of Centralized DoH providers, rather than a large number of distributed DoH resolver providers and in stark contrast to the highly distributed nature of the DNS today. This is explored further in Section 5. While each implementer has so far configured DoH off by default, and users can opt-in, the apparent design target of some or all key implementations is to enable Centralized DoH by default at some point in the future (see Internet Society blog [20]. Thus, the current opt-in model is assumed to be temporary.

## 7. Potential for Rapid Centralized DoH Adoption

Implementation of some new protocols, such as IPv6 (see World IPv6 Launch site [21], Wikipedia article [22], LinkedIn blog [23]) or DNSSEC (see DNSSEC deployment history [24]), depended upon broad community technical coordination, extensive open measurement, extensive technical discussions over several years, and gradual adoption. But adoption of IPv6 and DNSSEC grew organically over time in part due to the wide variety and great number of parties that needed to independently take action to adopt those protocols. In contrast, there are far fewer major web browsers and operating

systems than network operators, websites, authoritative domain name server operators, and so on.

The result of this comparatively greater concentration is that if just two organizations implement DoH, then the adoption of Centralized DoH could increase quite rapidly, and quickly overtake and displace conventional non-DoH DNS query traffic. It appears to be unprecedented that a new protocol could be so rapidly deployed and thus displace an existing, long-standing, highly distributed protocol based on implementation by just two implementers.

This extraordinary potential for rapid Centralized DoH deployment alone suggests the need for a high degree of testing, discussion, and consensus in the global Internet community that is broader than the much more limited consensus necessary for adoption of proposed IETF standards.

To illustrate the potential for rapid Centralized DoH, if just two organizations, Google and Mozilla, were to implement Centralized DoH in Android, Chrome, and Firefox, then global adoption of DoH could occur rapidly and represent the majority of DNS queries on the Internet.

All the above being said, it is important to note that this is not necessarily a criticism of the motivations of the potential Centralized DoH providers and that scale and market share are neither objectively good or bad attributes. Indeed, as IETF chair Alissa Cooper noted in an interview about consolidation with the Internet Society [25], "In some cases larger entities can have faster, broader, positive impacts on end users. Today, if one or a small handful of the largest web properties, content delivery networks, or email service providers chooses to deploy a new security technology or implement a performance-enhancing feature, those improvements can benefit millions or billions of users on short order."

Thus, on the one hand rapid adoption of new security protocols can be good and adoption can be hastened by the actions of a few key players. But it is important to also acknowledge that this may simultaneously be in tension with other goals for the design and operation of the Internet, requiring thoughtful consideration of the pros and cons and extensive discussion in the Internet community and elsewhere.

## 8. Potential Technical Risks

There are a variety of potentially significant risks to the security, stability, and performance of the Internet as a result of Centralized

DoH implementation, and resulting consolidation of DNS operations. These include the following potential and speculative risks:

1. Significant Operational Shift of Global Internet Infrastructure: Shifting from a large quantity of highly distributed DNS resolvers to a few centralized ones will likely have significant impacts on how the Internet operates, is administered, and how routine troubleshooting is performed. The full implications of such a significant and potentially sudden change require deep study by a range of actors across the Internet ecosystem.

2. Decreased Stability:
   Significant centralization can increase the fragility of a technical system, because there are fewer points of failure and thus the impact of any individual failure can be quite high. The net effect suggests that if DNS operations become significantly centralized as a result of DoH, then the stability of the DNS is likely to be negatively impacted. While not directly related to DoH, there are examples of widespread Internet outages when large DNS-related platforms experience technical faults or attacks, such as Cloudflare (see Cloudflare blog [26]), DynDNS (see Dyn blog [27]), and many others.

   Even without the advent of Centralized DoH, which appears to be a potentially significant concentrator of DNS traffic, a recent paper from Harvard University ( see Zittrain et. al., "Evidence of Decreasing Internet Entropy, The Lack of Redundancy in DNS Resolution by Major Websites and Services" [28]) raises concerns that may only worsen with DoH. They write, "We find an increasing concentration of DNS services in a small number of dominant cloud services companies. Coupled with domains apparent tendency not to employ DNS services from multiple DNS providers, this concentration could pose a fundamental threat to the distributed resilience of the Internet. Our results also suggest ways to mitigate these issues... The Dyn attack provides a vivid illustration of how DNS infrastructure vulnerabilities - and DNS space concentration - can wreak havoc on the stability of the Internet."

3. Increased Security Threats:
   Centralization due to DoH could mean a dramatic reduction in the number of recursive DNS operators. This seems likely to lead to fewer points of failure on which attackers can focus, potentially altering the return on investment (ROI) necessary for a large scale attack, compromise, or disruption to succeed. Such threats may include the outsized effect of Border Gateway

Protocol (BGP) hijacks (see Internet Society blog [29], Freedom to Tinker blog [30], CSO Online article [31], ZDNet article [32], Ars Technica article [33], Google whitepaper [34], Distributed Denial of Service (DDoS) attacks (see Dyn blog [35]), or regular Denial of Service (DoS) attacks made against a small number of systems.

4. Loss of Security Threat Visibility:
Some users will lose or have a degraded ability to use DNS blocklists, which are one of the primary and most effective ways to protect a network and its users against malware, phishing, spam, DDoS attacks, etc.

This is because there has long been a notion that as a network connects to the Internet, that the network can exercise some degree of local policy control, which remains local to that network and does not propagate beyond the boundary of their administrative domain. This includes monitoring and protecting the security of the network and devices on that network. Over time, one of the practices that has evolved and become widespread is the use of the DNS to monitor for, remediate, and/or prevent malware infection or other security problems. This functionality is deployed in many types of networks, from ISPs to networks used by enterprises, small businesses, government offices, schools, churches, libraries, and others. In some cases the DNS server may reside inside the network, while in other cases it may be external (aka cloud-based, such as OpenDNS). To illustrate this, many networks monitor the FQDNs of DNS queries for matches against lists of well-known malware command and control hosts. In some cases when matches occur, the device owner or local network administrator may be notified of a potential malware infection. In other cases, the DNS is configured to re-write the response for a query of a malware-associated FQDN, providing an address that points of a server alerting the end user of a malware risk, providing a NXDOMAIN response to cause the DNS lookup to terminate in failure, or other response. This functionality will fail if DNS queries bypass the servers that perform this function to Centralized DoH resolvers. Thus, Centralized DoH can create blind spots in this critical area of security threat visibility.

5. Loss of Parental Controls or other Content Controls:
Similar to using the DNS on local networks to monitor for and prevent security issues, the DNS is often used to implement local content controls such as parental controls. With these controls a parent can configure a service on their home network

to prevent children from accessing inappropriate or other disallowed content. For example, a parent may configure policies to bar their two children, aged 5 and 7 years, from accessing any sites associated with social media, gambling, illegal drug use, pornography, and so on. Such opt-in services are highly popular, especially because they can work across device types (e.g. PC and mobile) and device ecosystems (e.g. Android and Apple), software (e.g. Mac and Windows), and platform ecosystems (e.g. Google, Apple, and Amazon).

Similar to the malware example, this is usually implemented via DNS response matching and re-writing, with the end user presented with either a redirection to a content block page or receiving an NXDOMAIN response. This functionality will fail if DNS queries bypass the servers that perform this function to Centralized DoH resolvers. And while one suggestion may be that the Centralized DoH provider offer such services, this is not a choice users are being permitted to make. They may be perfectly satisfied with their current solution, not want to take the time to setup a new service, or not want to use the Centralized DoH provider for this function. In addition, mature and highly customizable parental control and content control systems that meet the needs of enterprises, schools, parents, and others do not appear to be offered by Centralized DoH providers. To the extent that similar solutions seem to exist, they appear to be very basic, and lacking in the customization and functionality that has developed in this marketplace over the last 20 years.

In addition, if users wish to configure their own independent DNS resolver that provides features such as parental controls, as many do today, this may become more complicated and varied with Centralized DoH to the extent that some software like browsers or other applications are over-riding configurations set by users in their operating system.

6. Split DNS Problems:

Split DNS [RFC8499] is an implementation in which separate DNS servers are provided for internal and external networks as a means of security and privacy management. This is most often used in enterprise, education, and government networks. In practice this means that there are names that only resolve on an internal network, or that resolve to special internal hosts for internal network users and publicly accessible hosts for users outside of the network. For example, an enterprise may have an internal service named "Accounting-System" reachable on the web via https://accounting-system or https://accounting-system.example.com, and connected to via internal, non-routable

RFC1918 IPv4 addresses such as 192.168.1.77. These domains or fully qualified domain names (FQDNs) are maintained only on a network's local DNS resolvers, and are not resolvable using the Internet's authoritative DNS infrastructure. These names will no longer be resolvable based on the expected implementation of DoH because the local resolvers that can provide a valid response for these names is no longer in the resolution path for the end user on that network - they are skipping past the local resolver to a centralized resolver on the Internet. It is certainly possible to criticize the use of split DNS, like Network Address Translation (NAT), but whether it is a supposedly good practice or not, it seems a pervasive practice nonetheless and should be considered by new DNS protocol implementations.

7. Enterprise Data Leaks:
When split DNS names are used, as noted in the above example for a user on an enterprise network attempting to connect to a host at https://accounting-system.example.com, the lookup with a centralized DoH resolver will typically fail (NXDOMAIN). But because the internal name was sent to the centralized DoH resolver, that private name has "leaked" outside of the local / enterprise network. Similarly, lookups of reverse DNS names (in-addr.arpa) will leak private IP addresses as well. The leak of IP address data could occur regardless of whether or not split DNS is used.

8. Potentially Reduced Software Diversity:
Consolidation of recursive DNS functions to a few Centralized DoH providers suggests that there will be fewer types of DNS server software over time, or at least that a very small number of DNS server software packages will account for the overwhelming volume of DNS traffic. This leads to less software diversity over time, which is in some cases considered a negative in this realm (see IEEE Explore paper [36], Freedom to Tinker blog [37]). This may also shift most DNS traffic away from platforms using open source software to proprietary software. In addition, the impact of any DNS software exploits (such as the BIND "packet of death" [38]) against the software used by the few key Centralized DoH operators seems likely to have an outsized impact on the global Internet.

9. Potential for Increased Commercial Use of DNS Data:
As a result of the highly distributed nature of the DNS today, and of recursive DNS operations specifically, there are

essentially no - or at least few - global data sets of end user DNS queries. The possible exception to that is for large public DNS operators that receive hundreds of billions of queries per day. But as Centralized DoH potentially leads to consolidation onto a few large platforms, very large DNS query datasets will emerge, which carries the risk that organizations will be tempted to or find it otherwise necessary or advantageous to make commercial use of that data. This might especially be the case of those operators that offer DNS services for "free". Furthermore, even if data sets are in some manner "anonymized", it seems likely that some organizations will possess enough other datasets that the combination of the two may trivially enable de-anonymization. See [Narayanan-Shmatikov-1], [Narayanan-Shmatikov-2], and [Narayanan-Shmatikov-3]. In addition, a user may be uncomfortable with or unhappy with having their DNS traffic sent to a pre-configured Centralized DoH with whom they have no relationship. As noted earlier in the document, this can be particularly problematic in light of the GDPR and other laws and regulations around the world.

10. Potentially Negative Impact on Content Delivery Network (CDN) Localization:

It seems there is some risk that some CDNs may be less able to provide good content localization with Centralized DoH, equivalent to the localization that they provide today. This is because CDN localization today depends upon accurately estimating the rough location from which client queries originate, whether derived from EDNS-Client-Subnet (EDNS0) [RFC6891] [RFC7871] or some other method employed by a CDN. This location information is then used to dynamically generate authoritative DNS responses that provide different responses based on that client location. The goal of the CDN is to provide highly localized responses, such as directing a client to content cached in their local city or region rather than that which is further away, such as across an ocean or across many networks.

The technical impacts of reduced CDN localization might include slower access to Internet content for end users and more traffic traversing backbone and sub-optimal peering points as opposed to localized points of direct interconnection between networks. It is difficult to estimate what, if any, the impact would be. But large-scale measurement platforms such as the SamKnows system that is used by many regulators around the world such as OFCOM and the FCC may be useful for exploring this further, as noted in Section 10.

11. Use of DoH for Malware Command and Control:
Related to the loss of security threat visibility, it seems clear that DoH is also now being used as a new and undetectable malware command and control channel. One example is DoHC DoHC2 [39]. As a result, from the perspective of a variety of networks, DoH is sometimes considered a security threat given its adoption as a covert malware command and control communications channel and thus may be considered a new avenue for abuse.

12. Disruption of Legally-Mandated National-Level DNS Blocks:
In an increasing number of countries, network operators are required by law to implement DNS-based blocking of names. Some democratic countries have developed laws and regulations in this area, including the UK, Sweden, Switzerland, France, Italy, Brazil, and others [CITATIONS NEEDED]. As a result, Centralized DoH resolvers appear unlikely to comply with these local laws and so legally-mandated national DNS blocks will become ineffective. National regulators may take a dim view of this and require that Centralized DoH resolvers comply with applicable national laws mandating DNS blocking. Whether or not national-level DNS blocking is either good, effective, or easily circumvented matters little; organizations operating within a given country are typically expected to comply with such applicable laws and so Centralized DoH resolvers will need to determine how to comply. (This point is not to be confused with the sorts of blocks that have historically been imposed on major content destinations by repressive political regimes and/or those with extensive censorship in place to limit or control speech.)

13. Potentially Negative Impact on End User Broadband Performance:
As noted above, it seems possible that the extent of localization of CDN-based content may decline somewhat. Should that be the case, this means that the performance or speed of access of CDN-based content will decline. Since most web content is CDN-based, this suggests the possibility that the general end user performance of the Internet will decline. An initial study by Mozilla [40] has suggested that the protocol itself (DoH vs. UDP/53 DNS) is roughly 5% slower. But that limited study only considers how fast it takes to get *an* answer, not how *local* or good that answer is from an end user perspective. More measurement is certainly necessary here, which can consider how local the answers are and what the end-to-end performance of web-based content is for users of centralized DoH vs. non-users.

14. Unknown Server-Side Performance and Scaling:
Many new protocols are implemented organically, which means the growth or adoption of the protocol is relatively gradual. As a result, software developers and system administrators have a longer period of time to learn about performance tuning and scaling, and to methodically test and deploy improvements, compared to a "flash-cut" sort of migration where a significant shift to the protocol or system occurs in a short period. In the case of the likely DoH implementation on which this document speculates, it seems a rapid shift is more likely. This raises the risk of instability and reduces the ability of technical personnel involved in development and deployment to learn and make technical changes gradually and with relatively minimal impact on systems and users due to relatively high levels of usage inherent in a flash cut or rapid migration scenario.

15. Increase in Exploits Targeting Individual DNS Engineers and Administrators:
Given the likely consolidation of most recursive DNS traffic to a very small number of operators, it seems logical to conclude that attackers will realize that a fairly small number of DNS engineering and operations/administration personnel (less than two dozen?) will control a key function of the Internet. As a result, it seems likely that a savvy attacker would target exploits such as spear-phishing [41] or advanced persistent threats (APT) [42] against this small number of people in order to gain access to systems that administer or control recursive DNS functions.

16. Increased Complexity and Cost of End User Troubleshooting:
Today, ISPs and other network operators can guide users through troubleshooting to determine, often via a simple command line interface, what DNS servers they have been assigned and what responses they are receiving from those resolvers. In the Centralized DoH model, determining what DoH servers are being used and testing responses from those servers seems likely to be relatively more complicated and varied. This could increase the complexity and cost of routine end user troubleshooting.

17. Disruption of ISP Walled Garden Functions and Other Captive Portals:
Many ISP networks utilize a DNS-based walled garden for customers to provision new service, to activate a new device, to re-establish an existing service after non-payment, and so on. It appears that Centralized DoH disrupts these widely used

functions, because the browser is over-riding the specially assigned walled-garden DNS server addresses and is instead attempting to use a Centralized DoH resolver. Similarly, other captive portals that may be affected include those to access WiFi networks on campuses, in airplanes and coffee shops, and so on. While new standards in the IETF's CAPPORT Working Group [43] may avoid this in the future, CAPPORT standards are still developing and/or are not widely deployed.

## 9. Potential Business Risks

New IETF standards are not introduced in a vacuum. Rather, IETF standards have real-world impacts on technologies, markets, and societies. As a result, potentially rapid shifts in adoption of these standards means that relevant IETF working groups cannot ignore potential real-world, technical and non-technical impacts.

If Centralized DoH is implemented quickly based on the business decisions of one or two organizations with significant operating system and/or web browser market share, with the resulting effect of greater centralization, then the following potential and speculative business risks are worth considering:

1. Smaller DNS Software Marketplace:
   The market for DNS server software may be disrupted, as default DoH resolver choices override typical DNS settings that direct DNS traffic today. As a result, the number of DNS server software developers may dwindle. This is because if ~70% of the world's DNS queries rapidly moves to two Centralized DoH resolver operators, then there is a diminished need for conventional DNS operators to continue to maintain their DNS infrastructure. This could impact DNS server software developers in both commercial and open source markets, such as Akamai, Cisco, CZ.NIC, Infoblox, PowerDNS, NLnet Labs, etc.

2. Fewer Public DNS Operator Choices:
   The market for public DNS resolution will likely be disrupted, as default Centralized DoH resolver choices override end-user-configured DNS settings. For example, an end user may configure their operating system to use a "public" DNS service that implements parental control functions. But when using their web browser, the browser sends its DNS queries - which are likely the great majority of queries from the user based on the prevalence of the web as an application - to a Centralized DoH resolver instead. After the adoption of these public DNS services declines dramatically, these organizations may struggle to

continue to justify the resources necessary to maintain the service. This could impact all those public DNS resolvers that are not the default partner of a Centralized DoH implementer (e.g. Cloudflare) or are not themselves DoH implementers (e.g. Google), such as Cisco's OpenDNS and Quad9.

3. Reduced CDN Localization and Competition:
The CDN market may be disrupted, as noted above, should some or most existing CDNs be less able to provide good content localization. This is because content localization is one of the key reasons an organization would purchase a CDN's services. So if this key reason goes away or is negatively impacted, there may be less demand for CDN services or the price of those services may decline as a result of reduced benefits to customers. This may also affect competition if some providers exit the market or alter their market behavior as a result.

4. Smaller DNS Labor Market:
The labor market for DNS engineering and operations expertise may also be disrupted. This is likely due to there being fewer independent developers of DNS software, as well as fewer recursive DNS operators, which can be expected to reduce the need for DNS technical resources over time.

## 10. Recommendations

This document makes the following recommendations:

1. Develop a Standardized DoH Resolver Discovery and Selection Mechanism:
[RFC8484] does not specify a mechanism to discover whether a DoH server is available as part of the local network configuration and configuration of the URI template used the construct the URL for resolution is explicitly stated as being out of band from the DoH protocol. Without such a discovery mechanism, there is little choice for DoH clients to use any other mechanism than pre-configured DoH servers, which by implication would be almost certainly be outside of the network of the ISP or other network operator, even if they offered a DoH service.

   There are efforts underway to discover and automatically associate a DoH server with a resolver, for example draft-ietf-doh-resolver-associated-doh [44]. Such configuration mechanisms, if adopted by DoH clients, would potentially ameliorate many of the issues with DoH deployment expressed in

this document, since it would provide a way for end-users to use the DoH server provided by the local network operator.

2. Conventional DNS Providers Should Begin Testing DoH:
ISPs and other network operators, as well as any other conventional DNS providers should begin to test DoH as a new protocol that will be added to their existing DNS services. In particular, it seems critical to develop appropriate, scalable, reliable, and cost effective deployment design that can deliver DNS resolutions at least at the level of performance that users expect of conventional DNS.

3. More Measurement is Needed:
Limited measurements collected thus far have been in some cases shared publicly, but the underlying datasets remain confidential and private. In the future, significantly more measurement data needs to collected, shared publicly, and debated in the Internet technical community. Past deployments of new protocols can be a guide here, such as measurements undertaken in support of the deployment of IPv6, such as World IPv6 Day and Launch [45].

4. Defaults Matter - Consider Them Carefully:
Make opt-in by default during initial deployment. Off by default is less risky for initial deployment. That should likely remain so until there has been significantly more technical testing, global measurement, and Internet community consensus-building.

5. Internet Corporation for Assigned Names and Numbers (ICANN) Review:
ICANN coordinates and/or administers key Internet functions, such as the Internet Assigned Numbers Authority (IANA) and the global Domain Name System (DNS). ICANN maintains a group of technical experts in the SSAC [46] that advises the ICANN Board and community on the security and integrity of the Internet's naming and address allocation systems, including domain name operations, administration, and registration. Given that SSAC focused on threat assessments and risks related to the stability and security of the DNS, they seem like one appropriate party to assess some of the risks that have been briefly explored in this document or other DoH implementation-related risks and issues.

6. Additional Expert Reviews:

In addition to the ICANN SSAC, several other organization to be appropriate parties that are well situated to assess risks and issues as they pertain to those organizations or their members/ participants. They include, but are not limited to:
- DNS Operations Analysis and Research Center (DNS-OARC)
- Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG)
- Network Operator Groups (NOGs), such as the African Network Operators Group (AfNOG), Australian Network Operators Group (AUSNOG), Caribbean Network Operators Group (CaribNOG), Latin American and Caribbean Region Network Operators Group (LACNOG), North American Network Operators Group (NANOG), Pacific Network Operators Group (PACNOG), Reseaux IP Europeens Network Coordination Centre (RIPE NCC), Slovenian Network Operators Group (SiNOG), etc.
- DNS registries outside of ICANN, such as Council of European National Top-Level Domain Registries (CENTR).

7. Detailed Community Assessment of Risks and Issues:
All of the risks in Section 8 and Section 9 should be assessed. In addition, when a change needs to happen to a protocol or a system, it seems important to debate a few other key things such as:
- What is the threat model that makes this change important enough to justify?
- What are the security and privacy implications of this change?
- What are the implications for stability, operations, network and systems administration, software development and diversity, and other key issues?
- Do the benefits outweigh the drawbacks?
- What alternatives should be considered or developed?

8. Continue to Focus on DNSSEC Adoption:
To the extent that one of the underlying concerns motivating DoH adoption pertains to modification of DNS responses via man in the middle attacks, it seems that DNSSEC signing of domain names and DNSSEC validation (including in clients) may be able to mitigate that issue. DNSSEC remains important because DoH, whether centralized or distributed, only provides security for the transmission of DNS queries/responses over the wire (in transit, or channel security), and does not provide assurance that the response itself is secure and unmodified (content security). This issue is explored in more detail in an APNIC blog [47] and an ICANN presentation [48].

9. Conduct Enterprise, Education, and Government Network Testing:
   This documents several issues related to these non-ISP types of networks. Additional testing should be conducted by these entities in order to document actual and/or potential issues, including the extent or severity of those issues, and provide that feedback to appropriate standards and industry groups.

10. DoH Client Software Developers Should Investigate Region-Specific Differences:
    DoH can improve user privacy, especially in certain countries/regions with known surveillance and/or manipulation of DNS queries and other data, which can pose human rights risks in these areas. But many other countries/regions have more privacy-protective expectations, rules, regulations, and laws. It may be worthwhile for DoH client software developers to consider developing application logic that enables Centralized DoH in the high risk areas, while not leveraging DoH or leveraging a distributed approach to DoH in the low risk areas.

11. Develop Centralized DoH Data Privacy Guidelines/Frameworks:
    Assuming Centralized DoH is a viable model for implementation of DoH, what sort of measures are needed to limit the potential for problematic behavior by Centralized DoH providers? Should there be a code of conduct (or equivalent) and, if so, who will develop/maintain that? Likely topics for some guidelines or framework might include how DoH client data may be collected, retained, processed, shared, monetized, and/or combined with other data sets, etc., whether and what limits there may be on generating unique-per-used FQDNs, whether and what limits there may be on web-related cookies/tracking mechanisms, detection of DoH servers that return bogus or bad/false data, policy statements from DoH providers on how client data is used, measures to ensure DoH client data is suitably anonymized to minimize the risk of re-identification of individuals by combining DoH data with other data sources, etc.

## 11. Document Reviewer Acknowlegedments

The authors thank the several individuals for performing a detailed review of this document, noting that this acknowledgement is not intended to imply that they endorse the document. We specifically wish to thank: Greg Aaron, Rob Alderfer, Bill Check, Neil Cook, Joe

Crowe, Glenn Deen, Andy Fidler, Peter Hagopian, Paul Hoffman, Yiu Lee, Jim Reid, and Ralf Weber.

## 12. IANA Considerations

RFC Editor: Please remove this section before publication.

This memo includes no requests to or actions for IANA.

## 13. Security Considerations

This document does not introduce any new security considerations. However, it does highlight a number of potential security considerations related to how [RFC8484] might be implemented in the future, especially Centralized DoH. For example, an attacker could substantially disrupt the global Internet by targeting one or two major platform providers. See Section 8 for more information.

## 14. Privacy Considerations

This document does not introduce any new security considerations. However, it does highlight a number of potential privacy considerations related to how [RFC8484] might be implemented in the future, especially Centralized DoH. For example, with Centralized DoH there will be a small number of large commercial platforms that have an extensive business collecting and leveraging user-related data that could extend and augment these data sets as a result of the data they can collect by handling the majority of global DNS traffic. See Section 9 for more information.

## 15. References

### 15.1. Informative References

[Narayanan-Shmatikov-1]
Narayanan, A. and V. Shmatikov, "Robust de-anonymization of large sparse datasets", IEEE Security and Privacy 2008, 2008.

[Narayanan-Shmatikov-2]
Narayanan, A. and V. Shmatikov, "De-anonymizing social networks", 2009 30th IEEE Symposium on Security and Privacy 2009, 2009.

[Narayanan-Shmatikov-3]
Narayanan, A. and V. Shmatikov, "Myths and fallacies of personally identifiable information", Communications of the ACM 53.6, 2010.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

[RFC7871] Contavalli, C., van der Gaast, W., Lawrence, D., and W. Kumari, "Client Subnet in DNS Queries", RFC 7871, DOI 10.17487/RFC7871, May 2016, <https://www.rfc-editor.org/info/rfc7871>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

## 15.2. URIs

[1] http://openresolverproject.org/

[2] https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/

[3] https://developers.google.com/speed/public-dns/docs/dns-over-https

[4] https://blog.mozilla.org/futurereleases/2018/11/27/next-steps-in-dns-over-https-testing/

[5] https://developers.google.com/speed/public-dns/docs/dns-over-https

[6] https://xconomy.com/boston/2009/10/20/arbor-networks-reports-on-the-rise-of-the-internet-hyper-giants/

[7] https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf

[8] https://www.sandvine.com/blog/youtube-rules-mobile-2019-mobile-internet-phenomena-report-released

[9] https://www.sandvine.com/blog/global-internet-phenomena-worldwide-and-regional-total-internet-traffic-share-video-and-file-sharing-are-tops

[10] https://arstechnica.com/tech-policy/2014/02/tim-berners-lee-we-need-to-re-decentralize-the-web/

[11] https://gizmodo.com/the-web-s-creator-now-wants-to-unfuck-it-1781260559

[12] https://www.nytimes.com/2016/06/08/technology/the-webs-creator-looks-to-reinvent-it.html

[13] https://blog.archive.org/2016/06/16/decentralized-web-summit-with-tim-berners-lee-vint-cerf-and-polyfill/

[14] https://spectrum.ieee.org/view-from-the-valley/telecom/internet/brewster-kahle-on-whats-next-for-the-decentralized-web-movement

[15] https://dci.mit.edu/decentralizedweb/

[16] https://decentralizedweb.net/

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

[18] https://www.ietf.org/blog/consolidation/

[19] https://www.internetsociety.org/globalinternetreport/2018/concept-note/

[20] https://www.internetsociety.org/blog/2018/12/dns-privacy-support-in-mozilla-firefox/

[21] https://www.worldipv6launch.org/

[22] https://en.wikipedia.org/wiki/World_IPv6_Day_and_World_IPv6_Launch_Day

[23] https://engineering.linkedin.com/blog/2018/06/celebrating-ipv6-launch-day

[24] http://www.dnssec-deployment.org/history/

[25] https://www.internetsociety.org/blog/2019/02/future-thinking-alissa-cooper-technical-impact-internet-consolidation/

[26] https://blog.cloudflare.com/today-we-mitigated-1-1-1-1/

[27] https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

[28] https://www.hbs.edu/faculty/Pages/item.aspx?num=53830

[29] https://www.internetsociety.org/blog/2018/05/what-is-bgp-hijacking-anyway/

[30] https://freedom-to-tinker.com/2018/04/11/routing-attacks-on-internet-services/

[31] https://www.csoonline.com/article/3320996/possible-bgp-hijacking-takes-google-down.html

[32] https://www.zdnet.com/article/persian-stalker-grayware-targets-telegram-instagram-users/

[33] https://arstechnica.com/information-technology/2018/04/suspicious-event-hijacks-amazon-traffic-for-2-hours-steals-cryptocurrency/

[34] https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf

[35] https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

[36] https://ieeexplore.ieee.org/document/4768648

[37] https://freedom-to-tinker.com/2004/02/19/monoculture/

[38] https://www.nominet.uk/the-packet-of-death/

[39] https://github.com/SpiderLabs/DoHC2

[40] https://blog.nightly.mozilla.org/2018/08/28/firefox-nightly-secure-dns-experimental-results/

[41] https://uk.norton.com/norton-blog/2016/12/what_is_spear_phishi.html

[42] https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

[43] https://datatracker.ietf.org/wg/capport/about/

[44] https://datatracker.ietf.org/doc/draft-ietf-doh-resolver-associated-doh/

[45] https://www.worldipv6launch.org/measurements/

[46] https://www.icann.org/groups/ssac

[47] https://blog.apnic.net/2018/08/17/sunrise-dns-over-tls-sunset-dnssec/

[48] https://www.icann.org/en/system/files/files/presentation-sunrise-dns-tls-sunset-dnssec-13jul18-en.pdf

## Appendix A. Change Log

RFC Editor: Please remove this appendix before publication.

- -00: First version published
- -01: Fixed formatting issue with title at top of each page
- -02: Removal of 2 ICANN-related recommendations that don't appear applicable

## Appendix B. Open Issues

Section will be removed before final publication

- Citations are needed in the legally-mandated DNS blocking section.
- Improve the formatting of extended quotations.

## Authors' Addresses

Jason Livingood
Comcast

Email: jason_livingood@comcast.com

Manos Antonakakis
Georgia Institute of Technology

Email: manos@gatech.edu

Bob Sleigh
BT Plc

Email: bob.sleigh@bt.com

Alister Winfield
Sky

Email: Alister.Winfield@sky.uk