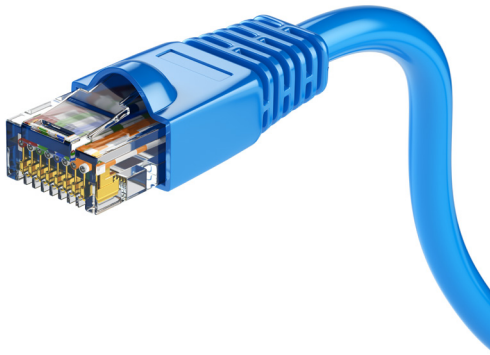
Issue Brief:
DNS over HTTPS

SPP 540: Internet Governance and Information Policy
UMass Amherst

Steve O'Neill
DACSS M.S. Student
December 2023

Increased security? Maybe not.



Internet titans like Google, Cloudflare, and Mozilla are gradually implemeting DNS over HTTPS (DoH), a protocol which directs certain internet traffic towards a few large companies - bypassing ISPs, governments, and corporate network administrators. While the technology has valuable applications in certain regions, it also introduces hidden risks to net neutrality, industry competition, and privacy. This issue brief discusses the impact of DoH on end-users, ISPs, IT administrators, and governments.

Thought of as the "phonebook of the internet", DNS (the Domain Name System) translates human-readable addresses (like www.google.com) to corresponding IP addresses (like 142.250.80.36), letting computers connect to each other after the lookup is completed. To perform the job of DNS, the internet relies on DNS providers. Usually, your DNS provider is decided by where you get your internet service – for example, if you have a Comcast router at home, you are likely to be using a Comcast DNS server. DNS has long been one of the most fundamental – if poorly secured – protocols of the web.

Although much attention has been paid to the global administration of DNS – e.g., the creation of new generic top-level domains like ".amazon" [1] – there is a new protocol on the horizon that is positioned to dramatically change interactions between end users

SOPA/Getty Images

Key Terms

IP Address

A unique numeric identifier - like **54.239.28.85** - associated with a networked computer or website. Analogous to a home address.

Domain Name

Human-readable text associated with an IP address. Example: **amazon.com**.

DNS

Acronym for Domain Name System, a protocol of the internet that translates human-readable domain names to IP addresses. Example: the domain name **amazon.com** is associated with the IP address **54.239.28.85** by DNS.

ISP

An ISP is an **I**nternet **S**ervice **P**rovider: Comcast, AT&T, and Verizon are some of the largest ISPs in the United States.

DoH

Abbreviation of **DNS over HTTPS**, a new protocol for **encrypted** DNS.

and DNS providers at the ground level. Descriptively named “DNS over HTTPS” or “DoH”, the protocol addresses the insecurity of plain DNS, purportedly bringing much-needed modernization to an insecure aspect of the internet. However, in doing so, it also threatens to consolidate the provision of DNS to just a few ‘vetted’ corporate players, having downstream consequences for individuals, ISPs, and governments.

The Bad Old Days

As cybersecurity risks have increased, the desire to protect internet traffic from observation or interference has led to many protocols now common in the everyday internet: first introduced was SSL [Secure Sockets Layer], which introduced basic encryption to web browsing during the “Web 2.0 era” of the late 2000s. Following that, the underpinnings of SSL were developed into TLS [Transport Layer Security] and HTTPS [Hypertext Transfer Protocol Secure], two technologies which have provided encryption for most web traffic since the 2010s.[2]

Conspicuously left out of the encryption scheme of the internet, so far, has been DNS – the initial, preceding connection between a client (say, you) and a 'nameserver' (Comcast’s default DNS server is 75.75.75.75, Google’s is 8.8.8.8) before direct contact with the destination IP is made and HTTPS and TLS can kick in.

"DNS is far from the only insight into your activities that your ISP has."

The specifics of TLS and HTTPS won't be covered here, but the important thing is that they only protect communication between clients after the DNS request has been made. Functionally, this means that even if your web traffic is encrypted through HTTPS (and you see the reassuring “security lock” icon in your browser window), your ISP or employer may still know that you requested a potentially embarrasing or compromising website.

Indeed, even in 2023 with modern browsers like Chrome and Edge, most “lookups” still occur in plaintext, going straight to the DNS server of an Internet Service Provider (ISP) or whichever other DNS server the network administrator has specified.[3] As a matter of practicality and security, corporations regularly host their own DNS servers and rely on DNS filtering for content enforcement and network threat insight.[4]

To some, the open nature of DNS traffic has presented a worrying security hole. To others, including repressive governments, security-conscious organizations, or even parents wishing to block certain content, it has been a useful side door for filtering and monitoring.[5] [6] Generally shared, however, has been a general consensus that something should eventually replace unencrypted DNS.

A New Option

The “DNS over HTTPS” (DoH) standard was proposed in 2018 by the Internet Engineering Task Force (IETF) to address some of the issues above. [7] Officially still considered a work in progress, it has already been adopted by Mozilla Firefox and Google Chrome browsers as de-

2010s

SSL and TLS Gains Popularity Across Web

DNS traffic remains unencrypted

2018

IETF Introduces DoH Draft

Google, Cloudflare, Cisco begin DoH services

2020

Firefox Enables DoH as Default

Cloudflare selected as DoH provider for all Firefox users

2022

‘Oblivious DoH’ Draft Submitted

Experimental protocol seeks to improve privacy of DoH

Who is affected by DoH?

End Users

By shipping off DNS requests to a third party - even using the supposed protection that DoH provides - individuals are giving their sensitive data to yet another corporate intermediary, potentially resulting in a net-negative privacy outcome.

Enterprise Administators

If browser-makers like Google package their own DNS service as the default, organizations are deprived of a basic way filter their own networks for integrity and security.

ISPs

If enabled en-masse, DoH could threaten small ISPs by making the perceived performance of their internet rely on the performance of the biggest DoH provider, creating an incentive for the latter to throttle traffic.

Governments

While repressive regimes may miss the ability to directly inspect their citizens' DNS traffic, they can easily work around this by monitoring IP traffic, essentially nullifying the privacy benefit of DoH. Meanwhile, noteworthy jurisdictional concerns are introduced when DNS data is sent to DoH providers in foreign countries, e.g. the United States, where certain laws on data protection (like the GDPR) do not exist.

fault and configurable options, respectively. Although the IETF has not announced any recommendations for the implementation of DoH so far, it has already been supported in commercial operating systems like Microsoft Windows and Apple macOS since 2020.[8]

End-User Harms

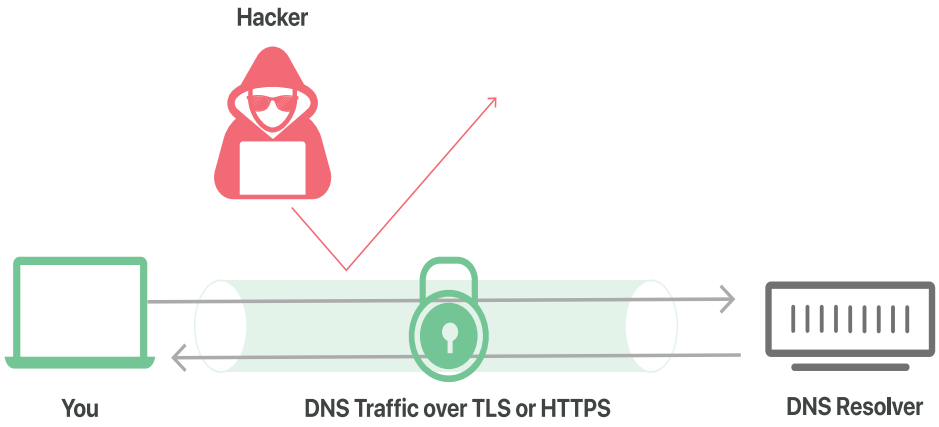
The most controversial feature of DoH is that it sends a personally identifiable stream of DNS queries to a third-party corporate intermediary, e.g. Cloudflare.[9] Communication between you and Cloudflare is encrypted, to be sure, but Cloudflare can still see, record, sell, and “improve its services” based on your DNS queries.[10]

Compare this to traditional DNS, where the covenant between you and your ISP is comparatively straightforward: they will provide you with internet service unless you break the law, and also be expected to comply with lawful subpoenas from your region’s government.

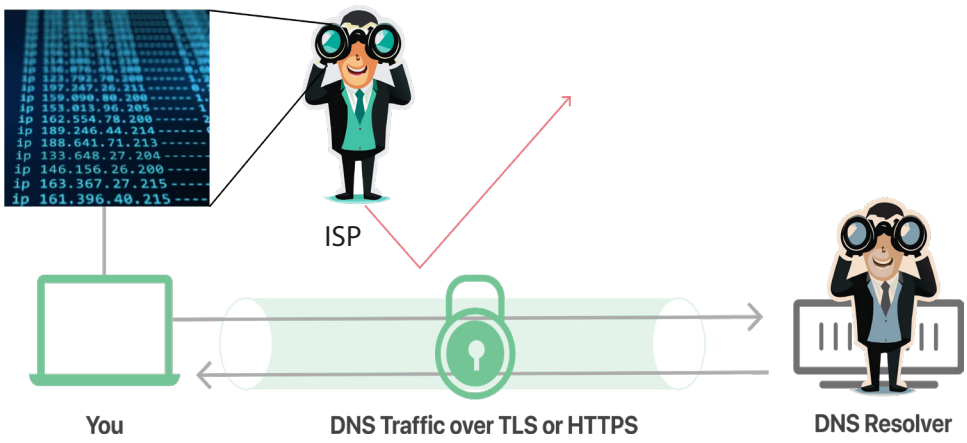
Now, a twist: if you are European and send your DNS requests to Cloudflare, a US-based corporation, you may be sending some of your most sensitive traffic to a region where your government’s data protections do not apply.

Equally, by choosing a "discrete" DoH provider outside of the US, a US-based internet user seeking anonymity may be sending their DNS traffic to a destination where the NSA or CIA can more easily collect the their data without the same due process afforded by just using the ISP's domestic DNS server.

It should be remembered that DNS is far from the only



Top: Infographic by Cloudflare: *"Why does DNS need additional layers of security?"*



Bottom: Author's alternative version of Cloudflare's infographic

"This is the privacy tradeoff implicit in DoH: by removing one small aspect of an ISPs capability to surveil and introducing yet another intermediary, is the new standard really 'more secure'?"

insight into your activities that your ISP has. Although the content of your traffic to most websites is encrypted by HTTPS, ISPs can still see which IP addresses you are connected to, your patterns in visiting them, and any non-HTTPS content you view - regardless of how DNS is provided.[11] Besides your ISP, the websites that you are visiting themselves are likely using cookies, gathering browser metadata, and selling your user data wholesale behind the scenes as well.[12]

This is the privacy tradeoff implicit in DoH: by removing one small aspect of an ISPs capability to surveil and introducing yet another intermediary, is the new standard really "more secure"?

Competitve Harm

The case against DoH gets another dimension when you consider that many DoH providers are also ISPs. Google is a good example: they provide a popular DoH service, easily selectable in Chrome, yet the same company is also involved in the provision of the internet as an ISP (Google Fiber).

Consider the possibility that Google, wanting to expand business in an area, could simply throttle DoH queries by fractions of a second to create a perception of slowness on an incumbent ISPs network. After experiencing frustrating slowness, customers may be keen to switch to Google's "superior" fiber or wireless plan.

The prospect that Google or another DoH provider may throttle their services is not abstract - currently, Google's Public DNS already has a rate limit for ISPs. And while Google itself has not been implicated in anti-competitive throttling of any kind so far, corporations with simillar profiles have been caught throttling web traffic in several instances throughout the decades: Comcast in 2007[13], Verizon in 2014[14], and AT&T in 2019.[15]

Anti-throttling is a core tenet of **'net neutrality'** - the principle that internet service providers should treat all data traveling over their networks equally and without interference.[16] In 2023, the FCC voted to restore net neutrality as a matter of federal policy.[17]

While net neutrality was developed as a way to protect 'content' companies like Google from ISPs seeking to throttle their services, the implementation of DNS over HTTPS now allows the former to turn the tables, shaping an infrastructural 'control point' - DNS - on

Policy Options

End Users

Presently, individuals can choose to accept or reject DoH on their own devices: alternative DoH providers can be selected in Chrome, Edge, Firefox, Android, Mac OS, and WIndows. Despite its drawbacks, DoH is seen as an important tool to "restrict the authoritarian toolbox" in certain countries or territories where internet is filtered with DNS-based methods. It follows that there is no one-size-fits-all application of DoH regulations.

Enterprise Administrators

Organizations seeking to filter their private networks can set up their own DoH services and enforce them on managed endpoints. However, this will not apply on devices that are not managed by IT departments, such as visitors' devices, vendor appliances, IoT devices, or employees' own devices (BYOD).

ISPs

The ISP industry is already lobbying Congress against DNS over HTTPS. Currently, the Electronic Frontier Foundation (EFF) regards these attempts as detrimental to overall security on the internet. However, ISPs may have valid issues to raise with regard to the competitive harm that 'consolidated' DoH could pose, and will likely continue to advocate for stricter regulation around DNS over HTTPS.

Governments

In the interest of fair internet governance, The Federal Communicaitons Commission (FCC) can request to regulate DoH providers under Title I or II of the Telecommunications Act. Cynically speaking, this could be bolstered by the fact that DoH does not meaningfully impact intelligence agencies' ability to surveil domestic internet use.

ISPs themselves.

Then, there's the question of user data: while hardly anyone will regret that ISPs may lose their edge in user surveillance, consider the advantages that only a few companies will reap from the wealth of DNS queries that come tumbling through their DoH endpoints. Google is likely already able to associate click-throughs between its search engine and DoH traffic, letting it observe an individual's internet browsing even after they leave the confines of its own web pages.[18]

Similarly, while Cloudflare's terms of service claim to prohibit selling personal data to most sellers, it includes an exception for improving its own services – DNS or not - and places a carveout for a "research partnership" with APNIC, the regional address registry (RIR) for Asia Pacific. [19] According to the APNIC website, "APNIC works proactively with LEAs [Asia-Pacific Law Enforcement Agencies] to create a better understanding of how the Internet registry system operates". [20] This is a potential area of abuse.

Coming Up Next: ODoH

Oblivious DNS over HTTPS

A July 2, 2018 draft submission to the IETF proposed "Oblivious DNS", stating:

> We argue that no single party should be able to associate DNS queries with a client IP address that issues [DNS] queries. To this end, this document specifies Oblivious DNS (ODNS), which introduces an additional layer of obfuscation between clients and their queries.

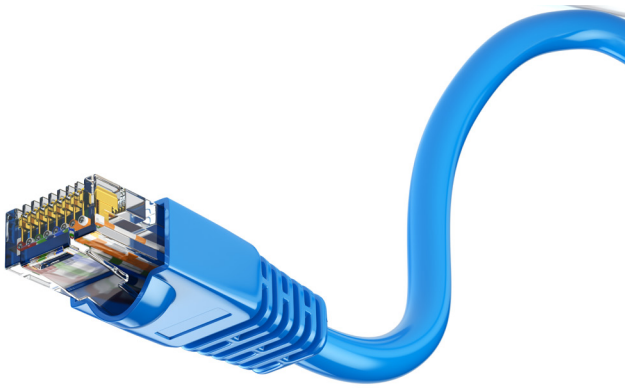
By obscuring the source IP address, a prospective "ODoH" protocol [21] would de-identify DNS queries and improve user privacy.

Such a standard would go a long way towards an increase in security, but still may not be sufficient due to another protocol named SNI, or "Server Name Indication". As an extension of TLS, SNI can reveal which IP a user is connecting from, even if the ODNS protocol is in use.[22] [23]

Regulatory Intervention

Currently the FTC's United States v. Google LLC antitrust lawsuit is investigating Google's dubious practices around default search engine settings.[24] In time, the FTC may take interest in Mozilla's knighting of Cloudflare to provide DNS over HTTPS to all users. Furthermore, the FCC could regulate DNS more stringently, potentially categorizing it as part of a "Title II" telecommunication service. In 2019, a FCC working group acknowledged that DoH adoption "could move DNS query traffic to a small number of centralized providers that are not currently regulated by the FCC", signaling an awareness of the problem.[25]

Overall, bringing DoH providers under the umbrella of regulation could be a worthwhile task.



Prepared By
Steve O'Neill

Student, M.S.

Department of Analytics and Computational Social Science, UMass Amherst

Feedback
stevenoneill@umass.edu

References and Other Sources
https://github.com/thefirstcircle/SPP540-Internet-Governance-Information-Policy