OPEN RIGHTS GROUP

DNS security getting it right

Recommendations for policy makers and technologists

About Open Rights Group

As society goes digital we wish to preserve its openness. We want a society built on laws, free from disproportionate, unaccountable surveillance and censorship. We want a society in which information flows more freely. We want a state that is transparent and accountable, where the public's rights are acknowledged and upheld.

We want a world where we each control the data our digital lives create, deciding who can use it and how. We want the public to fully understand their digital rights, and be equipped to be creative and free individuals. We stand for fit-for-purpose digital copyright regimes that promote free expression and diverse participation in culture.

We campaign, lobby, talk to the media, go to court — whatever it takes to build and support a movement for freedom in the digital age. We believe in coalition, and work with partners across the political spectrum.

We uphold human rights like free expression and privacy. We condemn and work against repressive laws or systems that deny people these rights. We scrutinise and critique the policies and actions of governments, companies, and other groups as they relate to the Internet. We warn the public when policies — even well-intentioned ones — stand to undermine the freedom to use the Internet to make a better society.

www.openrightsgroup.org

Executive summary

This paper addresses the privacy implications of two new Domain Name System (DNS) encryption protocols: DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH). Each of these protocols provides a means to secure the transfer of data during Internet domain name lookup, and they prevent monitoring and abuse of user data in this process.

DoT and DoH provide valuable new protection for users online. They add protection to one of the last remaining unencrypted 'core' technologies of the modern Internet, strengthen resistance to censorship and can be coupled with additional protections to provide full user anonymity.

Whilst DoT and DoH appear to be a win for Internet users, however, they raise issues for network operators concerned with Internet security and operational efficiency. DoH in particular makes it extremely difficult for network operators to implement domain-specific filters or blocks, which may have a negative impact on UK government strategies for the Internet which rely on these. We hope that a shift to encrypted DNS will lead to decreased reliance on network-level filtering for censorship.

Concern has been raised that DoT and DoH may decrease network efficiency by causing user traffic to be routed via geographically distant servers. We propose a number of mitigations for this issue, particularly suggesting that operators enable the Internet Engineering Task Force (IETF) standard of GeoDNS on their services. Network operators will have a number of choices like this to make as encrypted DNS becomes more widely adopted. Notably, captive portals – network landing pages requiring a response such as a login – are a key functionality which will no longer be viable with the roll-out of encrypted DNS, forcing network operators to choose how to respond. Recognising the desirability of captive portals for network operators, we recommend collaboration among stakeholders to develop new standards that allow a user to interact securely with a network operator's content before accessing their full service.

Activating DoT and DoH should always be a user choice. To avoid market monopolisation, a significant risk, we urge developers and application providers that integrate encrypted DNS as a default setting to offer their users a choice of provider. Users should also always be able to disable encrypted DNS entirely if they wish to do so. These options, however, should not be an excuse for service operators to burden users and escape responsibility. It is essential that network operators and DNS providers act to protect user privacy. Encrypted DNS must not be abused as an excuse for commercial entities to collect, store and share more data on their users, and we encourage companies to insert clear statements in privacy policies committing them in this regard.

Overall, encrypted DNS is a long-overdue step forward in protecting user privacy online. We support its continued development and adoption, and note that as a matter of net neutrality, it would not be legal for the UK government to limit or block its use by Internet Service Providers (ISPs).

Recommendations

All parties

1. All parties including ISPs need to recognise that the issues raised by encrypted DNS services are not just theoretical. Encrypted DNS services are already being deployed, and this trend is set to continue.
2. Traditional DNS remains a weak link for Internet privacy and security. Network providers and stakeholders must recognise that a move to a secure encrypted standard is inevitable, regardless of any pushback they may mount towards DoH or DoT.
3. Stakeholders should not fight the adoption of DoT and DoH on the mistaken basis that doing so will protect children. Children interacting with the Internet also deserve the improved privacy and security that encrypted DNS can provide.

Government

4. The Government should not seek to legally block or filter encrypted DNS technologies.
5. The Government and other stakeholders should acknowledge that, despite what some reports have claimed, DoT and DoH do not present any unique or specific challenges to age verification as implemented by the Digital Economy Act 2017.

Parents

6. Parents who wish to ensure that adult content filters continue to operate correctly should investigate configuring adult content filters and parental controls on a per-device basis.
7. DoT and DoH providers should consider offering optional filtered services for users who want content filtering to be enabled, and parents should consider these when they become available.

Network operators

8. Network operators who maintain physical control over the hardware deployed on the network (such as those managing corporate networks), should be aware of DoT and DoH but should not be critically concerned. They should update device management policies to send DNS traffic to internally-operated DoT or DoH servers, or to disable encrypted DNS altogether.

Encrypted DNS service operators

9. DoT and DoH server operators who expect to receive a large volume of queries from a global user base should investigate enabling GeoDNS on their service so that domain owners can route users to geographically-optimal servers.
10. Operators of DoT and DoH services (in particular those which may be enabled by default in devices or applications) should ensure that their services do not store any data which may allow end-users to be identified.

Developers

11. Application developers should ensure that they implement DoT and DoH technology in ways that allow the feature to be configured or overridden by device management software, such as that used by administrators of corporate networks.
12. Developers creating applications and devices which rely on third-party encrypted DNS servers should avoid becoming complicit in the increasing centralisation of power among a handful of large cloud providers. If left unchecked, this will create central points of failure and give large corporate third-parties access to many users' DNS queries.
13. Developers and application providers should offer users a choice of provider if their product enables encrypted DNS by default.
14. Even if typical users are not expected the benefits or drawbacks of encrypted DNS, developers must not remove user choice from their products. Users should always be able to select their own DNS servers, or to disable DoT and DoH entirely if they wish.

Standards bodies

15. Internet and technology standards bodies such as the IETF and Wi-Fi Alliance should accept that captive portals are a desirable technology for network operators, but that they are outdated and effectively require attacking user traffic. New standards should be developed to allow users to interact securely with a network operator's content before being granted full network access.

Terminology

CDN	Content Delivery Network
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DPI	Deep Packet Inspection
ESNI	Encrypted Server Name Indication
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
OSI	Open Systems Interconnection
POP	Point of Presence
SNI	Server Name Indication
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network

Introduction and background

DNS-over-TLS (DoT),[1] introduced in 2016, and DNS-over-HTTPS (DoH),[2] introduced in 2018, are two technical standards proposed and documented via the Internet Engineering Task Force (IETF) which aim to improve Internet users' privacy and security by adding encryption to Domain Name System (DNS) requests. This report reviews the problems that these standards are attempting to solve, analyses their effectiveness as solutions and identifies issues that network operators may face as a result of the rapid pace of adoption. It makes a series of recommendations aimed at protecting Internet users' online privacy.

The DNS system provides essential functionality for the modern Internet. It translates human-readable words into the numerical Internet Protocol (IP) addresses which are used by networked computers to locate each other. When a user types in a website URL such as *www.openrightsgroup.org*, their computer contacts a DNS server to look up the appropriate IP address for that particular domain – which will look something like *46.43.36.233*. DNS servers are often operated by a user's Internet Service Provider (ISP), but widely-used servers are also operated by large commercial entities such as Cloudflare,[3] Google[4] and Cisco,[5] and by smaller independent entities such as the Chaos Computer Club.[6] As with web servers, there is nothing to prevent anyone with an Internet-connected computer from running a DNS server or resolver.

By default, DNS requests are not private. Even in 2019, most DNS requests are sent unencrypted, and are therefore vulnerable to logging, manipulation or censorship. Requests reveal exactly which sites, apps and online services a user is accessing, which makes DNS a prime tool for state or corporate surveillance and content control. DNS providers could also collect and sell data about user's Internet activity or use it to target them with advertising. DNS is therefore a critical point of vulnerability in Internet privacy – which the IETF standards of DoT and DoH aim to address. Whilst the standards IETF oversees are not mandatory, smooth interoperation amongst internet devices requires consensus and common protocols, so IETF proposals carry significant weight and their standards see widespread adoption.

Other Internet technical standards that have been in use for decades, such as HTTP (web) or POP (email), have been updated over the years to add encryption to prevent eavesdropping or traffic manipulation. The DNS standard, however, has stagnated. The IETF has warned that as "other protocols become more and more privacy-aware and secured against surveillance, the DNS may become 'the weakest link' in privacy."[7]

Whilst DoT and DoH are relatively new standards, encrypted DNS services are already widely deployed. DoT is available on Android and plans exist to bring it to the Google Chrome web browser.[8] DoH is available in the Mozilla Firefox web browser and plans

1 IETF Memo, *Specification for DNS over Transport Layer Security (TLS)*, Document Reference RFC 7858, May 2016 <https://tools.ietf.org/html/rfc7858>

2 IETF Memo, *DNS Queries over HTTPS (DoH)*, Document Reference RFC 8484, October 2018 <https://tools.ietf.org/html/rfc8484>

3 <https://1.1.1.1/>

4 <https://developers.google.com/speed/public-dns/>

5 <https://www.opendns.com/>

6 <https://www.ccc.de/en/censorship/dns-howto>

7 IETF Memo, *DNS Privacy Considerations*, August 2015 <https://tools.ietf.org/html/rfc7626>

8 XDA Developers, *Google Chrome will add support for DNS over TLS providers like CloudFlare*, 21 September 2018 <https://www.xda-developers.com/google-chrome-dns-over-tls-cloudflare/>

exist to enable the feature by default for all users.[9] It is commonly expected that adoption and use of these standards will only increase: expansion is part of an ongoing effort within the Internet technology community to increase user privacy.

DoT and DoH have recently come under scrutiny, however, with media controversy around Internet companies and reports of intelligence agencies holding "crisis talks" over plans to encrypt traffic, particularly for users of Google Chrome.[10] In April 2019, *The Times* reported that encryption plans may "make it harder to block harmful material, including child-abuse images and terrorist propaganda."[11] Further concern was raised in a May 2019 Parliamentary debate.[12]

In ORG's view, encrypted DNS services should not be viewed cynically as a deliberate attempt by large technology companies to preclude Internet filtering, or to co-opt user browsing history for their own gains. They are largely a win for user privacy and security, and many of the concerns that adoption of such services raise can be obviated partially or entirely through close collaboration between implementers of the technology and regulatory stakeholders. This report proposes a number of recommendations for network operators and encrypted DNS operators to lessen the potential negative effects of the rollout of their services.

Unencrypted DNS: A privacy and security problem

Unencrypted DNS queries pose a major threat to user privacy online. While encrypted modern protocols such as HTTPS can shield the *content* exchanged between a user and a server from logging and monitoring, the lack of equivalent protection in DNS means that the *domain names* that a user chooses to visit may be exposed to eavesdroppers located between a user and their DNS server. Without encryption, potential attackers are able to observe all the domains a user's device queries, revealing which websites the user has visited and metadata about their use of other services such as mobile apps and messaging. Monitoring DNS queries may also enable an eavesdropper (and potential attacker) to distinguish between devices operating on a user's network by identifying requests for domains belonging to cloud services or software update servers that are device-specific.

DNS query metadata can reveal sensitive personal information about a user's health, sexuality, interests and other aspects of their lives. Much of this information might be considered "special category data" under the EU General Data Protection Regulation 2018 (GDPR) which data controllers need a specific established reason to process.[13]

ISPs and intelligence agencies have been accused in the past of exploiting DNS to surveil users or manipulate DNS responses. Documents released by Edward Snowden suggest that the USA's National Security Agency deployed DNS surveillance and manipulation as part of its QUANTUMDNS programme.[14] In 2017, the US Senate also voted to eliminate rules which restricted ISPs from selling their customers' web

9 Mozilla Hacks, *A cartoon intro to DNS over HTTPS*, 21 May 2018 <https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/>

10 Computer Business Review, *Gov't and ISPs in "Crisis Talks" over Google's Encrypted DNS Plans*, 23 April 2019 <https://www.cbronline.com/news/encrypted-dns>

11 The Times, *Warning over Google Chrome browser's new threat to children*, 21 April 2019 <https://www.thetimes.co.uk/edition/news/warning-over-google-chrome-browsers-new-threat-to-children-vm09w9jpr>

12 House of Lords Hansard, *Question: Internet Encryption*, 14 May 2019 <https://hansard.parliament.uk/Lords/2019-05-14/debates/E84CBBAE-E005-46E0-B7E5-845882DB1ED8/InternetEncryption>

13 Information Commissioner's Office Guidance on Article 9 Special Category Data <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/>

14 The Intercept, *The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics*, 12 May 2014 <https://theintercept.com/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/>

browsing histories; information which could be easily collected by surveilling user DNS requests.[15]

DNS query information can be revealing even when a user takes other steps to protect their Internet activity from surveillance, such as using a Virtual Private Network (VPN). Under certain conditions, even when connected to a VPN, an operating system may revert to using its default DNS services. This can cause "DNS leaks", where user traffic is routed via the VPN, but a user's unencrypted DNS queries remain visible to network-level eavesdroppers, undermining the anonymity a VPN should provide. The IETF has also noted that users can be re-identified through matching of DNS queries. Pattern monitoring, even across locations, may make it possible to establish that two apparently different users are the same person.[16]

The lack of encryption also means that DNS requests are easy to isolate from a user's other data for the purposes of manipulating them, especially since DNS lacks a method by which to verify the authenticity of a server's response. DNS requests can also be subject to "DNS hijacking", in which a rogue party redirects a user's DNS queries to a server which returns responses of that rogue party's choice. Damagingly, a rogue party could, for example, redirect the user toward malware, phishing, or otherwise unwanted domains. Similarly, a government or corporate eavesdropper located between user and DNS server could implement censorship by deliberately blocking or manipulating responses pertaining to specific domains.

ISPs often have reason to manipulate the data their own DNS servers return to customers – for example, to implement website filtering in compliance with a court order or for parental content control. These cases do not count as hijacking, since the users' queries are not being intercepted; instead, the ISP's own DNS server is returning false results. These, for example, may point to pages saying that a domain "does not exist" or that the page "will not load due to parental content filtering". This technique is known as "DNS spoofing" or "DNS cache poisoning".

As a result of the valuable nature of user data, the Internet industry has expressed a clear intent to develop and adopt standards that promote Internet user security and to work to mitigate surveillance. The IETF's current policy is that "pervasive monitoring" of communications is an attack, and should be mitigated as an inherent part of designing any new standards.

In its memo, *Pervasive Monitoring is an Attack*, the IETF notes that as technology advances, techniques that were once only available to extremely well-funded actors are becoming more widely accessible.[17] No matter what network operators and regulators may think of current encrypted DNS proposals, there is only a limited time left before unencrypted DNS services are replaced *en masse* with more secure alternatives. Even if a major regulatory pushback were mounted against DoT and DoH, DNS is too critical a part of the infrastructure of the modern Internet for stakeholders to allow it to remain in its current insecure state indefinitely. Unencrypted DNS remains a weak link for Internet privacy and security, and network providers and stakeholders must recognise that a move to a secure encrypted standard is inevitable.

Recommendations:

1. All parties including ISPs need to recognise that the issues raised by encrypted DNS services are not just theoretical. Encrypted DNS services are already being deployed, and this trend is set to continue.
2. Traditional DNS remains a weak link for Internet privacy and security. Network providers and stakeholders must recognise that a move to a secure encrypted standard is inevitable, regardless of any pushback they may mount towards DoH or DoT.

15 ARSTechnica, *Senate votes to let ISPs sell your Web browsing history to advertisers*, 23 March 2017 <https://arstechnica.com/tech-policy/2017/03/senate-votes-to-let-isps-sell-your-web-browsing-history-to-advertisers/>

16 See 7 above.

17 IEFT Memo, *Pervasive Monitoring is an Attack*, Document Reference RFC 7258, May 2014 <https://tools.ietf.org/html/rfc7258>

Previous DNS solutions: DNSSEC & DNSCrypt / DNSCurve

DoT and DoH are not the first attempts to solve the problems of privacy and security posed by traditional DNS services. This section discusses two main solutions that have previously been posited: DNS Security (DNSSEC) and DNSCrypt/DNSCurve.

DNSSEC

DNS Security, or DNSSEC, is the most notable of previous DNS security efforts. It comprises a set of extensions to the DNS protocol which do not provide additional privacy but aim to provide verifiability to thwart attempts at DNS hijacking or spoofing.

DNSSEC authenticates DNS responses by using public-key cryptography,[18] which verifies the legitimacy of DNS responses through a series of trusted digital signatures. For example, a response to a DNS request for *www.openrightsgroup.org* would be signed by (a) a key that would, in turn, (b) be signed by the operators of *openrightsgroup.org* using a key that (c) would itself be signed by the operators of the *.org* top-level domain. Finally, the *.org* top-level domain's key would be signed by (d) the keys belonging to the 'root zone', which has ultimate authority over the Internet's top-level domains, such as *.com*, *.org*, and *.uk*.[19]

In theory, DNSSEC creates a verifiable chain of trust which ensures that the response a user receives from their DNS server can be robustly verified as legitimate. In practice, however, it is complex and hard to understand even for domain operators, who must also first enable it by generating a unique signing key and configuring "delegation signer" (DS) records for their domain. Adoption levels remain low. In 2018, Cloudflare cited research by the Asia-Pacific Network Information Centre (APNIC) that estimated only 14% of DNS requests worldwide were being correctly validated with DNSSEC. According to Cloudflare, some of this is due to apathy by domain owners, but yet more is the result of some large DNS operators not supporting the option at all, requiring domain owners who want to protect their users to move to another DNS provider altogether.[20]

Although adoption of DNSSEC has been slow, the take-up that has happened provides evidence of interest in improving DNS security and hints at a continuing trend toward solutions which put DNS queries out of reach of tampering or manipulation – such as DoT and DoH.

DNSCrypt / DNSCurve

DNSCrypt and DNSCurve are early software attempts to solve the privacy threat posed by an eavesdropper able to observe DNS queries. Although they predate DoT and DoH, they similarly encrypt DNS requests so they cannot be seen by anyone other than the user making the request and the server issuing the reply. Neither DNSCrypt nor DNSCurve has seen a significant level of adoption among users, and the standards do not have the level of interest and support from large commercial entities that DoT and DoH currently enjoy.

---

18 Wikipedia, *Public-key Cryptography*, Accessed 31 May 2019, Last edited 11 May 2019 <https://en.wikipedia.org/wiki/Public-key_cryptography>

19 The "Root Key Signing Key" is managed by the Internet Assigned Numbers Authority (IANA), and is used to sign other keys roughly four times a year in a so-called "Key Signing Ceremony" <https://www.iana.org/dnssec/ceremonies>

20 Cloudflare Blog, *Expanding DNSSEC Adoption*, 18 September 2018 <https://blog.cloudflare.com/automatically-provision-and-maintain-dnssec/>

User benefits of encrypted DNS

DoT and DoH, today's leading versions of the DNS protocol, both provide a functionally similar experience for end users. Both prevent middle-man eavesdropping by encrypting DNS queries and ensuring that queries cannot be modified as they travel between user device and DNS server. Neither provides inherent protection against rogue responses being returned by the DNS server itself. They can, however, be coupled with DNSSEC to provide this functionality. Both standards have seen significant interest from major Internet stakeholders such as Cloudflare, Google and Mozilla.

DNS-over-TLS (DoT)

DoT requires all connections with DNS servers to be made using Transport Layer Security (TLS), which is also the most common protocol used by HTTPS sites to encrypt web traffic between user and server.

The key flaw for users of DoT is that it does not attempt to disguise the fact that DNS requests are taking place. This means that it continues to facilitate web filtering. The Transmission Control Protocol (TCP) port used by DoT, 853, is unused by other common protocols[21] and is therefore easily identifiable to network filter systems and its use can therefore be blocked by network providers if desired.

A pro for users is its flexibility. DoT can be enabled transparently on devices using a feature known as "opportunistic mode", which allows users or devices to transition to DoT seamlessly. When set to opportunistic mode, devices will automatically use encryption if both network and DNS server support it. If either does not, the device will fall back to using regular DNS. However, actively selecting and configuring this mode may be beyond the knowledge or ability of regular Internet users, which limits its effectiveness.

A number of large public DNS servers, such as those operated by Cloudflare,[22] Google,[23] and Quad9,[24] support DoT, as do versions P (2018) and later of Android.[25] Initial moves to add DoT to Google's Chrome browser have also begun.[26] DoT's adoption for Android is particularly significant since it accounts for approximately 75% of the mobile market as measured in April 2019.[27]

DNS-over-HTTPS (DoH)

From a user perspective, DoH is similar to DoT. The chief difference is that, rather than being a new protocol, DoH conducts lookups over the existing secure web content delivery protocol HTTPS, encasing DNS requests in encryption.

DoH uses the default port for HTTPS, TCP 443, which makes filtering and censorship significantly more difficult. DoH traffic cannot be distinguished from ordinary web traffic, which makes it impossible for it to be targeted outright by filtering equipment.[28] Blocking TCP port 443 outright would mean also blocking most HTTPS-enabled sites. Anyone wishing to reliably identify – and monitor or curtail – DoH traffic has to rely on a created inference that HTTPS traffic between users and servers which only provides DNS services is likely to be DNS traffic. This is an unreliable method of identification as servers offering DoH services may also offer other things, and while it may work for large publicly-operated DNS resolvers such as those run by Cloudflare or Google, it is likely that small or short-lived DoH servers will arise specifically to evade this form of censorship if it becomes commonplace.

---

21 Speedguide, Port 853 Details <https://www.speedguide.net/port.php?port=853>

22 Cloudflare explanation, DNS over TLS <https://developers.cloudflare.com/1.1.1.1/dns-over-tls/>

23 Google Security Blog, *Google Public DNS now supports DNS-over-TLS*, 9 January 2019 <https://security.googleblog.com/2019/01/google-public-dns-now-supports-dns-over.html>

24 RipeNCC, *Quad9, a Public DNS Resolver – with Security*, 21 November 2017 <https://labs.ripe.net/Members/stephane_bortzmeyer/quad9-a-public-dns-resolver-with-security>

25 Google Security Blog, *DNS over TLS Support in Android P Developer Preview*, 17 April 2018 <https://security.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html>

26 See 8 above.

27 Statcounter, *Mobile Operating System Market Share Worldwide*, April 2018 – April 2019 <http://gs.statcounter.com/os-market-share/mobile/worldwide>

28 *DNSCrypt* also uses TCP Port 443 for by default for encrypted lookups, however it also uses its own protocol which is identifiable as DNSCrypt traffic. DoH traffic is indistinguishable from other HTTPS traffic.

DoH is not quite as widely deployed as DoT, but it has major support from Cloudflare in particular, which provided native support for DoH on its 1.1.1.1 DNS resolver at launch.[29] Cloudflare's mobile application is available for Android and iOS and automatically configures phones to use DoH.[30] Google PublicDNS[31] and Quad9[32] also support DoH on their public DNS servers.

Mozilla Firefox, which accounts for almost 10% of all desktop web traffic,[33] added native DoH support in 2018.[34] As of April 2019 Mozilla is continuing to roll out DoH, posting regular updates on studies of the performance and privacy impact of enabling DoH by default.[35] Mozilla's eventual stated goal is to ship the Firefox browser with DoH enabled by default and with a pre-configured list of "trusted" DNS servers that will bypass the DNS settings on the user's operating system or network.[36] They stated in 2018; "We'd like to turn [DoH] on as the default for all of our users. We believe that every one of our users deserves this privacy and security, no matter if they understand DNS leaks or not."[37]

A critical additional benefit for users in DoH is that it has the capacity to also be combined with Tor software to create a holistic system of DNS resolution that is not only resistant to censorship but also provides full anonymity. With this combination, a DNS server cannot see where a user is located or link their queries together. Cloudflare has already demonstrated this approach to be functional and usable, although it presents the experiment as a technical exercise.[38]

Appeal of DoT/DoH for Internet of Things manufacturers

DoT and DoH provide compelling features for developers of online applications and Internet of Things (IoT) hardware. With this encryption, developers will be able to ensure that their product makes use of a trusted DNS server. The result will be to increase reliability and reduce customer service issues for products which are likely to reach disparate, perhaps global, marketplaces. Anti-virus software vendors have already proven the demand for this type of trusted and encrypted DNS resolution functionality, although they have had to create their own proprietary solutions, with one example being Avast's *SecureDNS*.[39]

---

29 Cloudflare Blog, *Announcing 1.1.1.1: the fastest privacy-first consumer DNS service*, 1 April 2018 <https://blog.cloudflare.com/announcing-1111/>

30 See 3 above.

31 Google Guide, *DNS-over-HTTPS* <https://developers.google.com/speed/public-dns/docs/dns-over-https>

32 Quad9 Blog, *DoH with Quad9 DNS Servers*, 5 October 2018 <https://www.quad9.net/doh-quad9-dns-servers/>

33 Statcounter, *Desktop Browser Market Share Worldwide*, April 2018 – April 2019 <http://gs.statcounter.com/browser-market-share/desktop/worldwide>

34 Daniel Stenberg Blog, *Inside Firefox's DoH Engine*, 3 June 2018 <https://daniel.haxx.se/blog/2018/06/03/inside-firefoxs-doh-engine/>

35 Mozilla Blog, *DNS-over-HTTPS(DoH) Update – Recent Testing Results and Next Steps*, 2 April 2019 <https://blog.mozilla.org/futurereleases/2019/04/02/dns-over-https-doh-update-recent-testing-results-and-next-steps/>

36 See 9 above.

37 Ibid.

38 Cloudflare Blog, *Introducing DNS Resolver for Tor* <https://blog.cloudflare.com/welcome-hidden-resolver/>, 5 Jun 2018

39 Avast Anti-Virus SecureDNS <https://help.avast.com/en/av_abs/10/etc_tools_secure_dns_overview.html>

Issues for network operators in encrypted DNS

While DoT and DoH may appear to be a win for network users, they raise some notable concerns for ISPs, Governments and other network operators concerned about Internet security and network efficiency.

Increased difficulty of domain filtering and blocking

Both DoT and DoH make it more difficult for network operators to block individual domains. DNS-based filtering is currently widely deployed by ISPs and corporate networks as an easy and generally-reliable method to prevent users from accessing particular domains, such as those blocked by court order in the UK (generally domains hosting content which infringes intellectual property rights)[40] or those which a corporate network owner may wish to prevent employees from accessing. The Government also leans heavily on domain blocking as a possible enforcement measure in various current Internet policy proposals. A BT presentation recently described DNS filtering as "the most granular tool in the kit box used by UK ISPs to implement Government / Regulation blocking orders."[41]

As deployment of DoT and/or DoH increases, network-level DNS filtering will begin to work only on devices which rely on regular unencrypted DNS. ISPs that were previously able to manipulate users' DNS traffic will no longer be able to do so for devices using DoT or DoH. Network operators will still be able to prevent customers (or employees) from connecting to specified IP addresses; however, it will be difficult to block sites that use many IP addresses, or sites which rapidly change addresses, such as those that serve content from behind a large cloud service such as Cloudflare or Akamai, which protect customers from large spikes in traffic or add geographic redundancy. This will make it more difficult – although not impossible – for ISPs to comply with official blocking requests.

It should be noted that network-level filters are already generally trivial to bypass for users who have control of their devices, with services including VPNs and Tor allowing easy circumvention of filters. DNS filtering is, however, effective against users who do not have sufficient technical knowledge or control of their devices to use such circumvention tactics. Court blocking orders have also only been imposed to date on large network operators which already had blocking capabilities available in their network. No orders have been served compelling providers to do something they cannot already do. Furthermore, if a provider implements DNS-based filtering technology for sites which it has been ordered to block, the fact that some users could circumvent the block does not necessarily mean that the network operator has failed to comply with the order – it has done what it can, in line with its legal obligation.

We anticipate that the spread of DoT and DoH may lead the UK Government to adopt alternative domain blocking measures, such as serving injunctions or other legal notices on third-party encrypted DNS providers. These however may be ineffective, especially where online service providers lie outside UK jurisdiction.

Other means of network-level filtering

Security researcher Richard Clayton of the University of Cambridge Computer Laboratory has identified three basic methods of blocking content that are available to ISPs and network operators. These are "packet dropping", "content filtering", and "DNS poisoning".[42] As only the last method relies on having access to a user's DNS queries, it is important to investigate the viability of filtering through the other described methods before drawing conclusions about the impact of encrypted DNS services.

"Packet dropping" effectively prevents packets of data travelling across a network from reaching their intended destination. To block a domain using packet dropping, a network operator must enumerate all of the IP addresses used by that domain and will then simply drop connections destined for any of these addresses. This can work where domains resolve to single or small numbers of IP addresses, but it is

40 A comprehensive list of UK court-ordered blocks can be found on the *Blocked!* project website <https://www.blocked.org.uk/legal-blocks>

41 BT presentation, *Potential ISP challenges with DNS over HTTPS*, 5 April 2019 <https://indico.uknof.org.ukc/event/46/contributions/668/attachments/898/1109/UKNOF43_Potential_ISP_challenges_with_DNS_over_HTTPS_Issue_1A_050419.pdf>

42 Richard Clayton, *Failures in a Hybrid Content Blocking System*, Conference Paper May 2005 <https://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf>

an imperfect solution. As already noted, IP-based blocking may not be feasible for larger domains using cloud services, or smaller domains which may use a single server to host content for multiple sites. In addition, Distributed Denial of Service (DDoS) protection services operated by providers such as Cloudflare or Akamai can cause a single IP address to appear to be serving content for many different domains at once, or a single site to have many IP addresses. Even as far back as 2003, research by Benjamin Edelman, then a Student Fellow at Harvard Law School, indicated that 87% of tested sites on the *.com*, *.org*, and *.net* domains shared IP addresses with at least one other site, and 70% with 50 or more other sites.[43] Accordingly, packet dropping may cause collateral damage by blocking content from 'innocent' domains which share the targeted IP addresses.

Some domains have yet to adopt encrypted HTTPS connections and could therefore still be filtered through Clayton's "content filtering", which relies on analysing the content of communications to a particular IP address and filtering it as desired. Content filtering has the distinct advantage over packet dropping that it is able to distinguish based on the specific content being accessed, rather than purely by IP address and the ability to control for false positives and collateral damage in filtering is therefore much higher.[44] This method of filtering, however, has become less viable in recent years as more sites have moved towards serving content to users over encrypted HTTPS connections. When the content is encrypted, filtering based on content ceases working properly. It is still the case, however that network operators can observe and block traffic to sites which do not use HTTPS. Time is running out for content filtering, and it must only be regarded as a stopgap solution. Data gathered by LetsEncrypt and Mozilla suggests that the number of HTTPS-enabled pages loaded by users of the Firefox browser is rising dramatically.[45] Firefox, Google Chrome and other web browsers now also visibly highlight unencrypted HTTP pages as "Not Secure" to users, so the number of sites served over basic HTTP is expected to continue to dwindle.[46]

Even for HTTPS sites, however, some of the initial "handshake" establishing a connection between a user and a site is transmitted in plaintext, revealing to a network operator which site the user is trying to visit. This plaintext provides one other potential short-term solution for network operators looking to maintain their ability to filter. This is due to Server Name Indication (SNI), a feature of TLS encryption that allows content belonging to multiple domains to be hosted behind a single IP address. SNI requires a client to specify which domain they wish to load so the server knows which encryption certificate and site configuration to load in response. Cloudflare explains how this works: "The client adds the SNI extension containing the hostname of the site it's connecting to to the ClientHello message. It sends the ClientHello to the server during the TLS handshake. Unfortunately the ClientHello message is sent unencrypted, due to the fact that client and server don't share an encryption key at that point. This means that an on-path observer (say, an ISP, coffee shop owner, or a firewall) can intercept the plaintext ClientHello message, and determine which website the client is trying to connect to. That allows the observer to track which sites a user is visiting."[47]

The Cloudflare documentation from which that quote is taken goes on to describe Encrypted Server Name Indication (ESNI), a new method for encrypting SNI requests. ESNI is an extension to the latest version of the TLS encryption standard, TLS 1.3, which is supported by recent web browsers and web servers and already supported commercially by large cloud providers such as Cloudflare. Implementations such as Cloudflare's require no manual intervention from site operators to enable ESNI.[48] Inspecting SNI requests for blacklisted domains is accordingly no better than a short-term solution. Researchers from the University of Lorraine, France, have also demonstrated a number of weaknesses in this type of filtering that may allow it to be bypassed.[49]

Encrypted HTTPS websites which have not yet upgraded to TLS 1.3 also expose the requested domain name as part of the encryption certificate sent to a user when they connect. This is information which is

---

43 Benjamin Edelman, *Web Sites Sharing IP Addresses: Prevalence and Significance*, 12 September 2003 <https://cyber.harvard.edu/archived_content/people/edelman/ip-sharing/>

44 This is also how BT's Cleanfeed technology for tackling online child abuse imagery operated <https://web.archive.org/web/20160317030128/https://publicaffairs.linx.net/news/?p=154>

45 LetsEncrypt Stats, *Percentage of Web Pages Loaded by Firefox using HTTPS*, 2014 – 2019 <https://letsencrypt.org/stats/#percent-pageloads>

46 Google Chrome, *A Milestone for Chrome security: marking HTTP as "Not Secure"*, 24 July 2018 <https://www.blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure/>

47 Cloudflare Blog, *Encrypt it or lose it: how encrypted SNI works*, 24 September 2018 <https://blog.cloudflare.com/encrypted-sni/>

48 Cloudflare also offers a tool for end-users to check their device's support for ESNI and TLS 1.3 <https://encryptedsni.com/>

49 Wazen Shbair et al, *Efficiently bypassing SNI-based HTTPS Filtering*, Conference Paper May 2015 <https://www.researchgate.net/publication/269279295_Efficiently_bypassing_SNI-based_HTTPS_filtering>

therefore currently possible for a network observer to inspect using Deep Packet Inspection (DPI); however, as with inspecting SNI data, this is likely to be a short-lived solution as the TLS 1.3 standard, which encrypts the certificate exchange between a server and a user, is increasing in adoption rapidly.

Overall, whilst we recognise that DoT and DoH present difficulties for network operators, the alternative filtering and blocking methods available are also problematic. We hope that the shift towards encrypted DNS will lead to a reduced reliance on it for censorship, and will provoke a useful shift towards less-broad policies of filtering and blocking. This will also help to ensure that blocking and filtering have legal basis and are used only when necessary and proportionate.

Differences in filtering impacts between DoT and DoH

As noted earlier, differences in design between DoT and DoH mean that DoH may pose more problems to an operator wishing to filter particular DNS replies. DoT's use of a unique port, TCP 853, makes it easy to block via a firewall rule on the operator's network.[50] DoT's encryption is also only intended to conceal the content of DNS requests rather than the fact that a DNS request is being made. Therefore, even when a DoT server operator configures their DNS server to answer DoT requests via different port, a network operator could still identify and block DoT traffic by using DPI.[51]

By contrast, DoH content is indistinguishable from any other encrypted web traffic. It is not practical for a network operator to block all traffic to the port it uses, as many websites and applications would cease to work and the block would critically damage user privacy and security. DPI also won't help isolate DoH from other traffic on port TCP 443. The only reliable filtering ability, which depends on knowing that a particular DNS server *only* provides DoH services, is also a short-term solution, as the emergence of DoH servers that deliberately use infrastructure which also hosts other content will render it ineffective.

The second critical difference between the two protocols is that DoT is designed with two modes, "opportunistic" and "strict". The opportunistic mode allows seamless rollout, since "for opportunistic privacy, [...] one does not require privacy, but [only] desires privacy when possible."[52] In opportunistic mode, DoT-enabled clients use encrypted DNS via DoT where available and fall back to regular unencrypted and unauthenticated DNS where it is not. If a network operator blocks network packets destined for port TCP 853, clients which detect that their preferred DoT service is unreachable will silently fall back to unencrypted DNS, which a network operator then can filter or log as desired. This, however, is also likely to provide only short-term respite, as current 'silent' implementations of opportunistic DoT may eventually be followed by implementations which indicate plainly to users that secure DNS resolution is not available on the current network, much like the "Not Secure" markers used by web browsers for unencrypted HTTP pages.

Recommendation:

- **14.** Even if typical users are not expected the benefits or drawbacks of encrypted DNS, developers must not remove user choice from their products. Users should always be able to select their own DNS servers, or to disable DoT and DoH entirely if they wish.

Adult content filters

The impact of DoH and DoT on adult content filters is a significant point of interest for the UK. It is worth noting that, globally, ISPs implementing optional adult content filters is a very unusual phenomenon. Currently we are aware of only the UK attempting such an approach.

Adult content filters largely use DNS-based techniques similar to other types of filtering. However, adult content filters are distinct in that they are implemented with a target audience of children in mind. In this scenario, parents are likely to have physical control over devices and systems used by their children. Privacy and security mitigations are therefore not limited to those which may be implemented by ISPs and network operators.

In the medium term, moving away from network-level adult content controls and reverting to filters which are implemented by parents or device owners at the

50 This advice applies primarily to corporate networks rather than general ISPs, who would be prevented from blocking ports in this manner by EU Net Neutrality Regulations (which are discussed further below).

51 Wikipedia, *Deep packet inspection*, Accessed 31 May 2019, Last updated 22 May 2019 <https://en.wikipedia.org/wiki/Deep_packet_inspection>

52 See 1 above, section 4.1.

level of individual devices may be the best approach. Network-level filtering technology is both broad and fragile and was always going to be challenged by technological changes. Device-based parental control software is available for all major operating systems and mobile platforms.

Some device-based filtering approaches also make use of DNS as a means of filtering results to queries. This approach is distinct from network-level DNS tampering as described above, as here parents will specifically configure devices to use a DNS server which will filter responses for sites which have been deemed inappropriate for minors. One example of this is *OpenDNS Family Shield*.[53]

This approach relies on configuring DNS servers at the system level, which may leave such tools still susceptible to – potentially accidental – circumvention by encrypted DNS at the application level. For instance, a child user of Firefox may accidentally bypass this type of configuring if Mozilla achieves the goal of enabling DoH by default. In the long term, therefore, we call for implementers of DoT and DoH to work in conjunction with parents and parental control software to ensure that their technology can enable parental control aims, rather than hinder them. Kenji Baheux, a Product Manager with Google Japan, confirms that this is already a core focus of the team working on DoH for Chrome. He states that Google wants to "continue to support admins for Education and Enterprise use cases, and parents for family use cases", and recognises these audiences' desire to be able to continue to "prevent students/employees/kids from accessing unsafe/inappropriate websites."[54]

Proponents of encrypted DNS are not necessarily opposed to the aims of parents or those concerned with the prevalence of adult content online. Indeed, it is perfectly possible for DoT and DoH to work in conjunction with adult content filtering technology to provide a service that provides privacy and security for children's DNS queries while also providing the benefits of adult content filtering to suit parental needs. Creating these systems – similar to *OpenDNS Family Shield* – is likely to require cooperation between groups working on parental control systems and operating system and application vendors in order to ensure that all applications on a particular device respect and enforce parentally-configured secure DNS server settings. We encourage such cooperation to take place.

Recommendations:

6. Parents who wish to ensure that adult content filters continue to operate correctly should investigate configuring adult content filters and parental controls on a per-device basis.
7. DoT and DoH providers should consider offering optional filtered services for users who want content filtering to be enabled, and parents should consider these when they become available.

Age verification

Questions have been raised about the potential impact encrypted DNS services will have on the age verification scheme under the Digital Economy Act 2017.[55]

As of 15 July 2019, commercial providers of pornographic websites are required to actively verify the age of UK-based users to their websites. Since detection of UK-based users will be implemented by site owners, and will take place using the IP address of the user connecting to the website, DoT or DoH technologies will have no impact on this detection. UK users will be shown age verification prompts whether or not they make use of encrypted DNS services.

In terms of blocking sites for non-compliance with the age verification regime, encrypted DNS services will have the same impact as that which has already been discussed in the prior section on network-level filtering. Both DoT and DoH make it more difficult – although not impossible – for network operators to block individual domains. Despite this, DoT and DoH do not present any challenges which are unique to age verification.

It should also be noted that age verification systems will also be easy for determined users to circumvent using technologies such as Tor or VPNs. Age verification's effectiveness is limited for a number of reasons, including that it does not apply to social media services. We have discussed the lack of effectiveness and numerous other concerns with age verification in previous publications.[56]

---

53 See, for example, OpenDNS Family Shield <https://www.opendns.com/home-internet-security/>

54 IETF Mail Archive, Correspondence Kenji Baheux, 13 March 2019 <https://mailarchive.ietf.org/arch/msg/dns-privacy/kpt6ZYMN5H3DsXPVi_QldmbAdJw>

55 See 11 above.

56 Open Rghts Group Age Verification publications at <https://www.openrightsgroup.org/campaigns/digital-economy-bill-hub/age-verification/>

Recommendations:

- **3.** Stakeholders should not resist the adoption of DoT and DoH on the mistaken basis that doing so will protect children. Children interacting with the Internet also deserve the improved privacy and security that encrypted DNS can provide.
- **5.** The Government and other stakeholders should acknowledge that, despite some reports, DoT and DoH do not present any unique or specific challenges to age verification as implemented by the Digital Economy Act 2017.

Lessened impact for network operators with control over user hardware

The impact of encrypted DNS is lessened where network operators are also in control of user hardware, which is frequently the case within corporate and educational networks. These network operators' control over hardware allows them to implement additional interception technologies as they are able to configure device-level settings which cooperate with their network-level filtering and logging equipment. Many such networks deploy "middleboxes" which can intercept traffic, strip its encryption and inspect it, before reapplying the encryption and either filtering the traffic or forwarding it to its destination.

Network operators in this position should be aware of the availability of this technology. However, we highlight the caution raised by security researchers from multiple universities as well as Cloudflare, Google, and Mozilla about the security implications of middlebox interception technologies. In a 2017 paper, the researchers noted: "As a class, interception products drastically reduce connection security. Most concerningly, 62% of traffic that traverses a network middlebox has reduced security and 58% of middlebox connections have severe vulnerabilities."[57] It is therefore critical that network operators who wish to implement such technology are diligent when researching the suitability of particular products with regard to retaining as much user privacy and security as possible.

As DoT and DoH technologies become more widespread, operating system designers may take note and integrate DoT and DoH as system-level services – as Google has already done for Android. This may give this class of administrators some additional control, since policies which restrict the use of encrypted DNS services could be implemented and enforced at device-level. Many widely-deployed business technologies have this kind of central administration functionality available; examples include Microsoft Windows' *Group Policy*, and Apple's *Mobile Device Management* for macOS and iOS. Such technologies could even be used to lock devices into using a internally-managed encrypted DNS server, providing privacy and security for employee DNS queries whilst also providing an easy method for the central filtering and logging of domain requests.

Recommendation:

- **8.** Network operators who maintain physical control over the hardware deployed on the network (such as those managing corporate networks), should be aware of DoT and DoH but should not be critically concerned. They should update device management policies to send DNS traffic to internally-operated DoT or DoH servers, or to disable encrypted DNS altogether.

Sub-optimal CDN endpoint selection

Large global domains use Content Delivery Networks (CDNs) to host the same content in multiple locations. This improves network performance, and helps keeps user costs down, by serving content from a location physically close to each user. It has been noted that encrypted DNS could have a negative impact on efficient content delivery and network operation.

The process of answering a DNS request is different for domains using a CDN than for smaller sites which may only have a single IP address. In both cases, the user's DNS server contacts an upstream server responsible for the domain and asks it for a list of corresponding IP addresses. Small sites hosted with single or small numbers of servers will return a list of all of the IP addresses corresponding to the site. For geographically-distributed sites, however, the upstream server will respond with a subset of IPs which belong to servers physically close to the DNS server which made the request. For example, a user in Manchester whose network operator runs a DNS

57 Zakir Durumeric et al, *The Security Impact of HTTPS Interception*, NDSS Symposium Paper, 27 February 2017 <https://dx.doi.org/10.14722/ndss.2017.23456>

server close by may receive IP addresses for UK servers located in London, rather than for servers in San Francisco which serve the same domain.

IETF, amongst others, has expressed concern that DoT and DoH users could submit their queries to remote third-party DNS servers and, as a result, receive suboptimal responses. For example, a Manchester-based user submitting queries to a DoT or DoH provider located in California might not receive a local London response, but might be directed to a site's San Francisco servers, causing the user's subsequent traffic to the domain to take an unnecessarily long and expensive path across the Atlantic Ocean. The IETF notes that "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.[58]

There are a number of mitigations available which could help lessen concern around the impact of DoT and DoH on efficient global routing. Many of these mitigations are already being put into practice even by unencrypted DNS providers, as the problem described is not unique to encrypted DNS. One of the simplest mitigations is for domain owners to use the approximate geo-location of the user's IP address to redirect them on their first arrival to the site. Some domains already do this for web content in order to provide localisation such as language or currency. For example, a site's main domain may be a *.com* top-level domain, but the site may redirect users whose IP addresses geolocate to the UK to the site's *.co.uk* version, which uses UK-located servers.

Another potential solution is for domain owners to investigate adopting Anycast routing, which maps a single IP address to servers in multiple geographic locations. Packets destined for that address take the quickest route possible from the user's device to a location that can serve the content. Anycast routing is already deployed by large cloud service providers. Cloudflare explains: "At the WAN level, every router in all of CloudFlare's 23 data centers announces all of our external-facing IP addresses. [...] When you send a packet to [an Anycast-enabled] IP address, it passes through a series of routers. Those routers look at the available paths to CloudFlare's end points and send the packet down the one with the fewest stops along the way."[59]

In practice, implementing the above mitigations may not even be necessary for site operators, since implementing DoT or DoH does not prevent DNS providers from also adopting new technologies that also attempt to solve the issue. The 2016 IETF standard *EDNS0-Client-Subnet*, sometimes known as *GeoDNS*, was drafted by Google engineers and describes a solution to the problem of a class of DNS servers that handle queries from "sources that are often not topologically close".[60] Under the method described by GeoDNS standard, DNS providers can ensure that the server responsible for the requested domain continues to return geographically optimal results by forwarding a portion of the end-user's IP address when submitting a query to the upstream DNS server responsible for a domain. The method is explained in the privacy policy of one DoH provider which has implemented the feature, *DNS-over-HTTPS.com*: "GeoDNS service uses your geographical information to determine servers that are faster and have lower latency to you. To make GeoDNS work, we send part of your IP address [...] to authoritive (sic) and recursive domain name servers."[61]

Less than a year after the GeoDNS standard's drafting, DNS provider Dyn estimated that it was implemented on about 20% of all global queries, with usage gradually increasing, predominantly as a result of increased use by Google PublicDNS.[62] Large DoT and DoH service providers with geographically-distributed networks are likely to enable GeoDNS on their services. We encourage smaller encrypted DNS providers to also investigate the GeoDNS standard and consider implementing it where appropriate.[63]

---

58 IETF, *DNS over HTTPS (DoH) Considerations for Operator Networks*, Internet-Draft, 9 March 2019, Expires 10 September 2019 <https://tools.ietf.org/id/draft-reid-doh-operator-00.html#rfc.section.5.2>

59 Cloudflare Blog, *Load Balancing without Load Balancers*, 6 March 2013 <https://blog.cloudflare.com/cloudflares-architecture-eliminating-single-p/>

60 IETF Memo, *Client Subnet in DNS Queries*, Document RFC 7871, May 2016 <https://tools.ietf.org/html/rfc7871>

61 DNS-over-HTTPS.com Privacy Policy <https://dns-over-https.com/privacy/>

62 Dyn Blog, *Personal Data in the DNS*, 11 April 2017 <https://dyn.com/blog/personal-data-in-the-dns/>

63 Google acknowledges the potential privacy implications of the technology in its draft of the standard and encourages providers to "only enable it explicitly in those circumstances where it provides a clear benefit for their clients."

Recommendation:

9. DoT and DoH server operators who expect to receive a large volume of queries from a global user base should investigate enabling GeoDNS on their service so that domain owners can route users to geographically-optimal servers.

Captive portals

Network operators such as commercial venues offering public Wi-Fi commonly use "captive portals" to provide features such as customer log-in, customer billing, traffic logging for abuse purposes, or advertising. Captive portals are also frequently used for log-in services on corporate networks or member-only venues.

A captive portal usually works through DNS hijacking or DNS spoofing. After a user's device connects to a network, its first attempt at sending a DNS request to use the network will be hijacked, redirecting the user to an internally-hosted page that sets out the network operator's desired authentication features. This happens regardless of the actual domain the user's device requested, and is possible because the network can see the user's unencrypted DNS request and 'spoof', or redirect it. The network's captive portal page holds the customer 'captive' until they accept a set of terms and conditions, pay for access or otherwise engage with the network as the network operator desires.

Widespread adoption of DoT or DoH will stop these DNS spoofing techniques from functioning, which may have negative as well as positive benefits. On a poorly-configured network, DoT or DoH might bypass the captive portal entirely and allow free access to the network. In a stricter implementation, the network would be unable to redirect users to its captive portal and DoT or DoH users might find that all domains fail to resolve and nothing loads correctly.

As DoT and DoH become more widespread, network operators will see an increasing percentage of users for whom their networks are completely non-functional, like in the latter example above. This would present network operators with a difficult choice. Losing the captive portal may mean that businesses which currently provide Wi-Fi access to customers in exchange for payment or viewing advertisements may lose all incentive to provide their network. The shift may also reduce network operators' ability to handle reports of abuse, or malicious or illegal activity on their network because they will no longer be able to tie particular network activity to an identifiable, logged-in user.

Securely mitigating the issues encrypted DNS presents for captive portals is difficult, primarily because captive portals actively rely on techniques – known as "Man-in-the-Middle" attacks – which attempt to break security, which is exactly what DoT and DoH are designed to prevent. Wilfully weakening a security protocol in order to appease the demands of systems which abuse existing protocols should not be encouraged. We must therefore consider alternative mitigations.

One possibility is to call for developers to consider captive portals when they implement DoT or DoH. Developers could develop systems which ensure that DNS queries directly related to a user's activity are always encrypted but which attempt unencrypted DNS queries in the background in order to detecting whether a captive portal is present. Some operating systems and web browsers already provide this kind of functionality in an attempt to streamline connecting to portal-enabled networks. However, research by Google security engineers in 2017 found that "using network probes to detect captive portals is difficult and unreliable."[64] Google's research found unacceptably high rates of false positives (34%) and false negatives (30%) for captive portal detection. Google security engineer Filippo Valsorda has also highlighted the fact that silently probing networks to look for potential captive portals widens a device's "attack surface", as it enables an attacker to trigger the device to load content without user interaction.[65] Valsorda highlights that this has led to vulnerabilities in the past, notably in 2016 when an exploit allowed attackers to remotely execute malicious code on Apple's OS X operating system.[66]

Another potential, and preferable, mitigation would be to create a new standard that could be integrated into operating systems and devices which would provide secure authentication before granting full network access to a new device. This would provide the same functionality as captive portals do now, but would be specifically designed for the purpose, and would not rely on abusing existing protocols.

---

64 Google AI, *Where the Wild Warnings Are: Root Causes of Chrome Certificate Errors*, SIGSAC Conference Paper 2017 <https://ai.google/research/pubs/pub46359>

65 Filippo Valsorda Blog, *A Secure Captive Portal Browser with Automatic DNS Detection*, 16 September 2017 <https://blog.filippo.io/captive-browser/>

66 Common Vulnerabilities and Exposures, CVE-2016-1800 <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1800>

Recommendation:

15. Internet and technology standards bodies such as the IETF and Wi-Fi Alliance should accept that captive portals are a desirable technology for network operators, but that they are outdated and effectively involve attacking user traffic. New standards should be developed to allow users to interact securely with a network operator's content before being granted full network access.

Degraded network monitoring capabilities

Many network operators analyse DNS query data to provide insight about the activity on their network. This does not have to be at the scale of ISP or state-sponsored surveillance; it can be used positively on smaller corporate networks, for example, to detect the presence of malware or complete incident reports after users have been observed connecting to phishing domains. Widespread uptake of DoH will reduce the visibility of DNS traffic in operator's networks. This means that traditional server logs of DNS query traffic will be less representative (or even completely unrepresentative) of overall DNS activity.[67]

Many corporate networks which implement this kind of network monitoring have full control over both the network and the hardware running on it. As a result, there are many device-level solutions which can provide insight about the overall health and activity of network devices. These operators are in a position to limit the impact of DoT or DoH on their network monitoring by configuring devices to use their own DNS resolvers, or by disabling encrypted DNS resolution entirely.

Recommendation:

11. Application developers should ensure that they implement DoT and DoH technology in ways that allow the feature to be configured or overridden by device management software, such as that used by administrators of corporate networks.

Potential privacy concerns arising from encrypted DNS

In some cases, DoT and DoH could result in a negative impact on user privacy, as this section will discuss.

Risk of market centralisation

Concern has been raised that a handful of large providers will dominate the rollout of DoT and DoH servers, and these may have ulterior motives in the form of data collection. This is a valid privacy concern. As noted by a government official quoted in a recent Times article about encrypted DNS: "Google will have a lot more than their searches — it will have their entire browser history. That's an incredible amount of data."[68]

Centralisation is already visible; Cloudflare and Google have been particularly outspoken early adopters of encrypted DNS on their public DNS services. Indeed, Cloudflare's ability to provide high-performing services for a large volume of DNS queries led them to be Mozilla's partner of choice for their experiments testing DoH in Firefox. This caused concern among the Firefox user community, which noted that Cloudflare was already a vastly powerful cloud provider.[69]

Currently, DNS results are returned to users on a decentralised and distributed basis. Most users use the default DNS servers hosted by their network operators, whether on a corporate network or a domestic ISP, which in turn means that, globally, user queries are distributed over a relatively large number of providers. Relatively few users manually configure regular non-encrypted DNS services hosted by large entities such as Cloudflare and Google. The forced rollout of DoT or DoH services could shift this dynamic so that a large number of user queries are sent to already-powerful providers who will be able to collect information on every domain requested.

67 See 59 above.

68 See 11 above.

69 The Register, *Mozilla's opt-out Firefox privacy DNS test sparks, er, privacy outcry*, 20 March 2018 <https://www.theregister.co.uk/2018/03/20/mozilla_firefox_test_of_privacy_mechanism_prompts_privacy_worries/>

While companies who begin to provide encrypted DNS services may implement privacy policies which appear to protect user data, the dominance of a small number of powerful providers will raise issues if a provider decides to weaken its privacy policy whilst continuing to receive large volumes of DNS queries.

Further, it is not necessarily true that encrypted DNS services are largely settling around large cloud service providers simply because they are the early adopters in an early-rollout or 'beta' phase. Software publishers choosing in future to enable DoT or DoH by default may choose a provider without much concern for privacy – for example optimising for performance, a metric which will always favour DNS services operated by large cloud service providers with massively-scalable computing resources.

Developers and programmers who wish to create applications or products with DoT or DoH enabled by default should be aware of the risks of being complicit in the increasing centralisation of power and user data in the hands of a small number of large companies. Developers making these choices have an ethical obligation to ensure that their users' data will be handled in an ethical and protected manner and will not be bought, sold or distributed in contravention of data protection standards including the GDPR and ePrivacy. Developers relying on third-party encrypted DNS services should outline this fact in their privacy policy documents, along with the steps they have taken to protect user data.

Developers could look for inspiration to Mozilla, which outlines a strict list of privacy requirements to which a DoH provider must adhere before they will consider including it in Firefox. Among the requirements: the service may retain user data only for a maximum of 24 hours, and may not sell, transfer or combine it.[70] Ethical application developers should also provide users with an open choice of provider. This could take the form of a provider selection screen, similar to those used by Microsoft after decisions taken in a European anti-competition lawsuit.[71]

Recommendations:

- **12.** Developers creating applications and devices which rely on third-party encrypted DNS servers should avoid becoming complicit in the increasing centralisation of power among a handful of large cloud providers. If left unchecked, this will create central points of failure and give large corporate third-parties access to many users' DNS queries.
- **13.** Developers and application providers should offer users a choice of provider if their product enables encrypted DNS by default.

Google monopolisation

In an interesting modern web dynamic, it appears that DoT and DoH are succeeding where previous efforts have failed, largely due to the support they have found among influential technology vendors – in particular, Google. Google, as developer of both Chrome, which represents 63% of global web traffic,[72] and Android, which represents 75% of the mobile market,[73] carries an unrivalled weight and power with regard to the adoption of new internet standards. Google's control over such a large share of web traffic positions it as judge, jury and executioner for new standards, and it would appear that Google's approval is powering the rise of DoT and DoH.

This does not, however, mean that the technologies Google chooses to endorse are inherently negative or self-serving. Kenji Baheux, involved with implementing DoH in the Chrome browser, outlined some of the guiding principles behind Google's work on DoH, which include: a commitment to retain user control, not to silently force a particular DoH provider on users unexpectedly, and to work with enterprise and educational administrators to avoid hampering device-level filtering efforts.[74]

In short, it is right to raise concerns about the level of power that large entities like Google hold over the architecture of the modern web, and about efforts which could increase the amount of user data Google

70 Mozilla Wiki, *Security/DOH-resolver-policy*, Accessed 31 May 2019, Last modified 9 April 2019 <https://wiki.mozilla.org/Security/DOH-resolver-policy>

71 BBC News, *Microsoft offers browser choices to Europeans*, 1 March 2010 <http://news.bbc.co.uk/1/hi/technology/8537763.stm>

72 See 33 above.

73 See 27 above.

74 See 55 above.

is able to collect from users. However, commentators should not demonise new technologies simply because Google supports them. Google invests development resources into myriad internet technologies, many of which are positive for user privacy and security.

Risks Posed by Rogue DoT and DoH Servers

Whilst DoT and DoH both protect against an eavesdropper logging requests or tampering with the content of responses, it is important to acknowledge that neither technology protects against the potential effects of a rogue DNS server which returns false results for censorship or malicious purposes.

Both DoT and DoH can be deployed in conjunction with DNSSEC to allow client devices to verify the validity of query responses, and this should be encouraged as best practice.

Legal position and Net Neutrality Regulations

Under EU Net Neutrality Regulations, Internet service providers "shall not block, slow down, alter, restrict, [or] interfere with" users' network traffic.[75] Users must therefore be able to pick their own DNS servers at will.[76] Traffic sent by users to those servers must not be manipulated by ISPs, with one notable exception: where an ISP is required to block particular domains in order to comply with national legislation or a court order. This is how current court-ordered blocks are implemented for sites which host content infringing intellectual property rights.[77] A full list of domain blocks ordered by UK courts can be found on Open Rights Group's *Blocked!* project website.[78]

As DoT and DoH adoption begin to decrease the effectiveness of current systems used to implement court-ordered domain blocks, the Government may take an interest in restricting their use. If it does, it should be aware that under EU net neutrality laws, it would not be legal to block or filter encrypted DNS servers without appropriate legislation or a court order. The Government cannot simply demand that ISPs block encrypted DNS servers. Implementing a block on servers operated by an encrypted DNS provider would require specific legal backing and would need to pass tests of proportionality and necessity.[79] Since a DNS provider could be instructed to block specific results, it would be hard to assert that generically blocking that provider in totality was proportionate, unless it was in widespread use and ignoring legal instructions or specifically marketed as a tool to avoid injunction-related blocks.

However, nothing prevents the Government from engaging directly with DoT and DoH providers to request that they block particular domains from returning accurate IP address information when queried. The Government should consider whether working with encrypted DNS providers directly and implementing injunction powers with appropriate proportionality tests would be a more appropriate course of action than blocking encrypted DNS providers themselves.

Recommendation:

4. The Government should not seek to legally block or filter encrypted DNS technologies.

75 Art.3(3) Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN>

76 Art.3(1) of the above Regulation also states that users have the right to "use terminal equipment of their choice". If a device makes use of DoH/DoT to provide its functionality, then network-level restriction of encrypted DNS traffic could be construed as interfering with the user's right to use that particular piece of terminal equipment.

77 See 75 above.

78 See 40 above.

79 BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, para 79.

Data Protection questions and issues

Many third-party encrypted DNS services are arising which, by their nature, are able to observe every domain which a user looks up via the service. Many unanswered questions therefore remain about the data protection landscape with regard to such services. This is especially true where a developer or manufacturer may enable the use of third-party encrypted DNS services without the awareness of an end-user. It would be unreasonable to expect users to be aware of the potential consequences of third-party DNS servers or what may happen to the queries they submit via the device or piece of software.

The legal questions raised are complex and involve various factors which are likely to engage data protection legislation such as GDPR as well as the ePrivacy Directive and upcoming ePrivacy Regulation.

A full analysis of the legal implications of encrypted DNS services is outside of the scope of this paper; however, we strongly encourage developers of applications and devices which will use DoT or DoH by default to take steps to sufficiently inform users of the fact that third-parties may receive their DNS query information, and to ensure that all users always have the ability to opt out of the use of a particular provider, to override providers with their own, or to disable DoT or DoH entirely. We also encourage developers to only enable such third-party services if that service has given concrete assurances through its privacy policy that identifiable user data is not retained, analysed, or sold.

Recommendations:

- 10. Operators of DoT and DoH services (in particular those which may be enabled by default in devices or applications) should ensure that their services do not store any data which may allow end-users to be identified.
- 14. Even if typical users are not expected the benefits or drawbacks of encrypted DNS, developers must not remove user choice from their products. Users should always be able to select their own DNS servers, or to disable DoT and DoH entirely if they wish.

Conclusion

We welcome DNS encryption as a much-needed protocol update to ensure privacy and security over Internet traffic. Whilst we recognise the legitimate concerns raised by actors working to keep the public safe, we largely see DoT and DoH as positive steps forward for individual protection online, and, where these standards present risks and challenges, have identified a set of pragmatic recommendations aimed at mitigating these.

Internet infrastructure and technological operation are complex issues, often requiring expert knowledge to even comprehend, let alone discuss. However, it is increasingly important for rights-based policy actors working in the digital sphere to engage with these issues and grapple with their nuances. The way in which the Internet operates at a technical level determines how government ideas and demands are ultimately implemented and enforced. Technical protocols and standards inform digital policy effectiveness, which in turn shapes individual user experience. Ultimately, how the infrastructure of the Internet evolves fundamentally affects how individuals' fundamental rights are protected, or not. Ongoing conversations and sharing of information and expertise between actors in the Internet ecosystem and policy sphere are therefore essential to keep pace, monitor and check advancements where necessary, and develop sound policy proposals that can be realistically delivered.

It is also often difficult, especially when it comes to technical considerations which can be enveloped in incomprehensible jargon and code-based linguistics, for regular Internet users to know that these types of encryption changes and debates are happening, or to understand what different options or defaults mean for them in terms of data collection, privacy and consumer choice. To support user agency and promote genuine consent, it is vitally important that companies and government provide Internet users with clear, readable information and guidance before, during and after technical changes. After all, it is these users that ultimately lose or gain.

Open Rights is a non-profit company limited by Guarantee, registered in England and Wales no. 05581537

Open Rights Group, Unit 7, Tileyard Acorn Studios, 103-105, Blundell Street, London, N7 9BN

Registered Office: 12 Duke's Road, London WC1H 9AD

www.openrightsgroup.org/contact/

www.openrightsgroup.org