dnsop
Internet-Draft
Intended status: Informational
Expires: May 6, 2021

A. Fidler
BT plc
B. Hubert
OpenXchange
J. Livingood
Comcast
J. Reid
RTFM llp
N. Leymann
Deutsche Telekom AG

November 2, 2020

DNS over HTTPS (DoH) Considerations for Operator Networks
draft-fhllr-dnsop-dohoperator-00

Abstract

The introduction of DNS over HTTPS (DoH), defined in RFC8484, presents a number of challenges to network operators. These are described in this document. The objective is to document the problem space and make suggestions that could help inform network operators on how to take account of DoH deployment. This document also identifies topics that may require further analysis.

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 May 6, 2021.

Table of Contents

1. Introduction

Traditional DNS traffic between stub resolvers, recursive servers and authoritative servers is not encrypted. This can pose a privacy challenge for Internet users, because their access to named network resources can potentially be tracked through their DNS queries. In

principle, any network element along the path between the user and resolving or authoritative servers could observe this unencrypted traffic. DoT (DNS over TLS) [RFC7858] is one proposal for providing privacy of DNS queries and DNS over HTTPS (DoH) [RFC8484] is another. Both DoH and DoT encrypt the communications between the end client (user) and recursive resolver. Plaintext DNS traffic between recursive and authoritative servers is generally less of a privacy concern because it usually does not contain information such as the source address of the initial query that could identify the end client.

2. Terminology

DoH Server: A server supporting the DNS over HTTPS is called a "DoH server" to differentiate it from a "DNS server" (one that only provides DNS service over one or more of the other transport protocols standardised for DNS). Similarly, a client that supports the DNS over HTTPS is called a "DoH client".

Do53: DNS over port 53 - conventional plaintext DNS. Do53 server and Do53 client are the respective terms for a server or client that uses conventional port 53 DNS.

Operator: A large Internet service provider, typically a cable company or fixed/mobile telco with a national or international network.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Contrasting DoH and Conventional DNS

With conventional DNS (Do53), using UDP or TCP port 53, most users are assigned the IP addresses of several recursive resolvers via DHCP or similar network bootstrapping mechanism. These are usually the IP addresses of recursive resolvers that are administered by the network operator. Although there is currently no equivalent to this for DoH, the ADD Working Group is developing solutions for DoH server discovery.

Users sometimes also change to third-party recursive resolvers. In some cases, they may even operate their own local resolver. It is not yet clear how or if DoH will be applied in these scenarios more generally. Current DoH behaviour of the most widely used web browsers is documented and reasonably well understood. The same cannot yet be said for operating system software: stub resolver libraries and web toolkits for instance.

RFC 8484 defines the protocol for DNS over HTTPS (DoH). When DoH is used, client and server DNS traffic is encrypted using a TLS RFC 8446 [RFC8446] channel, typically to port 443. DoH clients will have little need for conventional DNS apart from an initial bootstrap query to find the IP addresses of a suitable DoH server. In some cases, this will mean the bulk of the client's DNS resolver traffic bypasses an operator's DNS resolver infrastructure because that traffic uses the resolver service provided by a third-party DoH server.

When DoH is used, the traditional DNS client-server model of clients making queries and waiting for a reply from a server might well change. It can be expected that DoH servers will sometimes use DoH opportunistically. For instance a web server could include application/dns-message elements in the returned HTML data, anticipating the domain names that the web browser might need to resolve before rendering some web page. In this scenario, the browser would not need to lookup those names with DoH or conventional DNS because the relevant DNS data have already been supplied.

DoH is already widely implemented and deployed by browser vendors. All the major web browsers support DoH. Sometimes, DoH is enabled by default. In others, configuration changes are needed to get the browser to use DoH instead of conventional DNS.

Since DoH is not yet natively supported by the most widely-used DNS implementations, DoH servers may need some sort of proxy or "shim" module to convert between application/dns-message elements in HTML and conventional DNS queries and responses. A number of organisations are already offering public DoH resolution service, typically using anycast technology. Some operators have either deployed or are planning to deploy DoH resolver service in their networks.

DoH changes the current, well established business model where an end user (customer) pays for Internet connectivity and recursive DNS service is part of that offering from the ISP. When DoH is used, the customer may be dependent on DoH servers operated by third parties and have no contractual or business relationship with those providers. It also cannot be assumed that these DoH servers will be operating under the same policy and regulatory conditions that are applied by the end user's ISP.

4. Regulatory and Policy Considerations

4.1. Local Policy Constraints

Operator networks often have local policy constraints which require some form of DNS blocking or rewriting - for example to offer customers parental controls, to restrict access to illegal content or to mimimise end user exposure to malware, phishing attacks and so on. These tend to be implemented by using data from threat intelligence providers, usually some sort of RPZ feed that is incorporated into the configuration of the operator's DNS resolver infrastructure.

It is not yet clear how or if this functionality can be made available by DoH servers. These protective measures will be less effective once DoH is used because end user DNS traffic will largely bypass the operator's DNS infrastructure, rendering such content and security protections useless. Some of these measures may be offered by some DoH servers, but as yet there is no defined mechanism to ensure that all local policy is implemented.

4.2. Regulatory and Legal Impacts

Operators can also be required to perform DNS blocking and filtering or rewriting for legal reasons: handling takedown notices or complying with court orders. This may also be necessary for operational and/or security reasons such as dealing with botnets and DDoS attacks. [CSRIC]

As before, it is not yet clear how or if DoH servers will provide this functionality. Some of these measures may be offered by some DoH servers, but there is no defined mechanism to ensure that all local policy is implemented, particularly those required in certain jurisdictions today. Current protective measures may be less effective once DoH is used because customer DNS traffic will be able to bypass the operator's DNS infrastructure.

Conventional recursive DNS services are generally located in the country where an operator is based. Since third-party DoH service providers are likely to be based and/or operated from outside those local countries, different protections and regulatory considerations may apply to the protection, storage and processing of user data processed on those servers. Typical regulations that could apply include General Data Protection Regulation (EU) 2016/679 [GDPR] and the EU-US Privacy Shield Framework [USPS]. These can sometimes have global scope - GDPR for instance. Overseas regulations may have lower, higher or even no commitments governing such services compared to those that would apply to a local operator. The potential impact of these regulatory obligations with respect to DoH services is unclear, including whether or not they apply or even could be applied at all.

4.3. Regulatory Constraints

Logs containing individual DNS queries and the IP addresses or other data correlating those queries to specific users or homes may in some legal jurisdictions be considered as Personal Data or PII, Personally Identifying Information. In such jurisdictions detailed DNS query logs may be subject to data protection and retention regulations, or other legal and/or compliance requirements.

Operators can also be subject to regulation or other legal instruments that require DNS query logs to be retained for a certain period of time and made available for law enforcement purposes as needed, such as under a court order or other legal process.

Since DoH potentially bypasses conventional DNS resolvers on which these privacy, regulatory, and legal requirements are imposed, it will reduce or eliminate the potential social value of these rules, and may even be viewed by some countries as a potential breach of regulatory compliance (whether by ISPs, DoH server operators, or others).

5. Network Operations

5.1. Impact on DNS query logging

Analysis of resolver query data is an important task in most operator networks. This can help with traffic management, load balancing and capacity planning as well as network and user security. Widespread uptake of DoH will mean an operator has reduced visibility of the DNS traffic in their network. Query traffic logged by traditional resolving servers will be less representative (or even completely unrepresentative) of the overall DNS activity in an operator's network.

5.2. CDN endpoint selection

End user queries made with DoH could mean that lookups return answers that are sub-optimal. i.e. directing clients to a distant CDN node that is outside the operator's network instead of to the localised CDN node(s) installed inside that network or directly interconnected with that network. Those DNS responses would be keyed on the source IP address of a resolving DoH server, possibly operated by a third party, rather than an address of one of the operator's resolving DNS servers or end client IP address information that those resolving servers might choose to provide through the Client Subnet EDNS0 option RFC 7871 [RFC7871].

The impact to an operator of directing clients to a distant CDN node that is outside the operator's network is not only slower access to resources provided by the CDN. It also incurs higher costs for the operator because traffic is routed over the operator's backbone and peering links rather than remaining within a part of the network that is geographically or topologically close to the end-user.

Additionally, operators have powerful technical, operational and business incentives to provide optimal user experience for their customers, particularly in terms of latency and speed of Internet services. This involves working with multiple CDN and content providers to ensure best performance when delivering those services, for example by providing Client Subnet EDNS0 option information. One risk is that DoH services could be provided by operators or distributors of web content who have different motivations. For instance a provider of DoH service may choose to offer fast access to the content that they host or distribute, but may decide not to offer the geographic information of the end-user (for privacy, policy or business reasons) to competing content providers/distributors.

5.3. Redirection for captive portals

Network operators also often use captive portal DNS to provide customer self-service activation and related customer account provisioning, billing and support activities. For example, captive portal DNS is used extensively to support functions such as self-service provisioning of customer owned and managed Customer Premises Equipment (CPE), service support, mobile pay as you go top up and access to national/regional WiFi hot spots. DoH traffic may bypass these operator-supplied functions that are essential for managing the network. This would significantly disrupt the manner in which networks are operated and managed.

5.4. Managed network services

The provision of managed network services, for instance to corporate or other enterprise clients will be affected by DoH. It could negatively affect bring-your-own-device policies which might introduce devices into these networks that are configured to use third party DoH servers. For instance there is a risk that internal domain names used extensively in such networks could leak to external DoH servers, presenting obvious privacy and security issues.

5.5. Resolver capacity management

Large operator networks are likely to operate their own DoH servers because of local policy or business considerations. This could mean an increase in TCP-based DNS traffic to port 443 as DoH displaces

conventional UDP-based queries to port 53. Transitioning from a primarily UDP-based service to TCP-based DoH would likely require substantial network capacity enhancements to an operator's DNS infrastructure. This might also require changes to existing load balancing and failover architectures. Establishing a DoH service in these environments would absolutely impact operational management and support.

It is unclear how much end-user DNS traffic will migrate to DoH and how quickly that happens since this will depend on the uptake of DoH-capable applications. There is also uncertainty about the default behaviour of these applications, for instance try DoH first then fall back to conventional DNS, use DoH only, try DoH and DNS in parallel and accept whichever answers first, etc. These unknowns have a further obvious impact on capacity planning and network operations.

5.6. Discovery considerations

Some networks offer DNS resolution services on locally scoped addresses that are not globally meaningful - for instance RFC1918 or link-local addresses. This arrangement is commonly found in operator and enterprise networks. Discovery of DoH servers (or other forms of encrypted DNS transport) in these environments is likely to rely on bootstrapping from a locally-addressed Do53 resolver to the chosen DoH server. That DoH server could either be offering resolution service at the same local address as the Do53 resolver, or at a different, possibly global, address. Both options need to be considered. In both cases the DoH server would offer a TLS certificate proving ownership of a name. This name should be meaningful to the end client, conveying the identity of the resolver operator. However given the lack of network authentication it does not currently seem possible to mandate a requirement that the name has to match anything that could be present in the client's configuration.

Many network operators use stub resolvers or proxies in CPE to handle end-user DNS requests. Depending on how the network is organised, these stub resolvers and proxies can either present public or private IP addresses to client devices. When these CPE devices use private IP addresses, it will complicate encrypted DNS discovery.

5.7. Failure recovery

It is not clear how DoH services will affect customers' approach to disaster recovery and fault reporting or influence their business continuity planning. For instance, if a client loses connectivity or access to their chosen DoH provider(s), they may lose Internet service even though they remain connected to the operator's network

and could otherwise use conventional DNS resolution services. It is assumed, but cannot be guaranteed, that DoH-capable applications will fall back to conventional DNS whenever DoH service fails. Applications might however be configured to only use DoH apart from an initial bootstrapping query that uses conventional DNS.

5.8. Impact on Network Address Translation

Techniques such as DNS64 [RFC6147] and NAT64 [RFC6146] are widely used for devices with IPv6-only transport, particularly in mobile networks to ensure continued access to parts of the Internet that are IPv4-only. These generally require the operator's DNS resolver server to carry out some form of IP address mapping. It is not known what impact DoH will have in these environments. It is unlikely that this will work with third party DoH providers because they will not have information about the operator's network that would allow them to map these IPv6 addresses.

In networks where the translator prefix is not the well-known prefix defined by RFC6146, the client's use of a DoH resolver outside the operator's network will prevent access to IPv4-only content, because the resolver will not know the correct prefix to use in its response. Even when the well-known prefix is used, the DoH resolver may not be configured to correctly use it in its response.

5.9. Load balancing and failover

Operator networks make extensive use of DNS-based solutions for load balancing and service failover. These might not work as expected with DoH clients which bypass the operator's DNS resolver infrastructure. Further operational problems may arise if stale DNS data are held in a DoH client's cache.

6. User Support

- Adoption of DoH is likely to decouple DNS from the provision of Internet connectivity. For most users, DNS resolution is currently part of the service provided by their ISP. With DoH, users can be expected to rely on DoH service providers and are likely to have no business or contractual relationship with those providers.

- Getting meaningful consent from users - how?

- The role of user consent and whether it is a necessary factor in the processing of user data is contextual. It depends on the nature of relationships between the involved parties - largely the ISP, the DoH provider(s) and the end user - and how those

relationships were established. Prevailing legislation and regulation such as GDPR can also be an important consideration, albeit one that is obviously out of scope for an IETF document. It is not clear whether reconfiguration of a device or moving it from one network to another would constitute implied consent in a legal sense.

- In any case, only a fraction of Internet users understand the mechanics of DNS resolution, which makes obtaining informed and meaningful consent difficult. Service providers should seek to explain data use in a way that's understandable to most people. Sustained and collective efforts by service providers to educate users (policymakers, legal scholars, teachers, etc.) about the Internet infrastructure to foster common understanding of these issues would be helpful.

- How will users be able to opt in/out of DoH services?

- Users may want to give meaningful consent to use DNS filters. Therefore, there should be an option for users to enable and disable DoH with neither behaviour assumed. Such permissions should also apply to DoH queries made by web-based apps using an API, not just the queries directly entered by the user. When users do provide consent for DoH-related data processing, the architecture must also support the ability for them to withdraw this consent at any time.

- How do users select their "trusted" DoH Provider? i.e. How is a user or application supplied with a list of DoH providers? How does it choose between them and what are the selection criteria? Presumably these could/should be considerations for the ADD Working Group.

- Clarification is needed on trusted certificate approach, e.g. is it enforced at application rather than the kernel/operating system layer?

- Can/should discrete apps be able to choose their own DoH server? Suppose a banking app is configured to use the bank's DoH provider. Can that default be over-ridden? Should it?

- How does a user get told about (and approve) a change of DoH service for a phone/tablet when they're roaming between mobile telcos or using whatever DoH service is offered in $coffeeshop?

- How is an operator expected to support the customer or troubleshoot problems caused by accidental or intentional change of DoH server? If the DoH provider deletes all their historic DoH

traffic, how do they support the ISP customer regarding troubleshooting?

- How will DoH provisioning take account of existing customer parental control/malware protection settings and flag the consequences of selecting a new provider on these?

- How will browsers/applications explain DoH/DNS options to customers so that they can make an informed decision, as many will not appreciate what DNS is. If they select a third party DoH provider, that may bypass their existing network operator's content and malware protection controls. The end user will presumably need to set these up again with their new DoH provider.

- How to explain to customers that they may need to check/contact both their DoH provider(s) and network provider to resolver performance and outage issues.

7. Provisioning

- If some list or registry of "trusted" DoH servers is needed, who/what is going to maintain this and manage it? What criteria and procedures are needed for adding or removing entries from that list? How does a DoH provider become trusted or become untrusted?

- What are the requirements to become a DoH trusted recursive resolver? Will browsers or applications only show global or application-specific DoH provider options? How can regional network operators offering DoH just to their customer base be supported? How will browsers and applications know which regional or local options exist and which of these should and should not be honoured?

- An industry approach for DoH discovery, trust and selection that operates in an open and transparent manner is needed. This should give the customer meaningful consent options.

- How to configure CPE and other edge devices (e.g. smartphone) to use the operator's chosen DoH provider.

- Can/should the operator's or application's choice of DoH server be overridden by the customer?

- How do web applications get to specify the DoH server they want? If web apps get to choose the DoH server, they could be pointing to a malicious server (security issue) or allowing a DNS provider other than that defined by the user to see the DNS queries (privacy issue).

- How will DoH provisioning and discovery take account of existing customer parental control/malware protection settings and flag the consequences of selecting a new provider on these?

- If a browser or other edge device can do DoH, what determines if the DoH is the preferred the choice?, e.g. if CPE or set top box devices also supports DNS over TLS, should DoH be an option? If multiple options for DNS resolution are available, what decision process is used to make the customer recommendation and how is this trusted?

8. Privacy Concerns

Compared to traditional DNS, DoH offers more privacy protection against passive surveillance because requests and replies are carried over an encrypted channel. DoH offers an equivalent amount of privacy protection against passive surveillance as DoT does because both rely on TLS for their security properties.

Content Delivery Networks use techniques like EDNS-Client-Subnet (ECS) to return DNS answers that direct a client to an optimal location, for instance the CDN's node in the operator's network which serves the end user. DoH has the potential to be more privacy intrusive than ECS, largely because DoH is based on HTTP and can leverage the rich per-user and per-device tracking that pervades the web today. The implications of that are not yet well understood.

A DoH server will have a direct HTTPS connection to the client, assuming there are no middleboxes in the path between them. That could for example enable DoH servers operated by CDNs to carry out much more fine-grained redirection and content delivery, perhaps even on a per-user or per-user-session basis. They would be able to serve content and advertisements based on the end user's choice of operating system, their browser and that browser's configuration in addition to the client's source IP address, web cookie data, or other factors as is prevalent on the web today.

Global DoH providers will have access to significantly more DNS query data, and therefore be able to perform richer big data analytics, combining these insights with those obtained from other global platforms (search engines, operating systems, browsers, ad trackers, analytics services, web sites, mobile apps, payment systems, e-commerce platforms, social networks, Bluetooth beacons, etc.), potentially leading to a poor privacy outcome for consumers.

The DoH provider may adhere to different privacy policies than the operator's DNS service, particularly where they are located in

different jurisdictions. This may lead to better or worse privacy outcomes for users.

Operators in some jurisdictions are required to perform DNS filtering functions on traditional DNS queries and responses. If this functionality has to be provided using DoH, the only available option may be to fully proxy the HTTPS traffic. That represents more of a privacy intrusion than filtering alone.

It is feasible that individual applications might have the ability to select their own DoH server, bypassing the system- or operator-defined DoH settings. That could lead to privacy violations because DoH queries get sent to an arbitrary DoH server with unknown privacy policies.

If users have no relationship with the DoH provider handling their queries, they may have limited ability to exercise data protection rights (erasure, objection, complaints, etc) or to pursue remedy for breaches. This may be further complicated if the provider is unknown to the end user, can't be easily contacted or is located in another jurisdiction.

9. Security Considerations

DoH will give new opportunities for bad actors to propagate malware, spam and botnets. Once they use DoH, as some botnets have already started doing for command-and-control traffic, their DNS traffic will be encrypted and anonymised, making it hard to deploy countermeasures to protect against and mitigate these serious security threats. This is likely to have an adverse impact on cybersecurity both at a network/country level as well as for end users. Use of DoH could make it slower to identify DNS-based DDoS attacks, more difficult to attribute patient-zero for malware infections and harder to block access to botnet command-and-control nodes. A proof of concept exfiltration channel tool based on DoH [GODOH] already exists and it is reasonable to expect others which are much less benign will emerge in the future.

DoH queries and responses will be intermingled with other HTTPS port 443 traffic. This provides good traffic flow security for the client, because it's not readily clear when a DoH request or reply is taking place (unlike DoT). However network analytics may fail to detect when a malware implant on the client is making DoH requests, which would present a security risk.

Security of DoH relies on the TLS session for the HTTPS connection. Therefore it inherits the security guarantees that TLS provides. There may be interactions between DoH and TLS, for example issues

arising from DoH servers handling large numbers of TLS connections to DoH clients simultaneously, that have not yet been explored.

DNS query traffic is often made available to providers of threat intelligence and reputation services. These providers typically aggregate such data from many operators, process these datasets and then generate whitelists and blocklists which operators can then apply in their networks. DoH is likely to mean there will be a reduced volume of query data readily available for this sort of analysis. Overall DNS query traffic would be spread across a combination of operator-run DNS resolver servers and a number of DoH servers who might (or might not) make their query traffic available to providers of threat intelligence and reputation services.

This will have two unwelcome results. First, threat intelligence and reputation services will have fewer data to analyse and therefore have a significantly less complete perspective of end users' DNS behaviour. Second, the quality and effectiveness of the data provided by threat intelligence and reputation services will be materially diminished. This seems likely to reduce the security of networks and users as a result.

Although DoH uses TLS to provides authentication and data integrity of the channel between client and resolver, this does not guarantee that the resolver is returning correct DNS data to the client. DoH clients may need to perform DNSSEC validation to verify data received from DoH servers.

There is a risk that internal domain names used extensively in managed enterprise networks could leak to external DoH servers, presenting obvious privacy and security issues.

DoH can be implemented within the browser, rather than the kernel or an operating system library. It is not yet clear if that will make endpoint-based malware detection more or less effective.

Browser APIs will allow web applications to make DoH queries. If individual applications have the ability to select their own DoH server, it is not clear if that change would only apply to DoH lookups by that application or if they had broader scope. When these changes over-ride system- or operator-defined DoH settings, they will affect other processes running on the DoH client and effectively hijack their DNS traffic by rerouting it to the application's DoH provider.

The interactions between infrastructure using Network Address Translation (NAT) [RFC3022] and DoH is unclear. In situations where a third party DoH server can return security threat data back to the

operator of the originating network, its value is likely to be diminished due to the IP address sharing inherent in using NAT.

10. Human Rights Considerations

Parental control systems relying on DNS filtering can be bypassed using DoH. This may lead to increased ability of minors to access restricted or otherwise inappropriate content on the Internet, creating a conflict with the UN Convention on the Rights of the Child [Insert Ref to actual treaty text.]

Using DoH to bypass local DNS filtering and provide anonymity for end users is a mixed blessing. Using DoH to bypass country-based DNS filtering may provide end users a way of bypassing censorship mechanisms put in place by restrictive regimes. On the other hand, DoH could also help criminals to evade detection by obscuring the source of their attacks or botnet control nodes, while increasing the commercial tracking of user activity and trade in that data.

In jurisdictions where DNS blocking schemes have been incorporated into law, widespread deployment of DoH could encourage policy approaches that are more restrictive of users' freedom of expression, their ability to access information or limit the generation and availability of online content.

11. Open Issues for Further Study

- DoH's reliance on TLS raises a number of concerns and unknowns. These include OSCP stapling, certificate life-times, scalability in managing session tickets, handling session resumption and the duration of TLS sessions. The trade-offs between certificate validation and session duration for possibly short-lived DoH transactions are not yet well understood. These factors will need careful analysis, particularly on DoH servers which get queries from large numbers of DoH clients.

- The impact of DNS traffic migrating from UDP and port 53 to TCP and port 443 needs to be modelled because of the extra packets and round-trip times needed for TCP connection setup and the TLS handshake: performance, capacity planning, network engineering and so on.

- DoH can leverage the rich per-user and per-device tracking that pervades the web today. Since the implications of that are not yet well understood, further work in this area is needed.

- How DoH services will develop new functionality to overcome any inherent performance impact from moving the service out of the

operator network. For instance, optimisations to reduce latency in 3/4/5G mobile networks.

- Clarification is needed around ECS blocking and options to avoid impacting existing network operator on-net caching strategy.

- What DoH service metrics will be available for users to compare DoH providers?

- DoH discovery in networks which use private IP addresses for CPE and stub resolvers or proxies could be challenging. Presumably this will be addressed in the add WG.

12. IANA Considerations

This memo includes no request to IANA.

13. Acknowledgements

Fill this in later

14. References

14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

14.2. Informative References

[CSRIC] FCC, "Cybersecurity Risk Management and Best Practices", <https://transition.fcc.gov/to-be-confirmed>.

[GDPR] European Union, "General Data Protection Regulation (EU) 2016/679", <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

[GODOH] Sensepost, "DNS exfiltration using DoH", <https://sensepost.com/blog/2018/waiting-for-godoh/>.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, DOI 10.17487/RFC3022, January 2001, <https://www.rfc-editor.org/info/rfc3022>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <https://www.rfc-editor.org/info/rfc6146>.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, DOI 10.17487/RFC6147, April 2011, <https://www.rfc-editor.org/info/rfc6147>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[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>.

[USPS] US Secretary of Commerce, "EU-U.S. Privacy Shield Framework", <https://www.privacyshield.gov/EU-US-Framework>.

Authors' Addresses

Andy Fidler
BT plc
BT Adastral Park
Martlesham Heath, Ipswich IP5 3RE
UK

Email: andrew.fidler@bt.com

Bert Hubert
OpenXchange
Rollnerstrasse 14
Nuremberg 90408
Germany

Email: bert.hubert@open-xchange.com

Jason Livingood
Comcast
1800 Arch Street
Philadelphia PA 19118
USA

Email: jason_livingood@comcast.com

Jim Reid
RTFM llp
St Andrews House
382 Hillington Road, Glasgow G51 4BL
Scotland

Email: jim@rfc1035.com

Nic Leymann
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
Bonn 53113
Germany

Email: N.Leymann@telekom.de