A UK ISP view on DNS over HTTPS

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

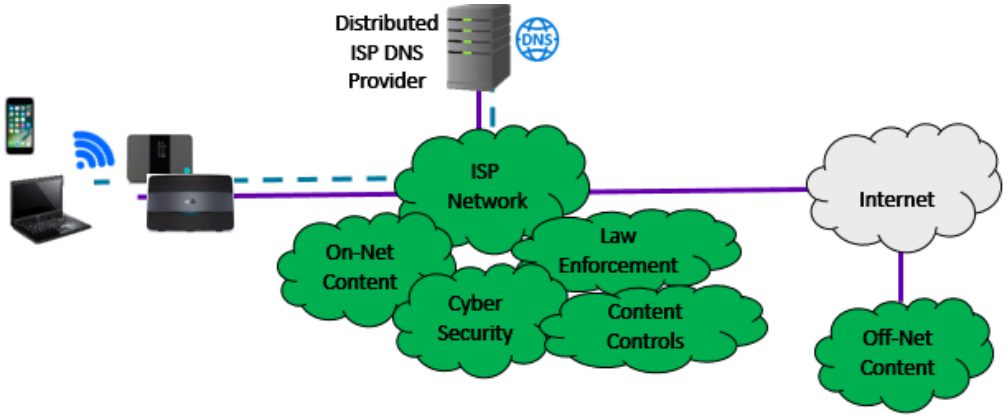
ICANN DNS Symposium 2019, Bangkok – Friday 10th – Saturday 11th May, 2019

DoH - good from a protocol perspective, so why are ISPs concerned?

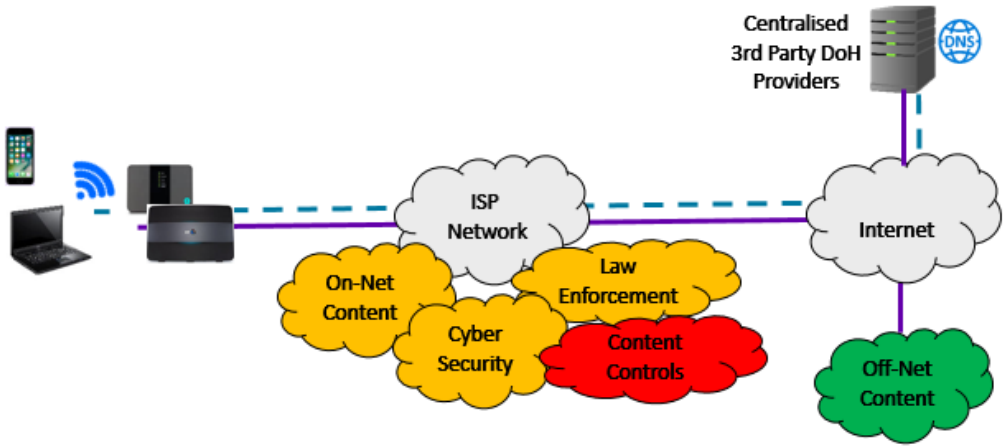
- **DoH from a protocol perspective has good privacy and security intentions**
  - **BT looks favourably upon anything that improves privacy and security for our customers**

- **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**

- **These implementation issues must be addressed through industry collaboration**



ISP as DNS provider



3rd party DoH Provider

Key implementation impact areas requiring industry cooperation

- **Key DoH implementation impact areas that ISPs would welcome industry and standards focus on are:**

Customer privacy and trust

Effect on existing Broadband Parental Control and Malware protection

Customer experience & Content Caching

Court Order / Regulatory Blocking Requirements

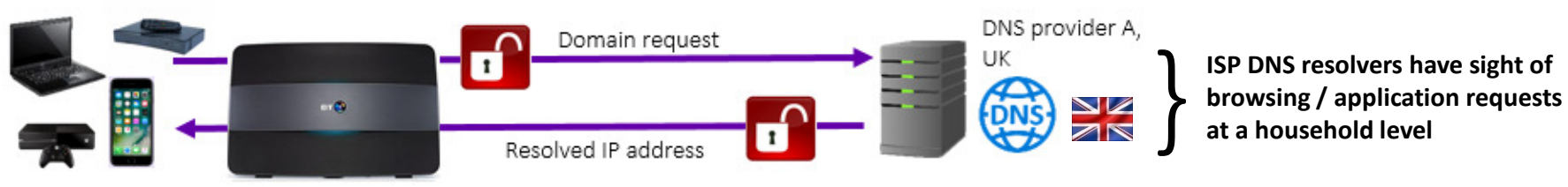
Cyber security capabilities

Key management

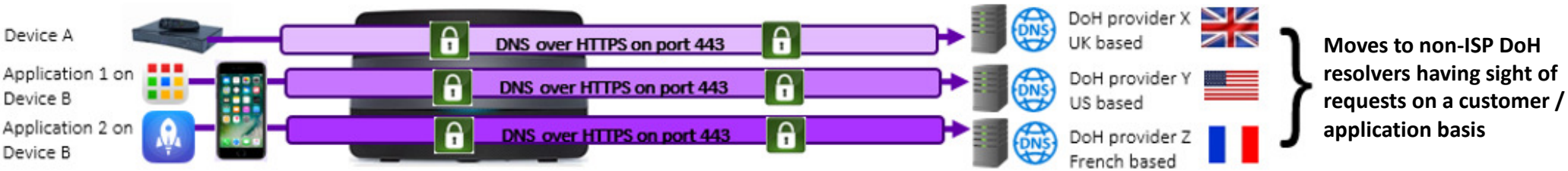
Enterprise, Corporate and Public sector risks

Customer Privacy & Trust

- **Presently, the majority of devices use their ISP's DNS, so ISPs have a "household view" from a privacy perspective**



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



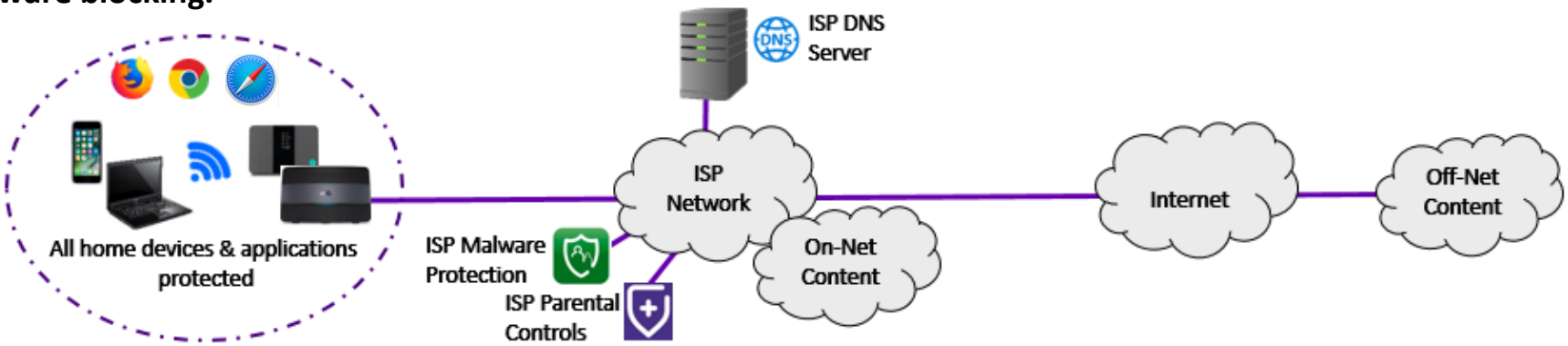
- **Could this result in DoH providers having a more "individual user/personalised view" from a privacy perspective?**

- **Appreciate DoH providers may have strict privacy policies to address this, e.g. not retaining data greater than 24 hours and only using it for the purpose of providing a DNS service.**

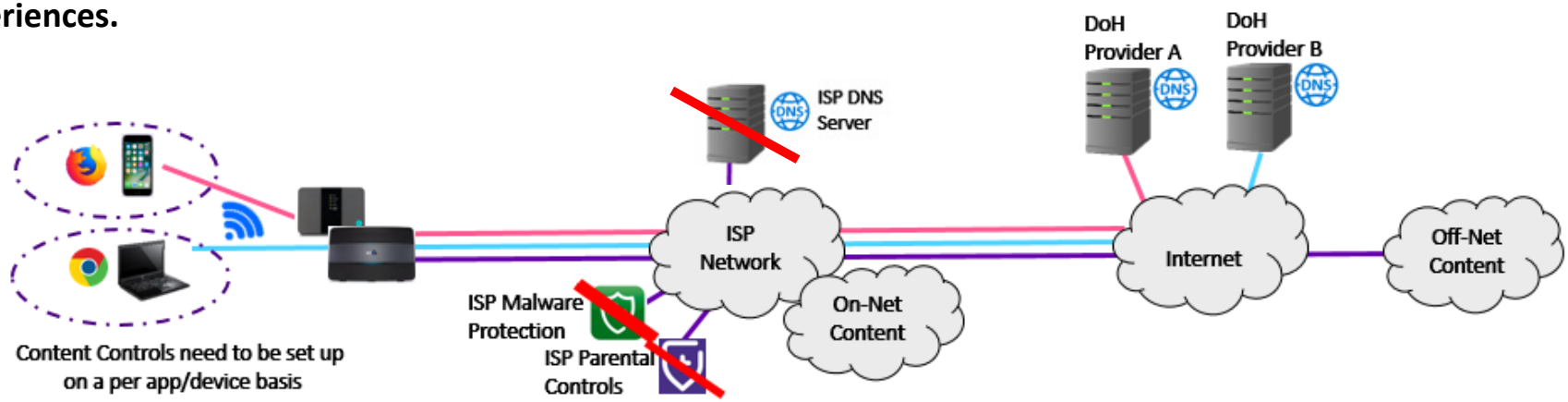
- **On a wider device note, how will individual app DoH choices impact other applications and device OS settings?**

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.**



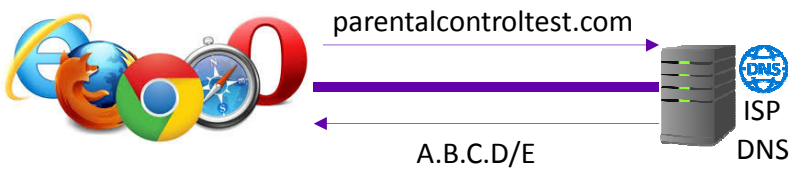
- **With DoH, customers may need to set-up content filtering on a per device / application basis, risking inconsistent experiences.**



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

Online Harm Protection – DoH mitigation options

- **Opportunities exist for Browsers/Applications and ISPs to work together to realise a better DoH customer experience.**
- **By identifying if customers have existing ISP parental control / malware services and providing advice based on this.**
- **For example, could Browsers run a test against a known FQDN with a known A/AAAA record response?**
- **Where by response A.B.C.D means ISP parental controls and malware protection are active?**
  - **Naturally this may need an RFC to specify FQDN and results, plus a privacy review e.g. GDPR compliance.**



1. Before defaulting to DoH or presenting DoH options, browser runs check to see If customer has any existing ISP parental controls enabled.

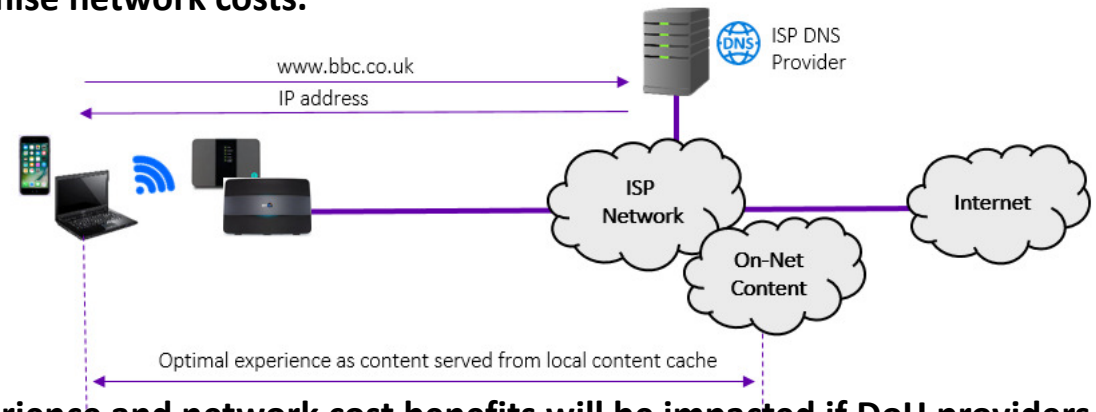
2. ISP DNS returns
A.B.C.D if Parental Controls active
A.B.C.E if not active

3. If customer has ISP parental controls active, browser advises customer that if they proceed with selecting a 3rd party DoH provider their existing parental control service will be bypassed and they will need to set-up new 3rd party protection.

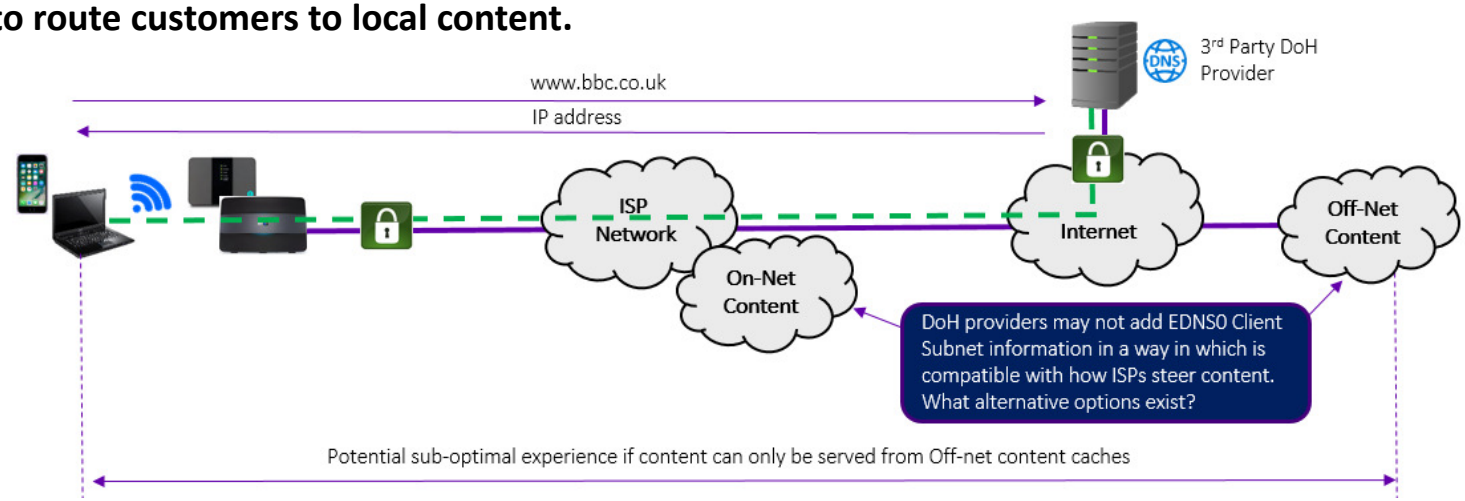
- **Are there alternative options e.g. a TXT record response, DHCP like discovery?**

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 to route customers to local content.**



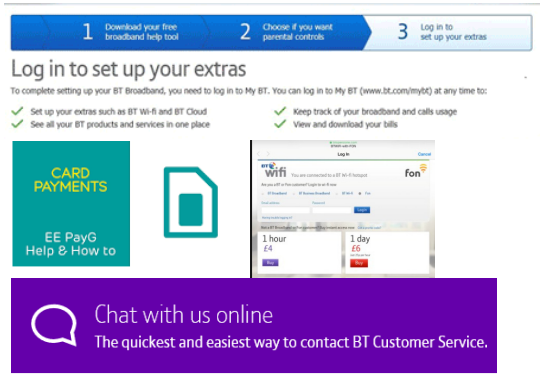
- **Do we risk some users getting less localised results and a suboptimal experience even if DNS resolution is improved?**

- **How can ISPs, CDN vendors and DoH providers work together on solutions to allow ISPs to continue to serve locally cached content to customers using 3rd party DoH Trusted Recursive resolvers? Plus explore measurement data?**

Customer Service

Customer Service:

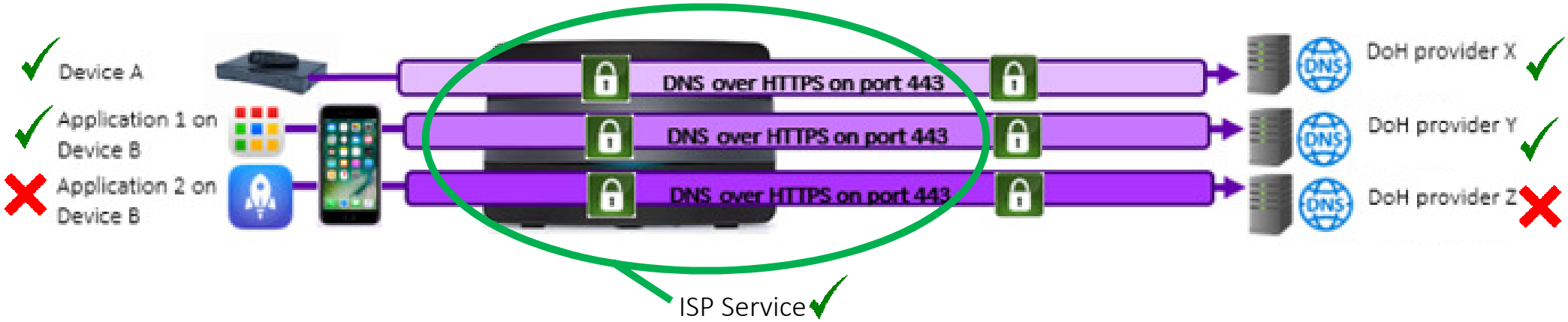
- **ISPs may use DNS redirects for service support, e.g.:**
  - **Device / hub set-up**
  - **Mobile Pay As You Go top-up**
  - **Broadband Account Support**



- **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 would you troubleshoot a customer calling in with only one application failing and ISP service working fine?**

- **How will ISPs and 3rd party DoH providers work together to resolve customer issues?**

Industry Benchmarks

- **UK 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?**
- **What's the best fora for measurement studies?**

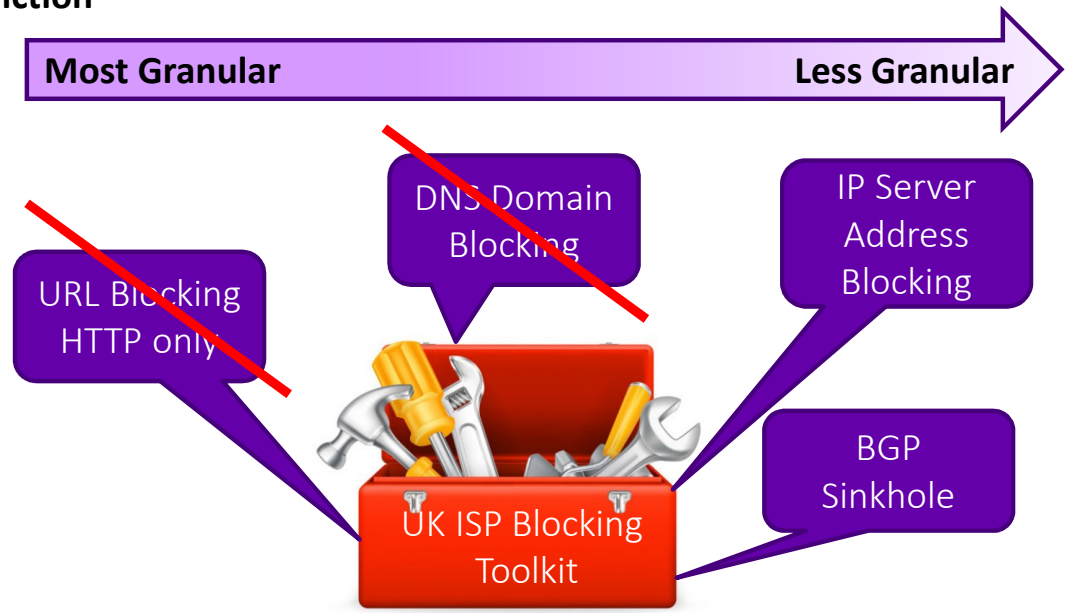
Court Order/Regulatory Blocking & Cyber Security

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**

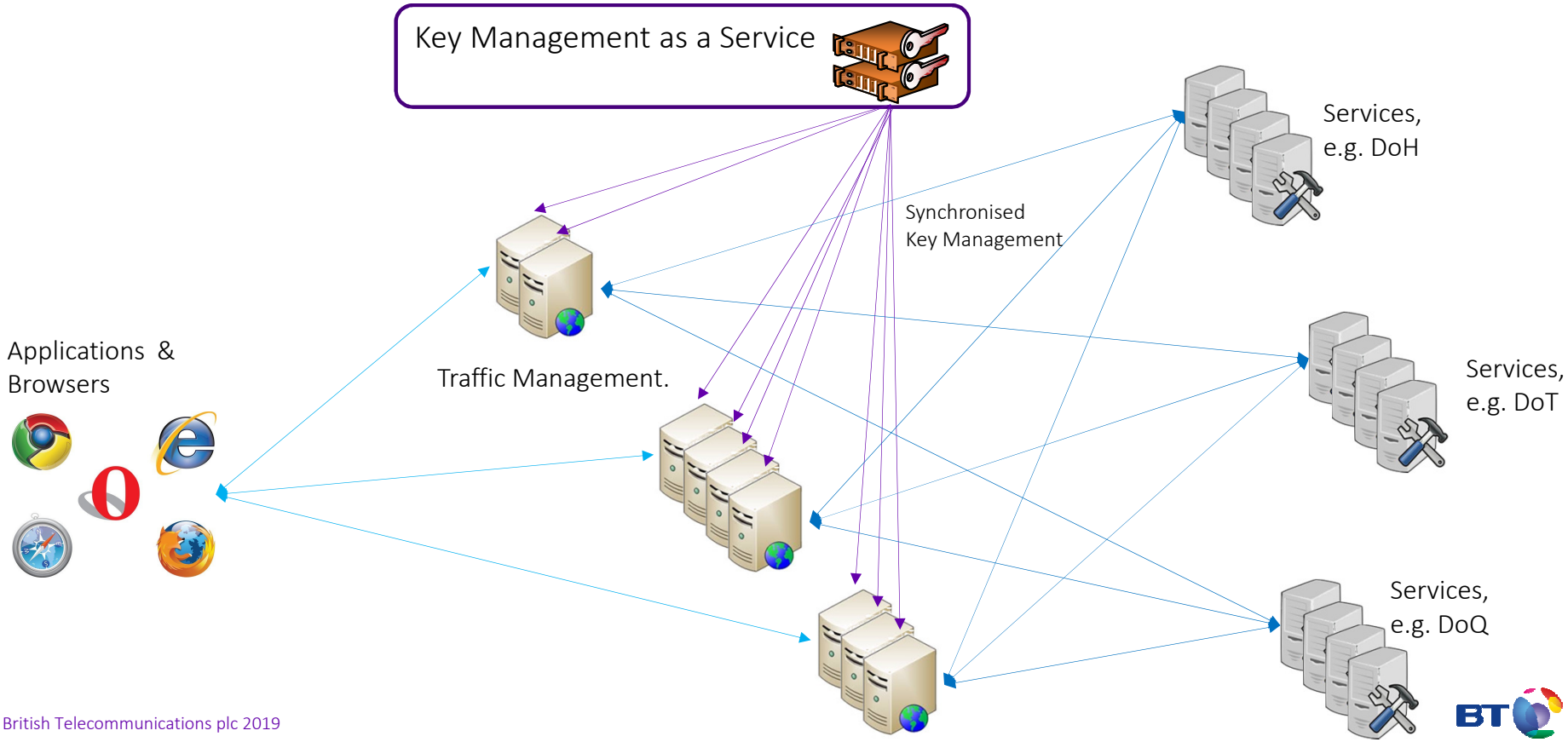
Cyber Security:

- **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?**



Key Management Services

- **Designs need to ensure that DoH servers can scale to support the likely increase in session encryption volumes.**
- **Historically industry has used Session IDs and Session Tickets to support these pseudo TLS sessions.**
- **We believe Session ID may not scale for DoH as session volume increases and server side storage is not bounded in size.**
- **As a result we believe Session Tickets with central Key Management may become a requirement.**



Enterprise, Corporate & Public Sectors

- **Impact is not just limited to Consumer customers, DoH will also impact Corporate, Enterprise and Public Sectors:**
  - **Corporate / Enterprise DNS based content filtering and malware protection will also risk DoH bypass**
  - **Split DNS and solutions for Internal Enterprise DNS names may fail**
  - **Internal Corporate names may leak outside of intranets**
  - **Negative impact on Bring Your Own Devices which will need to work across both home and work environments**

DoH Industry Implementation Examples

Industry statements within IETF:

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….We are considering a first milestone where Chrome would do an automatic upgrade to DoH when a user's existing resolver is capable of it"

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"

Mozilla:

Mozilla have issued a DoH Partner Policy List:
https://wiki.mozilla.org/Security/DOH-resolver-policy

BT thoughts:

Contrasting views here:

- Mozilla - a default on approach in some regions
- Google - initially only enabling DoH if existing provider supports it.

Great insight on deployment plans, but questions still exist:

- Who will define and govern the DoH TRR discovery framework?
- For Mozilla, what form will DoH 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?
- Mozilla DoH Partner Policy List:
  - 24 hour retention and data usage constraints may restrict ISP customer support and cybersecurity aspects.
  - Non propagation of client subnet DNS extension may impact ISP on-net content caching capabilities
  - No modifying of domain response may impact parental control, malware blocking notification and service support redirects.

Thoughts on DoH Next Steps within IETF

- **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 then IETF DoH WG session[1] and at a side meeting[2]**
- **Since Prague these discussions have shifted to a new Applications Doing DoH (ADD) IETF mailing list[3]**
- **How can industry increase the momentum of these discussions and be ready for discussions at IETF 105 in July:**
  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. **Turn the ADD mailing list into a new Working Group?**
  4. **If IETF is not the place for these operator implementation aspects, which fora are?**
- **Encourage active engagement with ongoing discussions through the ADD/DoH mailing lists[3,4]**

[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/add/

[4] https://mailarchive.ietf.org/arch/browse/doh/

Closing Summary

- **DoH as a 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**
- **We welcome ISP and Industry collaboration to develop solutions for these issues**

BT