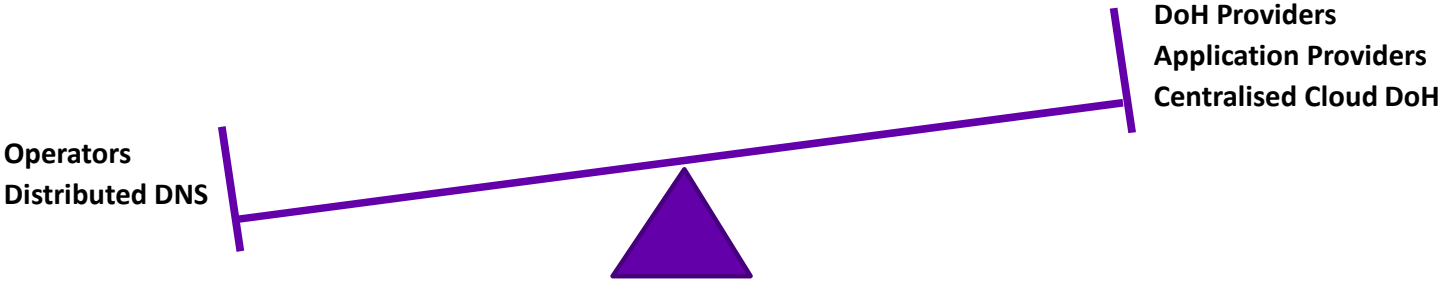
Potential ISP Challenges with DNS over HTTPS

Andy Fidler, Principal Network Architect
BT Technology
andrew.fidler@bt.com

UKNOF 43 – Manchester – Tuesday 9th April, 2019

DoH could be a game changer in Operator / Application Dynamics

- DNS over HTTPS (DoH) has the potential to be a game changer in Operator / Application Dynamics
  - Standards fast-tracked through IETF
  - Mozilla and Google have shared their early technical intentions
  - Now really a matter of when this will be launched
  - And how quickly / how much traffic will shift from plaintext DNS to DoH?

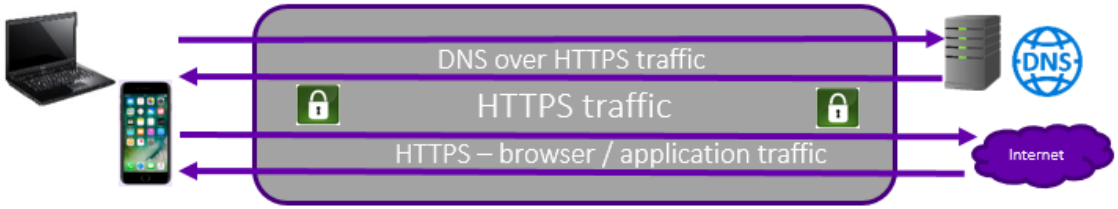


- Without cross-industry engagement, this step change has the potential to significantly impact Operators':
  - Customer Experience
  - On-line harm protection capabilities
  - Network cost base
  - Regulatory obligations
  - Cybersecurity capabilities

- Call to action on how UK Operators and wider UK Industry can respond to latest developments and smooth the adoption path through early mitigation of implementation issues.

What is DNS over HTTPS and why are ISPs concerned?

- **DoH – DNS requests sent via HTTPS, sharing port 443 and secured via TLS as defined in IETF RFC 8484 [1]**



- **DoH as an encryption based protocol has good privacy and security intentions**
  - **BT looks favourably upon anything that improves privacy and security for our customers**

- **Early adoption likely to be driven through centralised 3rd party DoH providers, bypassing wider ISP capabilities**
  - **Risking implementation, customer experience issues and other unintended consequences across the ecosystem**

ISP as DNS provider

3rd party DoH Provider

[1] https://datatracker.ietf.org/doc/rfc8484/

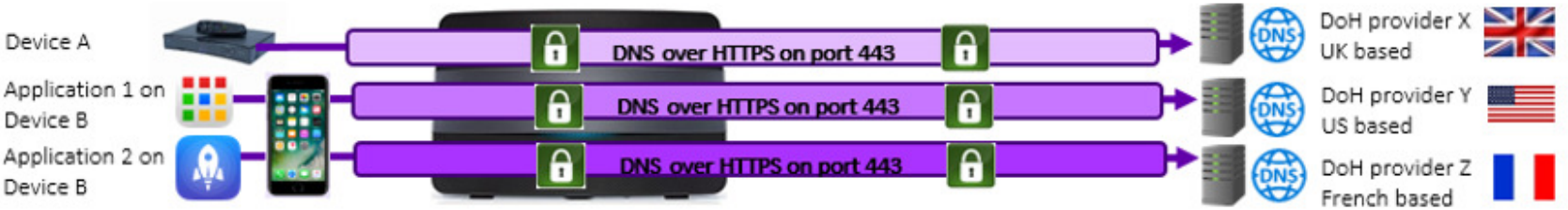
BT

How will DoH be realised on devices and applications?

- **Presently, the majority of devices use their ISP's DNS capabilities:**

ISP DNS resolvers have sight of browsing / application requests at a household level

- **DoH could drive a shift from ISP/ single device DNS settings to each application being able to select their own DoH provider:**



Moves to non-ISP DoH resolvers having sight of requests on a customer / application basis

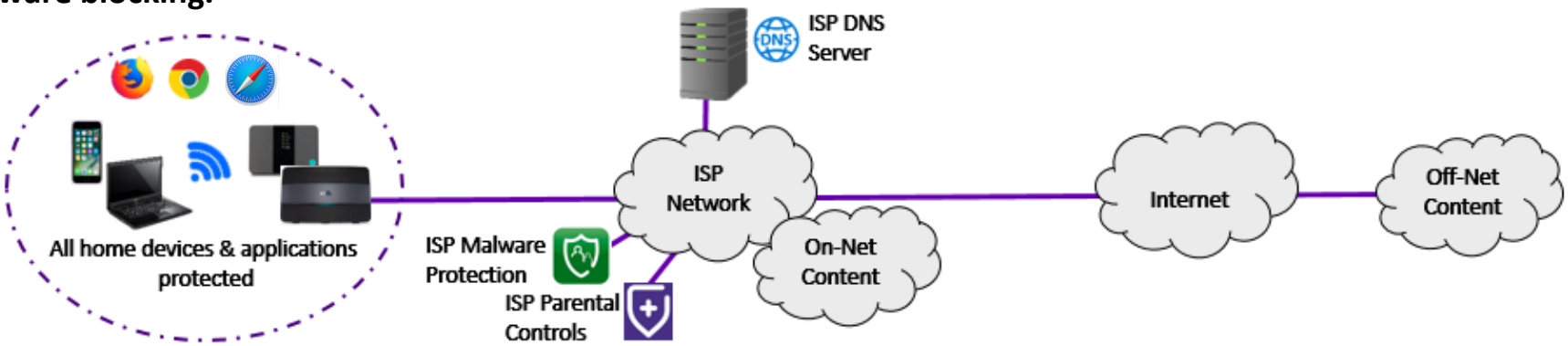
- **DoH service discovery standardisation is still ongoing within the IETF DoH WG**
  - https://datatracker.ietf.org/doc/draft-ietf-doh-resolver-associated-doh/

- **However there are many open questions on customer experience, privacy, trust and vulnerability exploitation risks**
  - **E.g. how will individual app DoH choices impact other applications and device OS settings?**

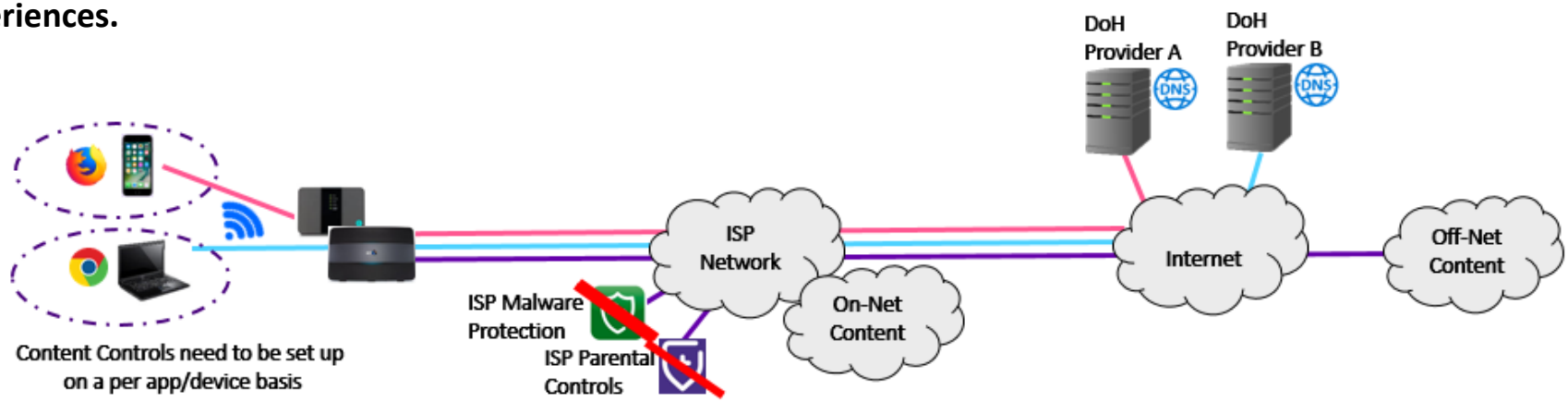
BT

Impact to Online Harm Protection

- **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 parental controls and malware blocking.**



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

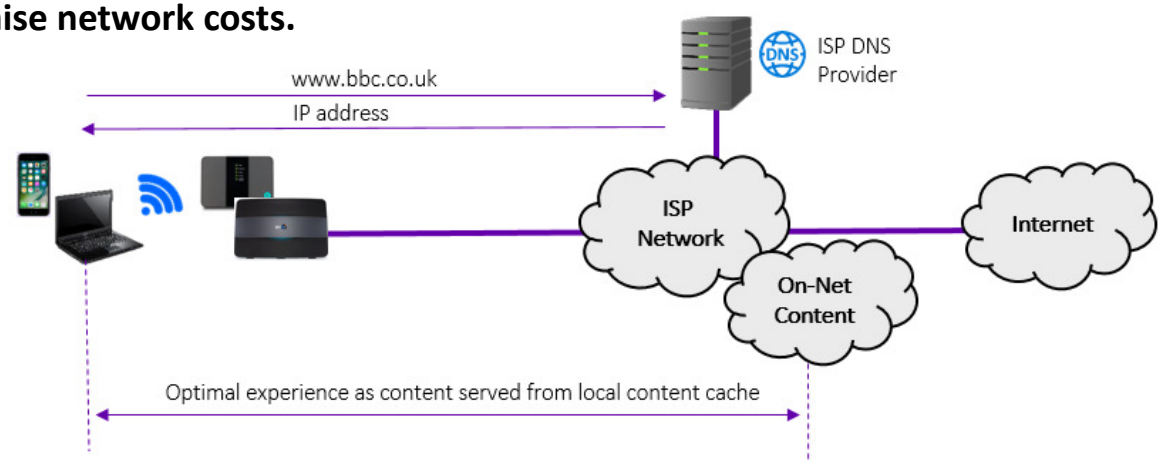


- **Will customers realise if they change to 3rd party DoH providers, it will bypass their existing ISP content filtering?**

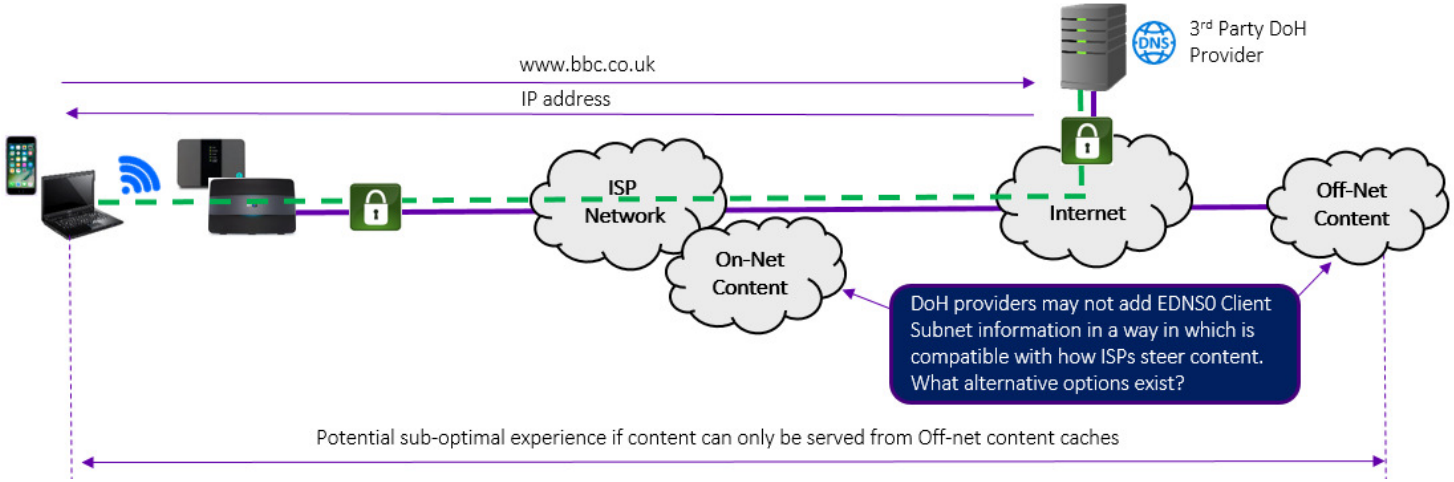
BT

Impact on 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 will be impacted if DoH providers block DNS information used by ISPs.**



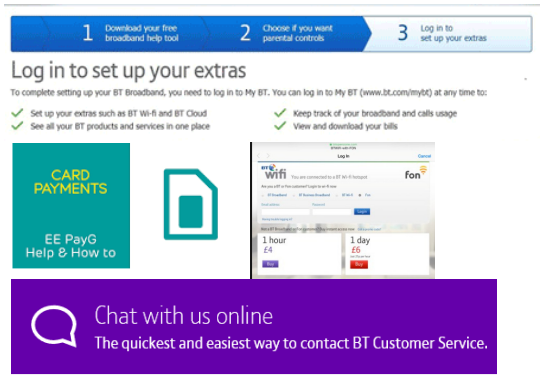
- **Do we risk some users getting less well localised results and a sub optimal experience even if actual DNS resolution is improved?**

BT

Impact to Customer Service & Industry Benchmarks

Customer Service:

- **ISPs may use DNS redirects for service support, e.g.:**
  - **Device / hub set-up**
  - **Mobile Pay As You Go top-up**
  - **Broadband Account Support**
- **Plus for Captive Portals for Wi-fi hot-spots**
- **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?**
- **How will ISPs and 3rd party DoH providers work together to resolve customer issues?**



Industry Performance Benchmarks:

- **Ofcom Additional BB Research Performance Metrics**

https://www.ofcom.org.uk/__data/assets/pdf_file/0027/113796/home-broadband-2017.pdf

Variable	Definition and importance
Web browsing speed	The time taken to fetch the main HTML and assets (text, basic code and content files) form a webpage *Dependent on download speeds, latency and DNS resolution times*
Latency	The time it takes a packet of data to travel to a third-party server and back *A connection with low latency will feel more responsive for simple tasks like web browsing and certain applications perform far better with lower latency*
Packet loss	The proportion of data packets that are lost in transmission over a connection *Important to online gamers and those streaming content or using VoIP as extended periods of loss lead to choppy and broken-up video and audio*
DNS resolution	The time taken for an ISP to translate website names into IP addresses When DNS servers operate slowly, web browsing and other activities suffer
DNS failure	The proportion of requests for which the DNS server cannot translate a domain name to an IP address *DNS failure results in error messages such as "Host could not be found"*
Jitter	Measures the rate of change of latency *The lower the measure of jitter the more stable a connection is and latency is important to gamers and VoIP users*

- **Potentially impacted by use of 3rd Party DoH**
- **How will we quantify the impacts?**
- **Do we need a UK measurement study?**

BT

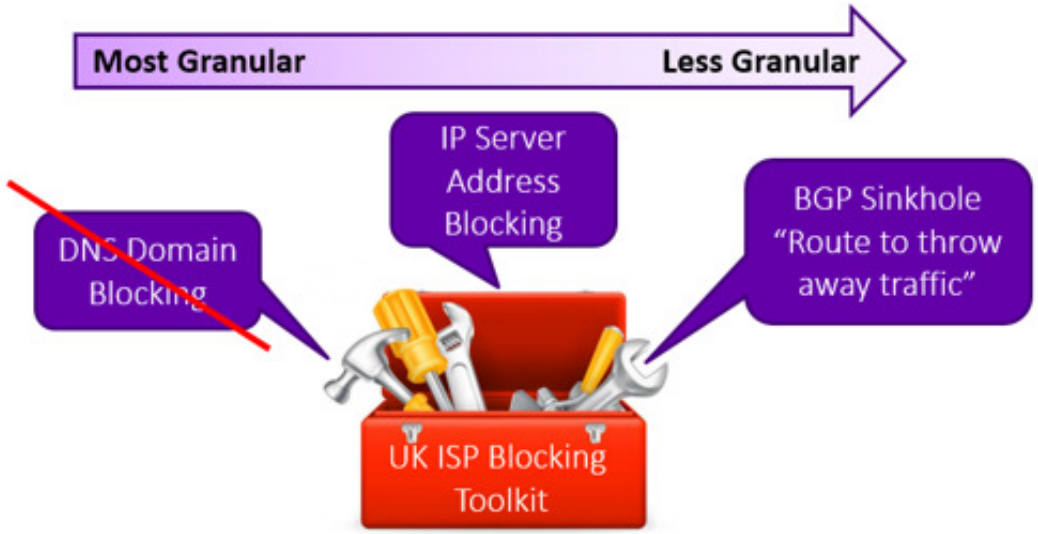
Impact to Government/Regulatory Blocking & Cyber Security

Government / Regulator Blocking:

- **DNS blocking is the most granular tool in the kit box used by UK ISPs to implement Government / Regulation blocking orders**
- **If UK ISPs are no longer in the DNS path, they may not be able to fulfil certain domain specific court order blocking requests**
- **Instead the Government may need to approach a collection of 3rd party DoH providers, who may be based outside UK jurisdiction**

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?**



BT

What's the latest on standard development from IETF 104 Prague

- Two Internet-Drafts (I-Ds) highlighting Operator implementation aspects submitted to IETF DoH Working Group:
  - https://www.ietf.org/id/draft-reid-doh-operator-00.txt
  - https://www.ietf.org/id/draft-livingood-doh-implementation-risks-issues-03.txt
- I-Ds were not formally accepted due to alignment questions with the current DoH WG charter
- However they received considerable discussion within the DoH WG session[1] and at a side meeting[2]
- IETF Area Directors are now considering the following next step options:
  1. After completion of DoH Discovery I-D, re-charter DoH WG to explore these wider operational I-Ds.
  2. Re-direct I-Ds to DNS Operations Working Group
  3. Create a new Working Group within the IETF to explore these wider operational / policy / governance aspects
- Encourage ISPs and Operators to actively engage with ongoing discussions through the DoH mailing list[3]
- However these I-Ds did prompt discussions that led to Google and Mozilla publishing their DoH plans.

[1] https://www.youtube.com/watch?v=RdYs0-sHXqM [2] https://mailarchive.ietf.org/arch/msg/doh/41ghhhhJNfXVbZ8ZCE9Pd9qs6Bs [3] https://mailarchive.ietf.org/arch/browse/doh/

Mozilla and Google IETF DoH Intentions

Mozilla:

https://mailarchive.ietf.org/arch/msg/doh/po6GCAJ52BAKuyL-dZiU91v6hLw

"we may have DoH/TRR on by default in some regions and not others….The user will be informed that we have enabled use of a TRR and have the opportunity to turn it off at that time"

Google:

https://mailarchive.ietf.org/arch/msg/doh/JhFPKoyGU2JqKmUk3GEe5yjuSHI

"Provide our users with meaningful choice and control, e.g. allow end users/admins to control and configure the feature, whether they want to use a custom DoH server or just keep on using their regular DNS….There are no plans to force any specific resolver without user consent / opt-in."

Great insight on deployment plans, but many questions still exist:

- **Who will define and govern the DoH TRR discovery framework?**
- **What form will DoH / TRR enablement notifications take?**
- **How will informed / meaningful consent be captured for DoH?**
- **How will DoH be explained to users not knowing what DNS is?**
- **How will impact on ISP services be explained, e.g. Parental Controls?**
- **Will custom entries be verified in terms of trust and authenticity?**

BT

Opportunities for ISPs to reduce DoH implementation risks

1. **Explore roadmap opportunities to uplift existing DNS servers to DNSSEC, DoT and DoH**
   - **Need to consider server capacity / performance impacts, additional load balancing, caching, DNS64/IPv6 and certificate management support requirements**

2. **Engage in ISP operational / implementation issue discussions within IETF**

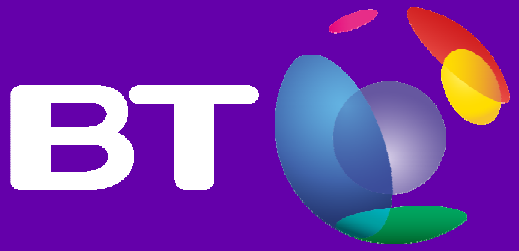
3. **Engage in UK ISP Alliance discussions with Government / Regulatory Policymakers**

4. **From an early engagement perspective ISPs should also be aware of the following IETF activities**
   - **DNS over QUIC - https://datatracker.ietf.org/doc/draft-huitema-quic-dnsoquic/**
   - **TLS 1.3 - https://tools.ietf.org/html/rfc8446**
   - **Encrypted Server Name Indication (ESNI) - https://www.ietf.org/id/draft-ietf-tls-esni-03.txt**

Closing Summary

- **DoH as an encryption based protocol has good privacy and security intentions**
- **However it may create ISP implementation issues and unintended consequences across the ecosystem**
- **Customer experience, network costs, regulatory obligations and cybersecurity may be adversely impacted**
- **Which fora in the UK are most appropriate for these discussions?**
- **We welcome Operator and Industry collaboration to work on these issues and develop solutions**

BT


BT