

**DNS New World Order:
QuadX! DoH! DoT!
Da Fuq?**

**Jim Troutman - jamesltroutman@gmail.com
@troutman**

Who is this guy and why is he cranky?

- ❖ Internet "Old Timer" & Engineer, online via a "paper TTY" with a 300 bps acoustic coupler modem in 1982, user of the Internet & UNIX since 1987. Tasked with building and running Internet infrastructure off and on since the early 90s. Have held a wide variety of roles in Internet operations, engineering, and management at various regional ISPs, CLECs, ILECs, cable TV companies, web hosts, and in IT. Independent Consultant for hire.

Disclaimer



NNENIX

**NORTHERN NEW ENGLAND
NEUTRAL INTERNET EXCHANGE**

- ❖ I am also a Director & Co-Founder of the non-for-profit Northern New England Neutral Internet Exchange (NNENIX.NET)
- ❖ Disclaimer: NNENIX hosts servers for Quad9

Topics of Presentation

- ❖ Domain Name System (DNS) in general & new encrypted DNS methods like DNS over HTTPS (DoH), DNS over TLS (DoT).
- ❖ Operational reasons why you should monitor DNS
- ❖ Cloud services offering easy to remember DNS servers & why they would want to give such a gift to the world
- ❖ Privacy implications of Web Browser product decisions
- ❖ Recommendations to mitigate the impact of new DNS encryption methods

New Troubleshooting Procedure

- 1.) "It's not DNS."
- 2.) "There's no way it's DNS."
- 3.) "It was DNS."

Domain Name System (DNS)

- ❖ Initially created in RFC882 in 1983, superseded by RFC1035 in 1987
- ❖ BIND (Berkeley Internet Name Domain) created in 1985
- ❖ DNS is the last major plain text protocol on the Internet.

Domain Name System (DNS)

- ❖ A network service that converts names in a hierarchical structure into IP protocol addresses that IP network use.
- ❖ www.cnn.com “A record”
 - ❖ IPv4 151.101.1.67
- ❖ www.cnn.com “AAAA record”
 - ❖ IPv6 2a04:4e42:200::323

Root DNS Servers

- ❖ 13 Root servers (A through M), operated by 12 different organizations (root-servers.org)
- ❖ Not 13 individual servers! Clusters of servers, with load balancers, and many Anycast instances
- ❖ Some root servers have ~160 separate physical instances around the world
- ❖ Allows scaling of traffic volumes, increase resiliency and redundancy, especially against directed attacks

Root DNS Servers

- ❖ Each root server gets double-digit billions of DNS queries per day
- ❖ Trillions of DNS queries answered per month
- ❖ DNS has scaled over 9 orders of magnitude over 35 years, and will continue to so

IP Anycasting

- ❖ Anycast is a technique where a unique IP address block is advertised in multiple physical locations, to different sections of the Internet, at the same time via BGP routing.
- ❖ Routing decisions “steer” traffic to the “best” nearest instance of that IP address via BGP decision making.
- ❖ Use for massively distributed services like the DNS root servers & DNS Cloud Providers

Traditional DNS (Do53)

- ❖ RFC882/RFC1034 and others
- ❖ Plain text protocol
- ❖ UDP Port 53 for queries, TCP Port for 53 for Zone file transfer to secondaries
- ❖ Some call it Do53 now
- ❖ Largely the same since 1985: ~35 years!

Traditional DNS (Do53)

- ❖ Because of plaintext, can be monitored over the wire easily
- ❖ Incredibly useful for knowing what your endpoints are up to, and finding malware & C&C traffic on your network

DNSCrypt

- ❖ 2011 - no RFC process, not done through IETF
- ❖ DNS over TCP/UDP Port 443, but not TLS
- ❖ Solved a lot of problems, but didn't get much traction at the time

DNS over TLS (DoT)

- ❖ RFC7858 May 2016, updated by RFC8310 March 2018
- ❖ Uses TCP Port 853 with TLS encryption
- ❖ Supported by Android 9+ for whole OS
- ❖ Microsoft has stated will support at Windows OS layer soon

DNS over HTTPS (DoH)

- ❖ RFC8484 December 2018
- ❖ Uses TCP Port 443 with TLS encryption
- ❖ DNS queries over a special HTTP GET with JSON responses
- ❖ Can be several milliseconds slower than Do53

DNS in the Cloud (DoC)

- ❖ For many years there have been “public” resolver DNS servers, operated mostly by ISPs as a public resource.
- ❖ 4.2.2.2
- ❖ 75.75.75.75
- ❖ lots of others

DNS in the Cloud (DoC)

- ❖ Google launched their service of 8.8.8.8 in December 2009
- ❖ To improve speeds and user experience verses old broken ISP DNS
- ❖ Also useful to work-around censorship issues at the time



@KADIKOYBASKA

DNS in the Cloud (DoC)

- ❖ Now there are others
- ❖ Cloudflare 1.1.1.1
- ❖ Quad9 9.9.9.9
- ❖ also other services like OpenDNS (Cisco Umbrella) 208.67.222.222

DNS is great for tracking

- ❖ If you can monitor DNS queries, you can know everywhere someone goes online
- ❖ Shopping, entertainment, work, medical sites, etc.

DNS comes great power

- ❖ If you control DNS, you can control where users go or don't go.
- ❖ Of course, DNS monitoring is great for fighting malware and intrusions
- ❖ Essential for blue team network defense

DNS = Monetization for ISPs

- ❖ Many (most?) large ISPs, CATV, ILECs, sell their customer's DNS information to advertising and tracking companies
- ❖ And they can tie it to YOU at your house
- ❖ \$3-5/user per year estimates

Web Browsers Pushing DoH

- ❖ Firefox 62, released in September 2018 added support for DoH through flags
- ❖ Firefox 72 (January 9th, 2020) has DoH as option in Network Settings
- ❖ They are enabling this in USA, just giving you the option to opt out.

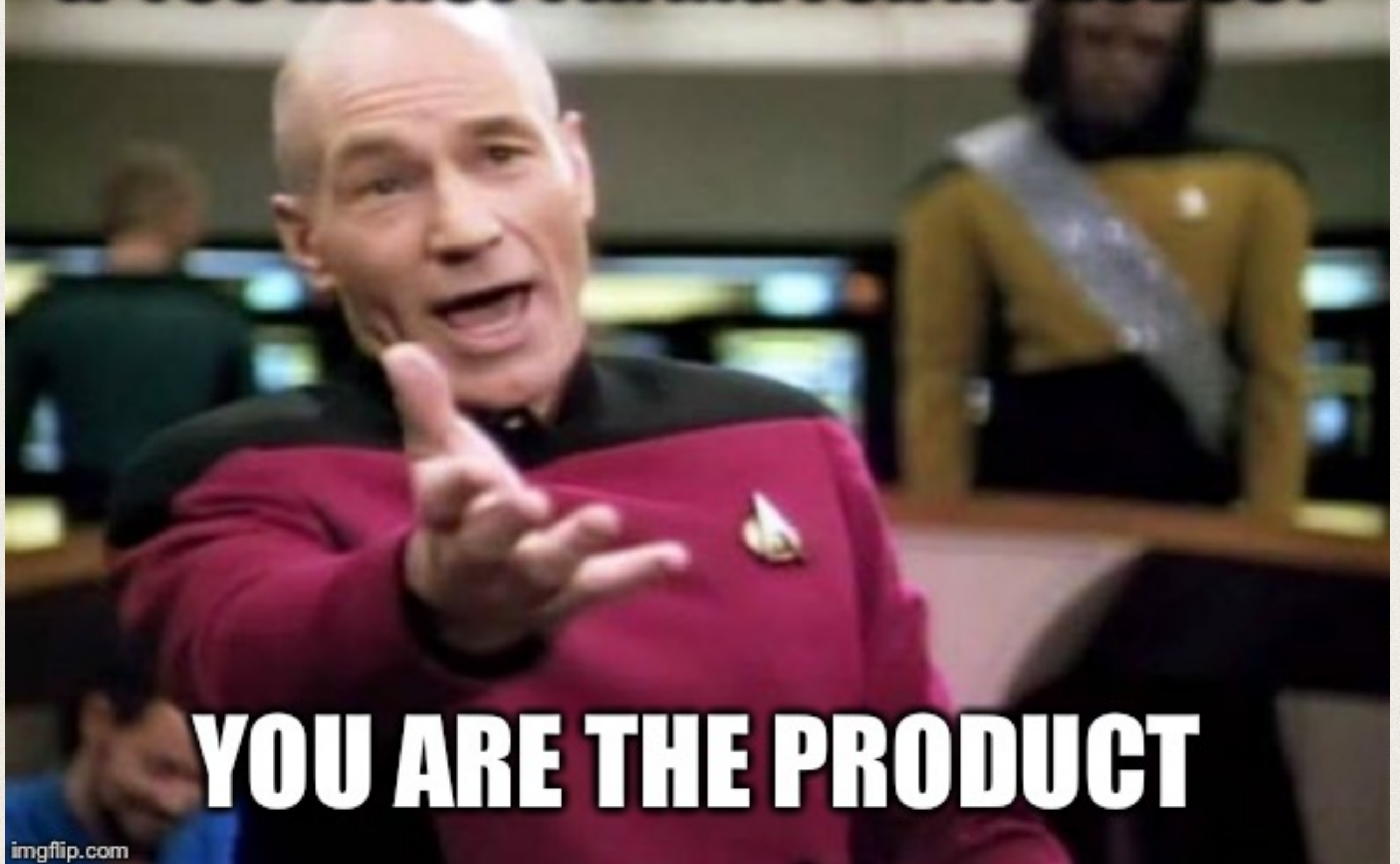
Web Browsers Pushing DoH

- ❖ Mozilla picked CloudFlare as first and default DoH provider. Requirements to honor and a contract
- ❖ Domain Name canary to disable if you control your DNS (so ISPs can disable DoH in Firefox, unless you override)
- ❖ A second non-CloudFlare DoH option will be coming soon - NextDNS.io

Web Browsers Pushing DoH

- ❖ Chrome supports DoH, not enabled by default
- ❖ Chrome will have a GPO to disable DoH entirely
- ❖ Microsoft chromium Edge browser supports
- ❖ Opera supports, not enabled by default

IF YOU'RE NOT PAYING FOR A PRODUCT



YOU ARE THE PRODUCT

imgflip.com

DoC = Surveillance

- ❖ Not all of the cloud providers have clear privacy policies.
- ❖ Data retention can be 24 hours to 2 years, if spelled out at all.
- ❖ Aggregate data trends kept for long time
- ❖ However...



Richard Bejtlich ✓
@taosecurity

Replying to [@dangoodin001](#)

DoH is an unfortunate answer to a complicated problem. I personally prefer DoT (DNS over TLS). Putting an OS-level function like name resolution in the hands of an application via DoH is a bad idea. See what [@paulvixie](#) has been writing for the most informed commentary.

7:16 PM · Sep 10, 2019 · [TweetDeck](#)



Nick Sullivan ✓ @grittygrease · Oct 20, 2018

DNS Queries over HTTPS (DoH) is now RFC 8484. This is a big step forward for DNS security. rfc-editor.org/rfc/rfc8484.txt

15

356

692



Paul Vixie
@paulvixie

Replying to @grittygrease

Rfc 8484 is a cluster duck for internet security. Sorry to rain on your parade. The inmates have taken over the asylum.

5:49 PM · Oct 20, 2018 · [Twitter Web App](#)

25 Retweets **73** Likes



Bert Hubert 
@PowerDNS_Bert



Replying to [@bortzmeyer](#) and [@FernandoGont](#)

DoH encrypts precisely zero data that is not already present in unencrypted form. As it stands, using DoH only provides **additional** leaks of data. SNI, IP addresses, OCSP and remaining HTTP connections still provide the rest. It is fake privacy in 2019.

8:10 AM · Sep 22, 2019 · [Twitter Web App](#)

11 Retweets **26** Likes



da_667.jpg.ps1

@da_667



-DoH is terrible, does nothing you think it actually does, and is essentially repeating the same mistakes we collectively made from the PRISM program: consolidating trust with confidential data to organizations that very clearly don't deserve it.

8:26 PM · Jan 2, 2020 · [TweetDeck](#)

15 Retweets **32** Likes



Tony Finch @fanf · Sep 8, 2018

youbroketheinternet.org/trackedanyway - **TLS session resumption** allows Google and Facebook to track you without cookies.



- ❖ This was new to me - TLS Session Resumption Tickets
- ❖ Can be used to track you everywhere by resuming old TLS sessions (HTTPS apps including DoH) across days.

DoC = Surveillance

- ❖ All these providers and cloud services are USA based and subject to National Security Letters, FISA 702, and other ways
- ❖ logs with detailed information about your Internet sessions can be grabbed by governments and law enforcement without disclosure

A meme featuring a smiling man in a Star Trek uniform. The text "HE WHO CONTROLS DNS" is overlaid at the top in large, white, bold, sans-serif font with a black outline. The text "CONTROLS EVERYTHING" is overlaid at the bottom in the same font style.

HE WHO CONTROLS DNS

**CONTROLS
EVERYTHING**

Recommendations

- ❖ Run your own internal recursive DNS server
- ❖ best performance by far!
- ❖ implement canary domain to block auto-enable of DoH for Firefox
- ❖ Your logging/monitoring goes here

Recommendations

- ❖ On your firewall
 - ❖ Block all outbound TCP/UDP Port 53 for all endpoints for regular DNS
 - ❖ Force endpoints to use internal DNS
 - ❖ Block TCP 853 to block DoT

Recommendations

- ❖ Set your endpoint configuration standards to disable DoH in browsers
- ❖ Point endpoint DNS servers to internal recursive only (via DHCP, GPO, static configs, regkeys, etc.)

Recommendations

- ❖ Use dnscrypt on your local internal recursive server to talk to the outside world
- ❖ will encrypt your DNS lookups to a public DNSCrypt server
- ❖ use a dnscrypt server with enough traffic to get “privacy mixer” herd protection for queries - in a GDPR country

Recommendations

- ❖ Consider internal network IP capture of all of the well known public DNS resolvers in addition to universal block at the edge
- ❖ Many IoT devices use hardcoded DNS
- ❖ Many, many ISPs and hotel networks do this already now — you don't always talk to the actual server you think you are

IT'S ALWAYS DNS



ALWAYS

memegenerator.net

Thank you!

- ❖ This slide deck will be available
- ❖ jamesltroutman@gmail.com
- ❖ Twitter: [@troutman](https://twitter.com/troutman)

Selected Bibliography & Resources

- ❖ https://en.m.wikipedia.org/wiki/Public_recursive_name_server
- ❖ <https://arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them/>
- ❖ <https://www.eff.org/deeplinks/2019/10/dns-over-https-will-give-you-back-privacy-congress-big-isp-backing-took-away>
- ❖ <https://digital.com/blog/isp-tracking/>
- ❖ <https://www.icsi.berkeley.edu/pubs/networking/redirectingdnsforads11.pdf>
- ❖ <https://epic.org/privacy/nsl/>

Selected Bibliography & Resources

- ❖ https://archive.fosdem.org/2019/schedule/event/dns_privacy_panel/
- ❖ <https://blog.powerdns.com/2019/02/07/the-big-dns-privacy-debate-at-fosdem/>
- ❖ <https://www.powerdns.com/dohdot.html>
- ❖ <https://www.isc.org/blogs/qname-minimization-and-privacy/>
- ❖ <https://blog.cloudflare.com/announcing-1111/>
- ❖ <https://www.zdnet.com/article/dns-over-https-causes-more-problems-than-it-solves-experts-say/>

Selected Bibliography & Resources

- ❖ <https://blog.cloudflare.com/encrypted-sni/>
- ❖ <https://www.zdnet.com/article/dns-over-https-will-eventually-roll-out-in-all-major-browsers-despite-isp-opposition/>
- ❖ <https://support.mozilla.org/en-US/kb/dns-over-https-doh-faqs>
- ❖ <https://support.mozilla.org/en-US/kb/canary-domain-use-application-dnsnet>
- ❖ <https://support.google.com/chrome/a/thread/10152459?hl=en>
- ❖ <https://www.chromium.org/developers/dns-over-https>

Selected Bibliography & Resources

- * <https://nakedsecurity.sophos.com/2018/10/25/could-tls-session-resumption-be-another-super-cookie/>
- * <https://www.darkreading.com/vulnerabilities---threats/benefits-of-dns-service-locality/a/d-id/1333088>
- * http://www.circleid.com/posts/20100728_taking_back_the_dns/
- * http://www.circleid.com/posts/20120103_dns_firewalls_in_action_rpz_vs_spam/
- * <https://blogs.akamai.com/2017/06/why-you-should-care-about-dns-latency.html>

Selected Bibliography & Resources

- ❖ <https://www.dnsleaktest.com/>
- ❖ <https://www.privacytools.io/providers/dns/>
- ❖ <https://blog.powerdns.com/2019/09/25/centralised-doh-is-bad-for-privacy-in-2019-and-beyond/>
- ❖ pi-dns.com
- ❖ <https://dnscrypt.info>

Selected Bibliography & Resources

- ❖ Privacy Policies
- ❖ <https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/security/umbrella-privacy-data-sheet.pdf>
- ❖ <https://www.quad9.net/policy/>
- ❖ <https://developers.cloudflare.com/1.1.1.1/commitment-to-privacy/>
- ❖ <https://developers.google.com/speed/public-dns/privacy>