DoH ecosystem update for LINX 108

What's happening with standards, browsers, resolvers, ISP trials and impact areas to watch

Andy Fidler, Principal Network Architect, BT Technology

What is DNS and why is it important to ISP services?

- Domain Name System (DNS) prime role is to turn user friendly domain names into Internet Protocol Addresses to allow devices and content servers to identify and connect to each other on the internet – "The phonebook of the internet".

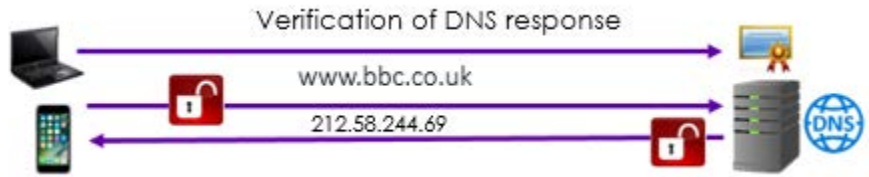
- Based on Internet Engineering Task Force (IETF) standards dating back to the 1980's and all data sent unencrypted.

- ISPs also use DNS information to support wider service capabilities:
  - Routing customers to local content caches
  - Broadband personalised content filtering
  - Malware protection
  - Regulatory / Court Order Blocking
  - Cybersecurity
  - Service support, e.g. device / hub set-up, mobile PAYG top-up, etc.

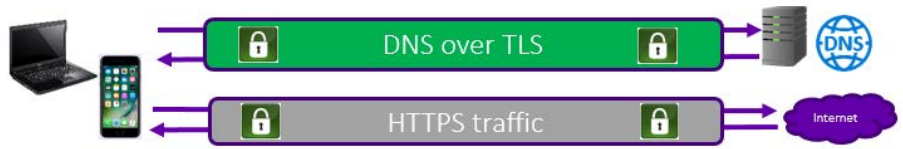
- Currently the majority of Internet clients use the serving ISP's DNS by default.

What are the various flavours of Encrypted DNS?

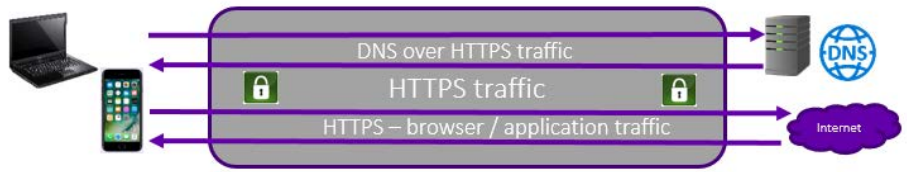
- **DNS Security (DNSSEC) – lets you verify that the DNS answers you receive are genuine but does not encrypt flow.**



- **DNS over TLS (DoT) – encrypts DNS requests / responses and uses a dedicated flow, separate from other device traffic.**



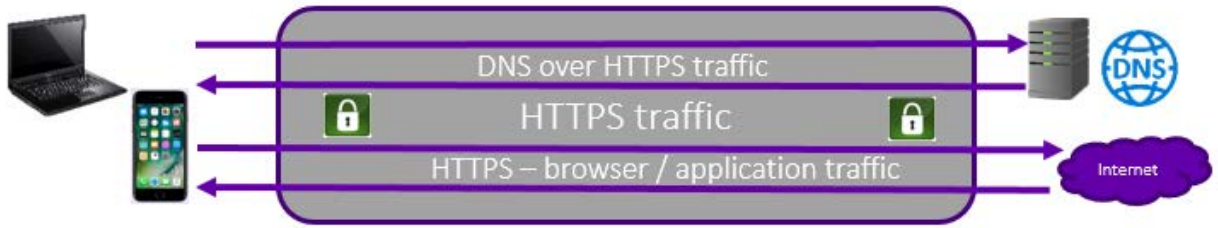
- **DNS over HTTPS (DoH) – encrypts DNS requests but mixes these in with encrypted HTTPS device traffic.**



- **Adoption will be driven by applications and devices. Network ecosystems need to evolve to support all options.**

What are the key DNS functions & models in the DoH ecosystem?

Client



Server

Browsers, Applications & Operating Systems Initiating the requests.

Two different support models

1. Default ON to a Centralised DoH resolver
   - Firefox (US)
2. Same Provider Only auto upgrade
   - Chrome, MS Windows

DoH Recursive Resolvers responding to Domains with IP addresses.

Two different support models

1. Distributed ISP Resolvers
   - Closed to just ISP customers & ISP networks
   - Open to all
2. Centralised Cloud Resolvers Open to all

Circa 40 DoH Public open resolvers available

What is the latest status on Browser / OS support for DoH?

- **Mozilla:**
  - **Phased roll-out of default ON in the US to Cloudflare**
  - **Recently added NextDNS as alternative custom DoH provider option, non-filtered service only**
  - **Support detection of existing ISP policies through a canary domain approach.**
  - **Not presently planning on implementing a default ON approach in the UK.**

- **Google:**
  - **Started experimenting with DoH functionality in Chrome 79.**
  - **Targeting Chrome 82 (stable ~April) for DoH privacy and security capabilities.**
  - **Default "same-provider auto-upgrade behaviour", only automatically upgrades if existing provider supports DoH.**
  - **Manual configuration options.**

- **Microsoft:**
  - **Early experiments with Windows DoH capabilities.**
  - **Considering DoH default on approach if existing DNS provider is on a recognised list of DoH providers.**

- **Apple:**
  - **Several proposals into IETF around DoH discovery.**

Where are the IETF with DoH?

- RFC8484 standard covering DoH requests and response protocol
- However this on its own does not fully cover all customer experience, application and operator aspects, e.g. DoH Discovery.
- Great to see the IETF forming a new Working Group – Adaptive DNS Discovery (ADD).
  - https://mailarchive.ietf.org/arch/msg/ietf-announce/mKMLvtwdF9XZ5Pz9GyVtGYzi9LM
- Encourage people to join in the discussions on the ADD mailing list and attend IETF 107 (21st-27th March) either in person or remotely.
  - https://www.ietf.org/mailman/listinfo/add

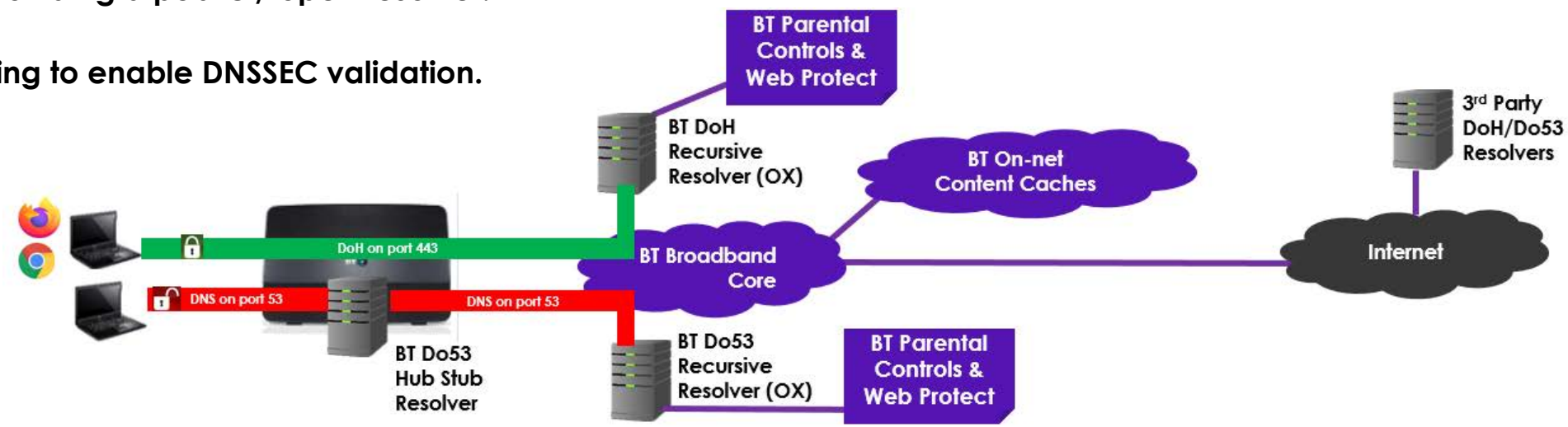
What about key Industry Alliances / Associations too?

- Encrypted DNS Deployment Initiative (EDDI) – defining user cases and deployment guidelines.
- UK ISP Association (ISPA) – exploring a UK model policy for trusted DoH resolvers.
- European Telecommunications Network Operators (ETNO) – published a positioning paper on DoH.
- GSMA.

BT

What is BT doing on DoH?

- **Running a DoH Experimental trial capability since 6th December, 2019.**
- **Available* at https://doh.bt.com/dns-query/ with test page at http://splashpage.doh.bt.com**
- **Currently testing across small base of BT employees.**
- **Built on and working with OpenXchange / PowerDNS.**
- **Supporting only IPv4 and RFC8484 implementation.**
- **For the trial providing a public / open resolver.**
- **Shortly planning to enable DNSSEC validation.**



***Please note this is not an official service in any way.** It is purely experimental, may not offer similar service performance to live services and may be taken out of service without notice. The experimental capability should support any existing BT customer parental control and/or web protect settings, however if you are testing the capability on family devices we would recommend that you check that parental controls are still applied. Personal data will be processed in accordance with BT's Privacy Policy - https://www.bt.com/privacy-policy/

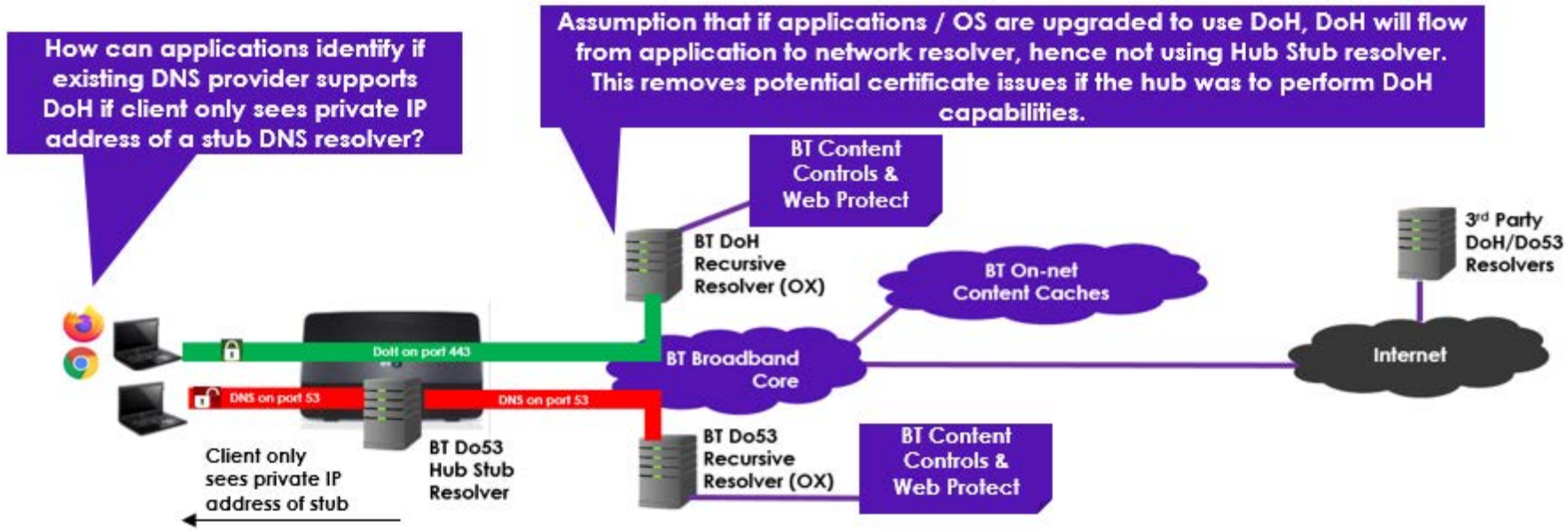
What are the key DoH impact areas network operators should consider?

- How will users discover and enable DoH and impact from current lack of a standardised discovery protocol?
- Impact of DoH on:
  - Wi-Fi captive portals
  - On-net content caching
  - DNS based content filtering
  - Court order / regulatory blocking & cyber security
  - Customer support
  - Page download response times & Industry performance metrics
- Potential additional server capacity overhead from TLS encryption
- Risks from variations in TLS/DoH settings without Best Current Practice guidelines
- Cookie handling and DoH namespace guidelines

Impact area #1 – lack of DoH Discovery Protocol

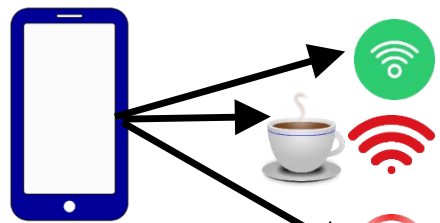
- Current plans for DoH "same provider auto upgrade" will only work for a subset of broadband users where hubs present a public IP address for the existing DNS resolver.

- Many UK and European ISPs using stub resolvers in hubs which only provide a private IP address, thus breaking this approach.



- To make DoH available to all the IETF need to develop a standardised context aware DoH Discovery Protocol

Devices & applications need to be context aware, offering DoH options for various network connection scenarios.



Trusted Home Broadband Wi-fi:
ISP DoH or Cloud DoH

Un-Trusted Coffee Shop Wi-fi:
Cloud DoH

Trusted Mobile Network:
ISP DoH or Cloud DoH

Impact area #2 – Wi-Fi Captive Portals

- Most public Wi-Fi providers do not pass TCP 443 until the end user has logged on to accept T&Cs and/or pay

- Login will be via a captive portal and to find that clients will need to use Do53
    - Or in some cases DoT or a DoH server within the captive network
    - Back to the need for a standardised DoH discovery protocol

- Do53 is likely to be the lowest common denominator for pre-login public Wi-Fi.

- Does this introduce an element of security and privacy risk, could this be exploited?

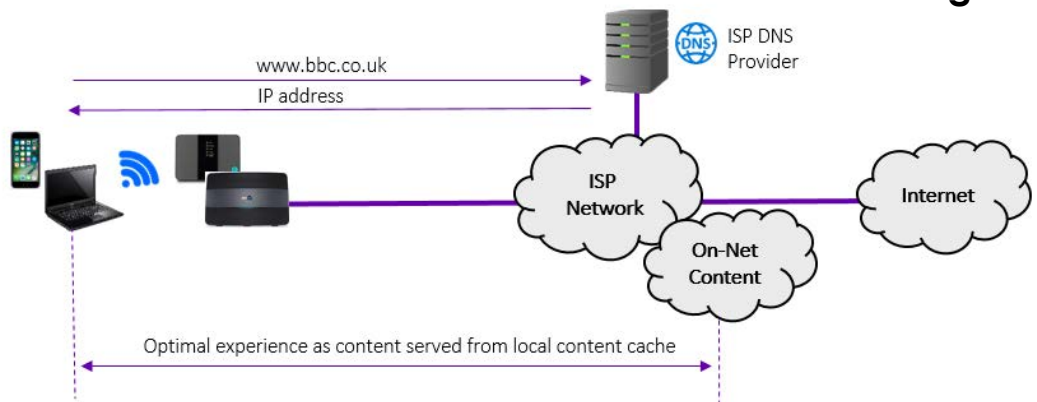
- But could this mitigated by device Captive Network Assistants not allowing access beyond this until sign-up is completed?

- Could public Wi-Fi providers also look to white list known DoH resolvers?

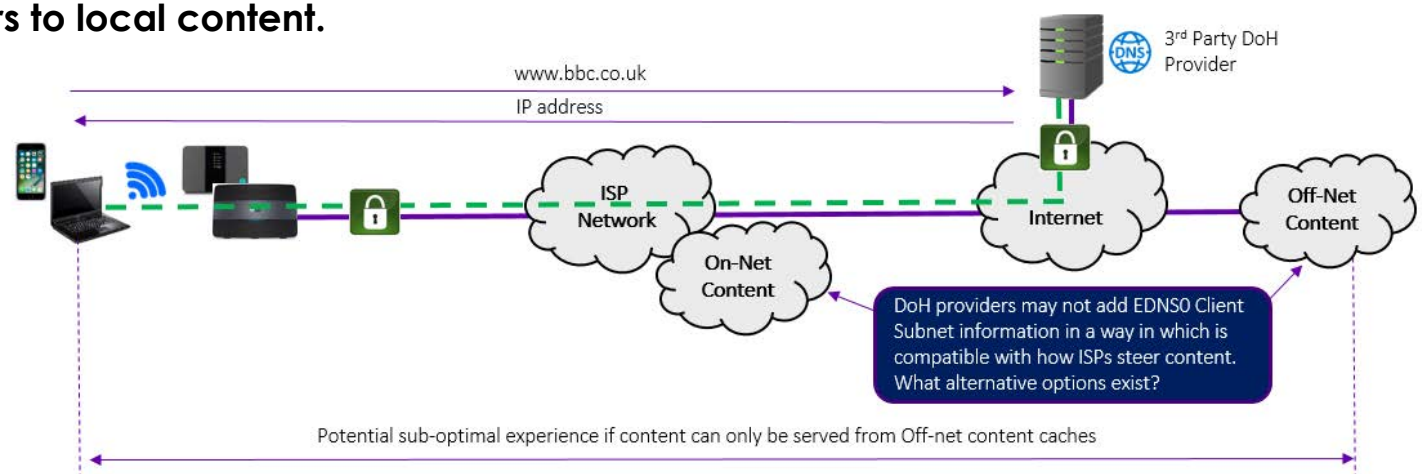
- Will IETF CAPPORT (Captive Portal Interaction) address all of these aspects in the longer term?

Impact area #3 - On-net Content Caching

- **ISPs and Content Delivery Network vendors have invested in On-Net content caches to give consumers the best experience and minimise network costs.**



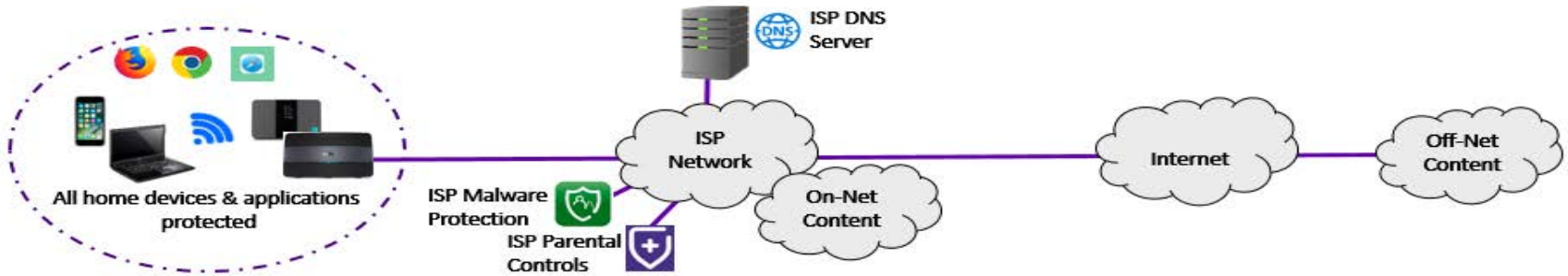
- **These Customer Experience and network cost benefits could be impacted if DoH providers block DNS information (ECS) used by ISPs to route customers to local content.**



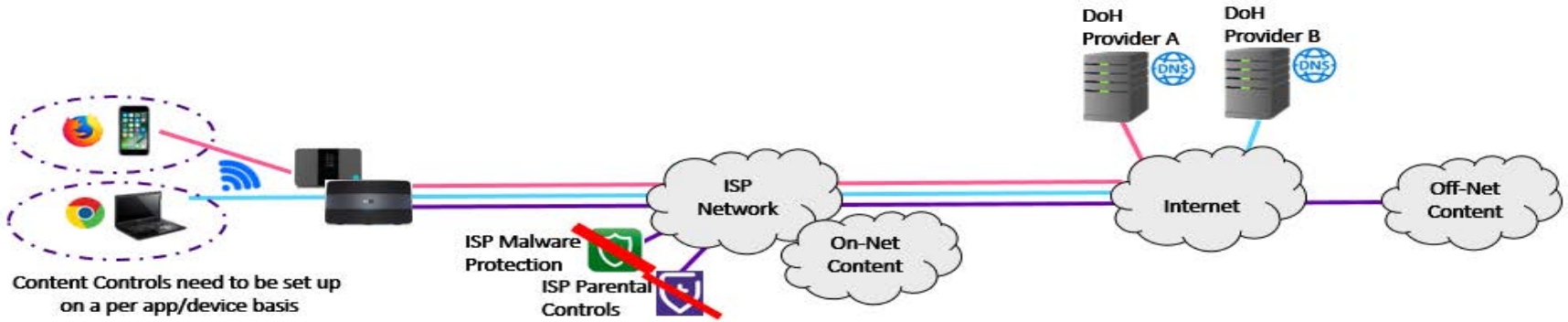
- **Do we risk some users getting less localised results and a suboptimal experience even if DNS resolution is improved?**

Impact area #4 – DNS based content filtering

- Presently most UK ISP broadband customers can set content protection settings once and then be reassured that all their home network devices - smartphones, tablets, game consoles are protected in terms of content controls and malware blocking.



- With DoH, customers may need to set-up content filtering on a per device / application basis, risking inconsistent experiences.



- Will customers realise if they change to 3rd party DoH providers, it will bypass their existing ISP content filtering?
  - Use of canary domains to detect existing policies will help here, but more work is needed to standardise approach.
  - Plus should policy detection apply to both auto discovery and custom / manual entry?

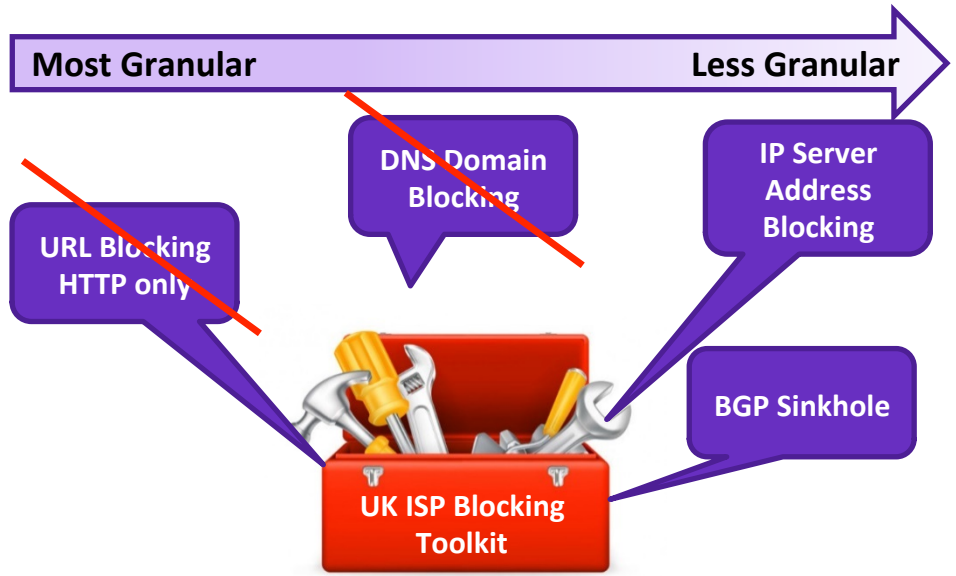
Impact area #5 – Court Order / Regulatory Blocking & Cyber Security

Blocking required by law:

- URL and Domain blocking are the more granular tools in the kit box used by UK ISPs to block, e.g. court orders.
- If UK ISPs are no longer in the DNS path, this could significantly undermine the efficacy of e.g. court or regulation orders.
- Instead a court or regulator may need to approach a collection of 3rd party DoH providers, who may be based outside local jurisdiction.
- Microsoft Windows and Google Chrome "same provider auto upgrade only" gives BT confidence around continued use of existing ISP DNS content filtering in the short to medium term.

Cyber Security:

- Reduced ability to derive cyber security intelligence from malware activity and passive DNS insight
- Will DoH offer up significant new attack opportunities for hackers?
- Will the adoption of new encryption protocols drive a demand for new tools within the ISP toolkit?



Note BT blocking of IWF blocklist via Cleanfeed will not be impacted by DoH.

Impact area #6 – Customer Support & Performance Benchmarks

Customer Service:

- ISPs may use DNS redirects for service support, e.g. device set-up & account support
- Will these capabilities be bypassed/impacted by DoH?
- When customers have issues, will they know who to contact? Their ISP or 3rd party DoH provider?

Industry Performance Benchmarks:

- Web browsing speed, latency, DNS resolution, DNS failure
  - Fine when majority of ISPs customers are using their DNS.
  - But is a new approach needed to consider impact of increased 3rd party DNS usage?
  - Plus distinguish between DoH and Do53 performance?
- What about the wider impact of HTTP/3 QUIC on measures?

Early DoH vs Do53 Comparison results from BT Trial:

Full look up time (s)	BT	Cloudflare	Google
DoH curl	0.34 (TLS 1.2)	0.26 (TLS 1.3)	0.20 (TLS 1.3)
Do53 pingu	0.013	0.014	0.02
Do53 curl	0.066	tbc	0.109

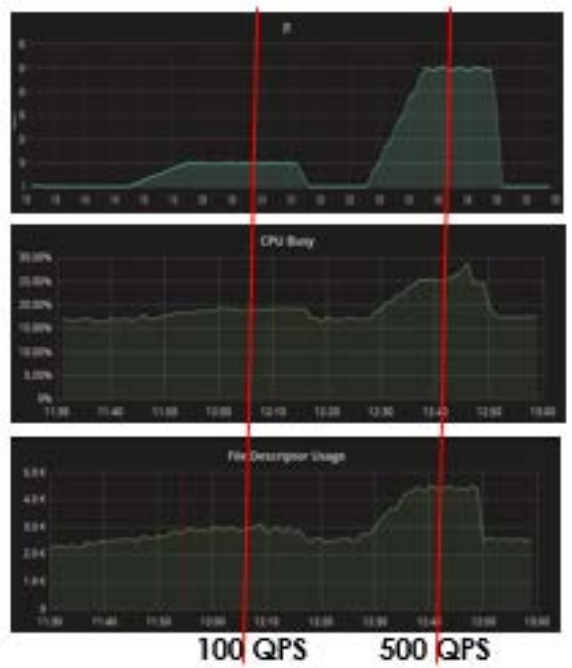
- Early measurements are suggesting DoH has greater latency due to TLS set-up.
- However BT is still exploring whether existing test probes are ideal for DoH. To assist this BT will shortly be testing DoH vs Do53 comparison with a small number of Sam Knows Whiteboxes in the field.
- It should also be noted that BT curl measurements reflect the worst case scenario of a TLS session per query.

Impact area #7 – Additional capacity overheads

- BT DoH trial measurements showing that using TLS1.2 instead of TLS1.3 with DoH adds an overhead

Full look up time in seconds from UK BT Broadband line	Cloudflare DoH	Google DoH	BT (UK) DoH	DT (Germany) DoH	Comcast (US) DoH
	TLS 1.3		TLS 1.2		
Facebook.com	0.260	0.267	0.262	0.414	0.610
a2.w10.akamai.net	0.263	0.271	0.277	0.317	0.835
google.co.uk	0.239	0.245	0.272	0.326	0.608
BT is observing that TLS 1.2 adds an overhead compared TLS 1.3					

- Early results from load tests seem to be implying a higher than expected TLS overhead on server capacity.



200 & 1k QPS distributed servers.
10% CPU increase
100% file descriptor increase

NB: Background trial usage < 10 QPS

Impact area #8 – variations in TLS/DoH settings without BCPs

- BT has run Curl tests* against 21 DoH providers, highlighting some interesting variations and need for Best Current Practices deployment guidelines.

DoH Provider	TLS 1.3	OCSP Stapling	Session ID Duration (s)	Ticket Session (s)	Cipher Choice
Cloudflare	Yes	No	7200	172800 (2 days)	TLS_AES_256_GCM_SHA384
NextDNS	Yes	No	7200	604800 (7 days)	TLS_AES_256_GCM_SHA384
PowerDNS	Yes	No	7200	7200	TLS_AES_256_GCM_SHA384
Comcast	No (TLS 1.2)	No	7200	No	ECDHE-RSA-AES256-GCM-SHA384
Deutsche Telekom	No (TLS 1.2)	No	7200	7200	ECDHE-RSA-AES256-GCM-SHA384
Andrews & Arnold	Yes	No	7200	7200	ECDHE-ECDSA-AES256-GCM-SHA384 TLS_AES_256_GCM_SHA384
Google	Yes	No	7200	172800 (2 days)	TLS_AES_256_GCM_SHA384
BT Plc	No (TLS 1.2)	Yes (7 days)	7200	300	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384

*Results based on tests run on 27/12/19

Saves client having to check status with CA.

Plus what about in-band authentication?

Client servers need to hold session resumption artefacts. Will 7200s take-up too much memory as DoH scales, should it be lower?

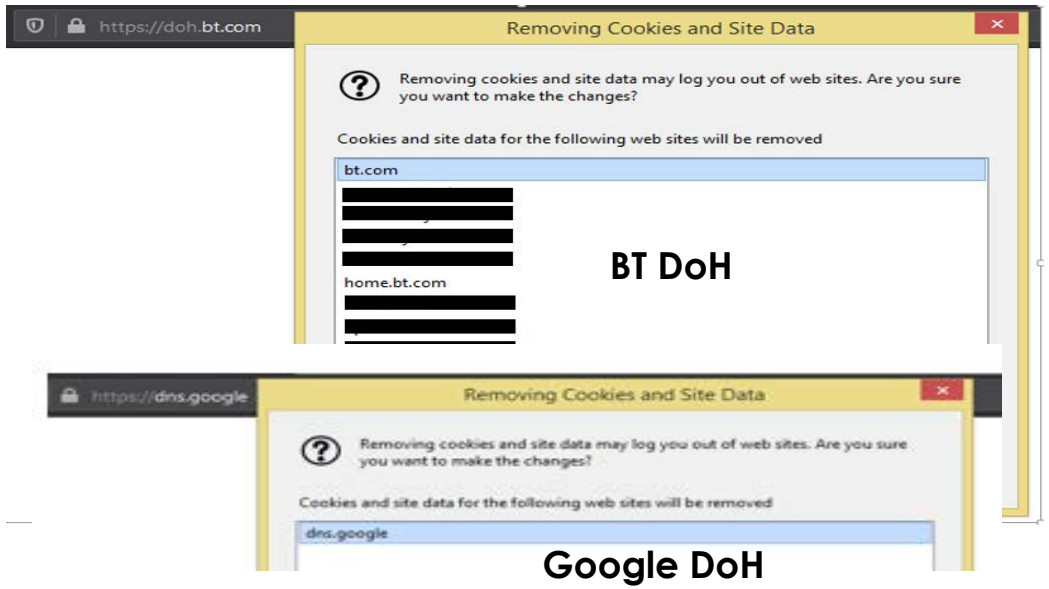
Why so varied and some so long?

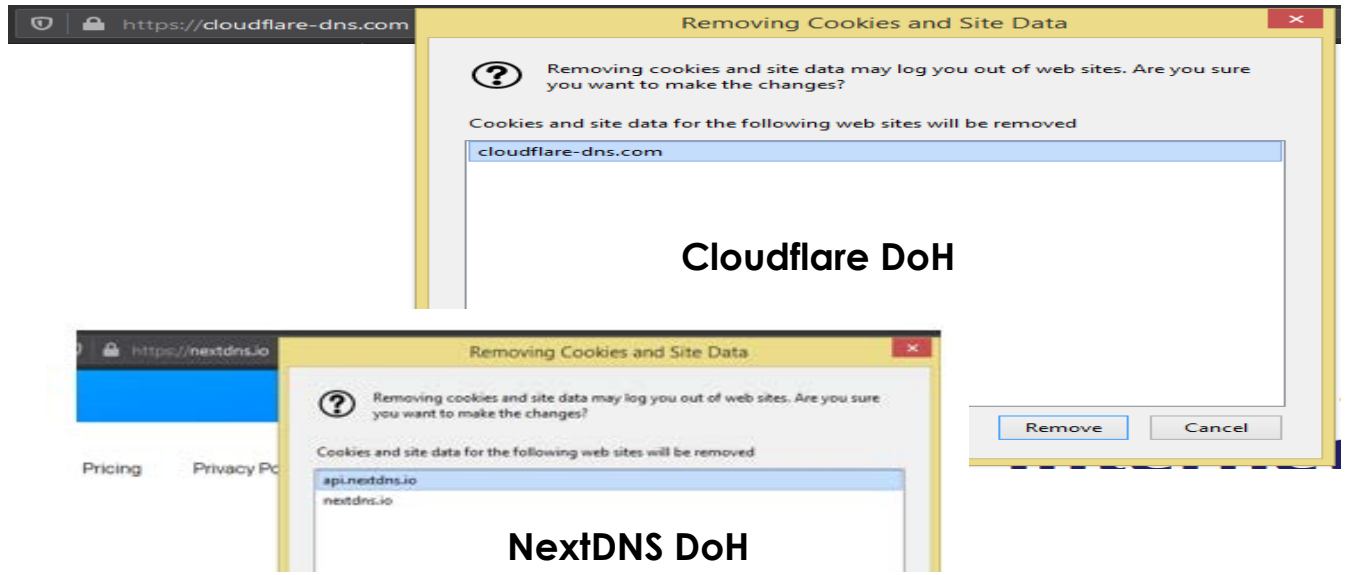
What's the best balance here between privacy and user experience?

Variation in Cipher Choice.

Impact area #9 – Cookie & Namespace guidelines

- User interfaces and policies may not be clear on how cookies are handled across browser and DoH databases. We appear to be seeing the browser side mention cookies for DoH domains.
  - We assume this is due to visiting the domain itself, but would welcome user interface clarity on which cookies are present in which database, and confirmation that browsers and DoH servers are not sending / accepting cookies in DoH messages.





- Further clarification may needed in DoH BCPs and subsequent I-D's / RFCs to state that:
  - Clients should not accept "Set-Cookie" as part of a DoH response.
  - Clients should not send "Cookie" headers they have previously learned for the relevant domain.
  - DoH servers should disregard Cookies.
  - Guidance on DoH namespace.

Conclusion

- Good direction with more DoH resolvers and trials
- However many open issues still exist
- Many of which will hopefully benefit from the creation of the new IETF ADD Working Group
- A standardised DoH discovery protocol is required and this needs to be context aware
- Plus support scenario where DNS stub resolvers are used in hubs with private IP addresses
- Best Current Practice guidelines are needed to address variations in DoH and TLS settings.
- More work needed on comparison of DoH vs Do53 performance and capacity overhead.
- DoH is not just about Browsers, ISPs need start considering applications, IoT & device aspects.