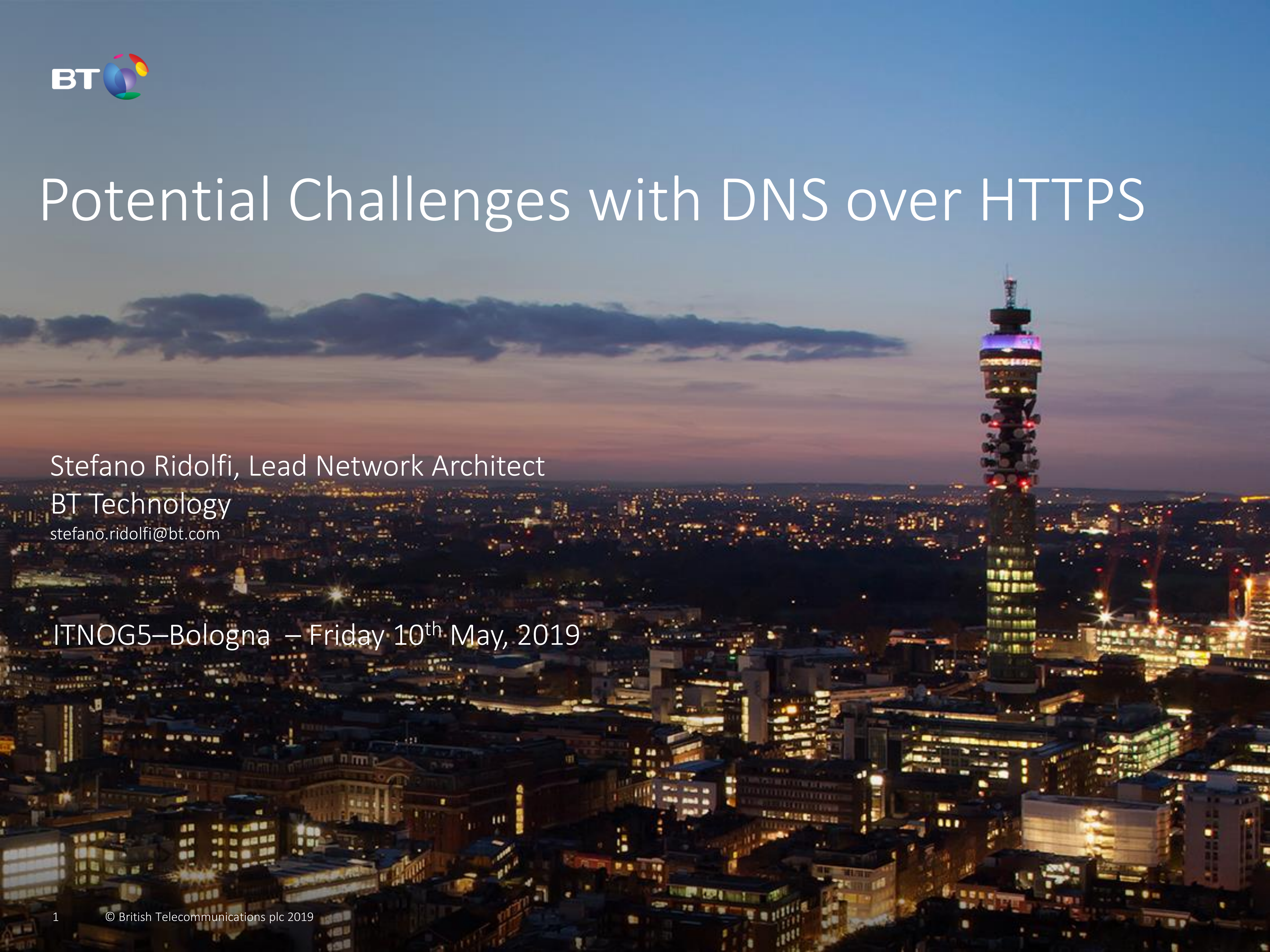


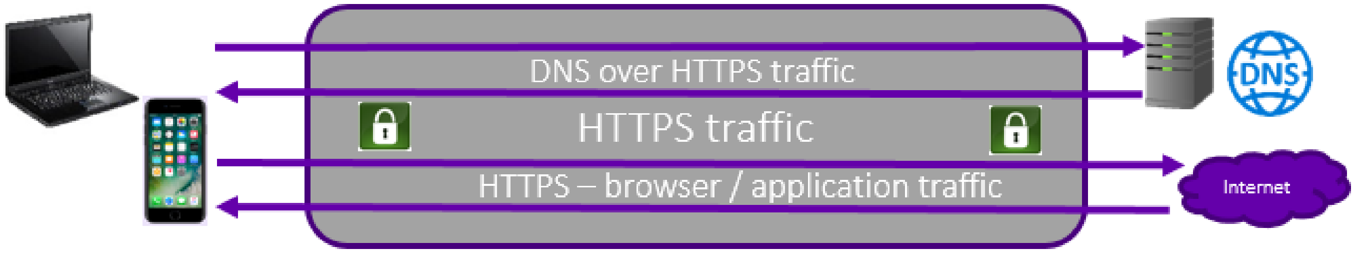
# Potential Challenges with DNS over HTTPS

Stefano Ridolfi, Lead Network Architect
BT Technology
stefano.ridolfi@bt.com

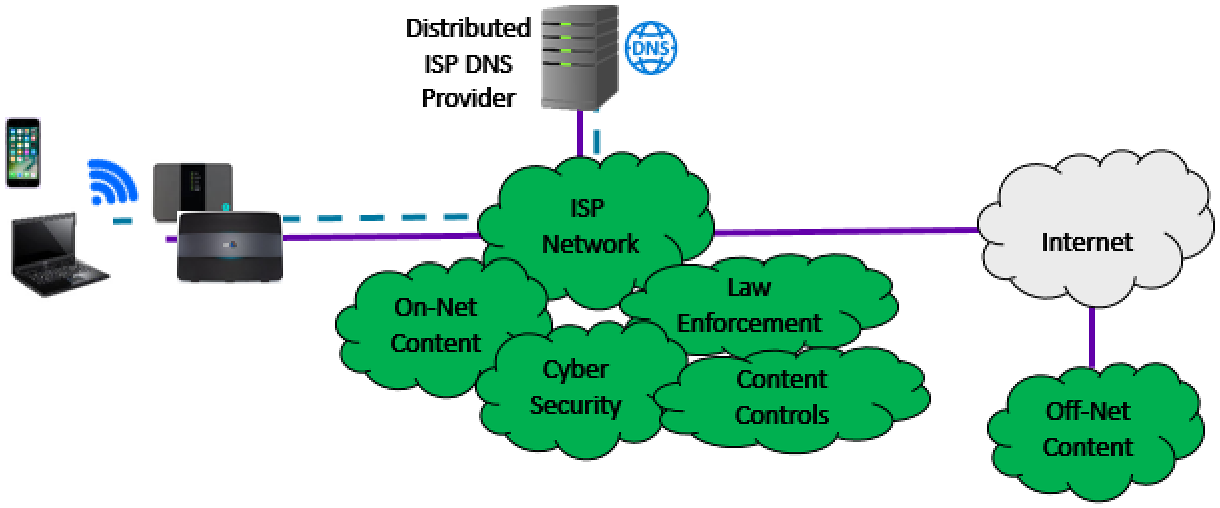
ITNOG5–Bologna – Friday 10th May, 2019

# What is DNS over HTTPS and why are ISPs concerned?

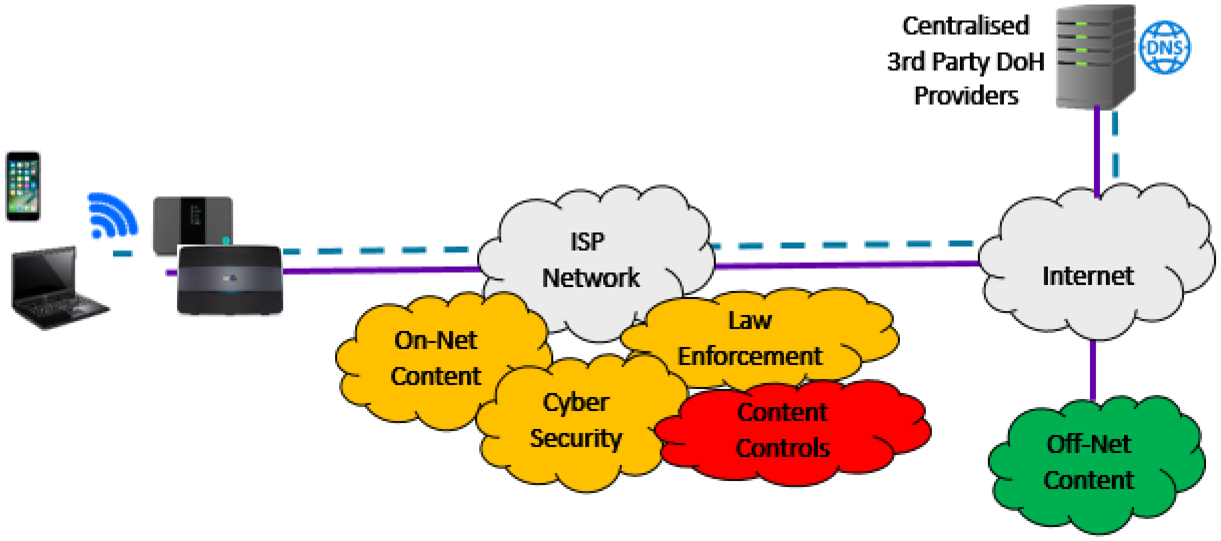
- **DoH – DNS requests sent via HTTPS, sharing port 443 and secured via TLS as defined in IETF RFC 8484 [1]**



- **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**

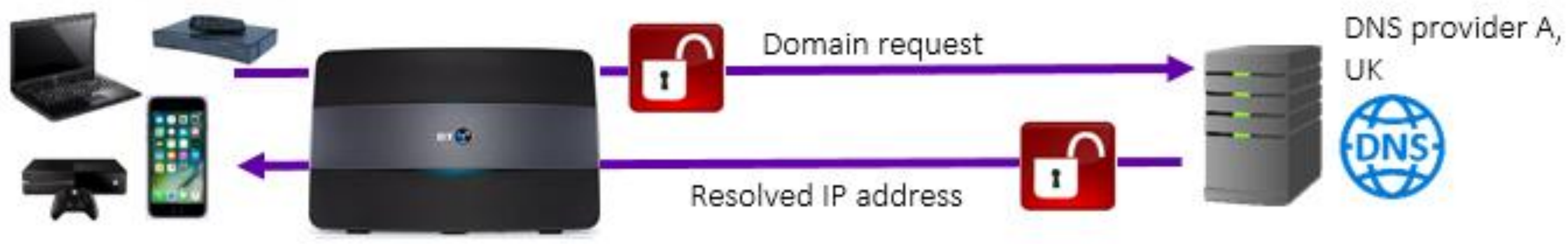


**3rd party DoH Provider**

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

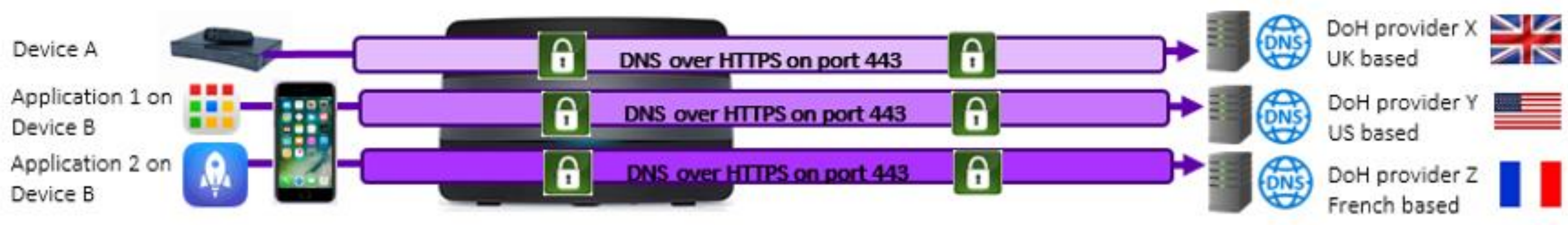
# How will DoH be realised on devices and applications?

- **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:**


Device A
Application 1 on Device B
Application 2 on Device B
DNS over HTTPS on port 443
DNS over HTTPS on port 443
DNS over HTTPS on port 443
DNS
DoH provider X UK based
DNS
DoH provider Y US based
DNS
DoH provider Z French based

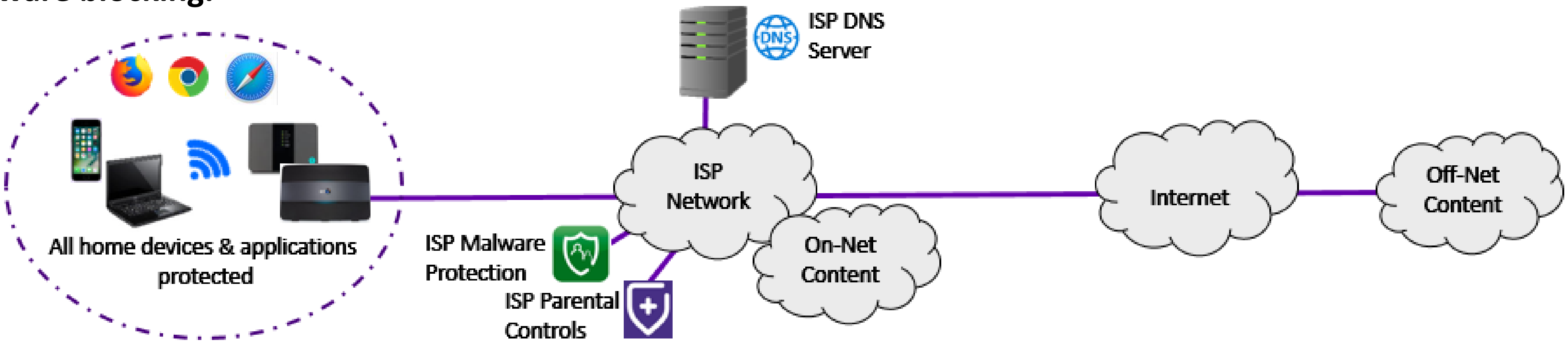
**Moves to non-ISP DoH resolvers having sight of requests on a customer / application basis**

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

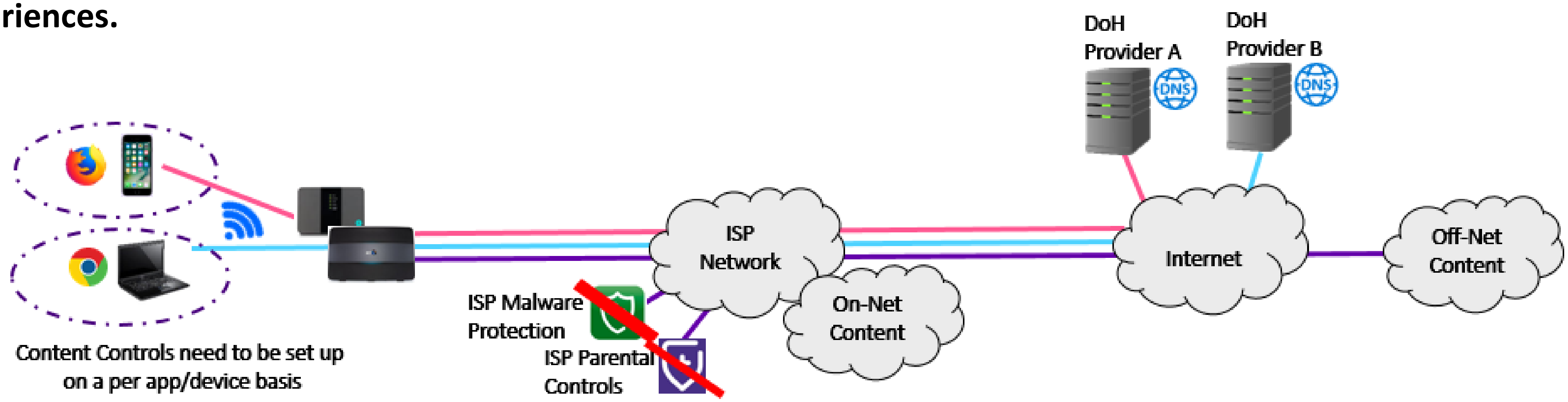
- **However there are many open questions on customer experience, privacy, trust and vulnerability exploitation risks**
  - **E.g. how will individual app DoH choices impact other applications and device OS settings?**

# Impact to Online Harm Protection

- Presently most  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.



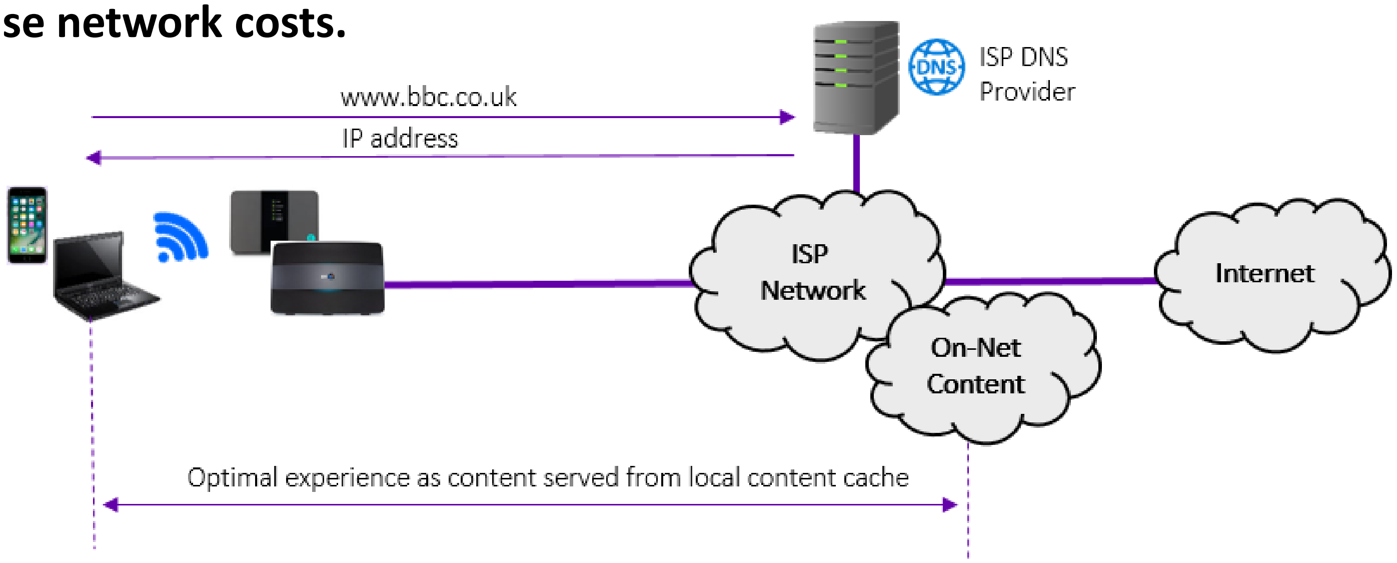
- With DoH, customers may need to set-up content filtering on a per device / application basis, risking inconsistent experiences.



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

# 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.**



ISP DNS Provider

www.bbc.co.uk

IP address

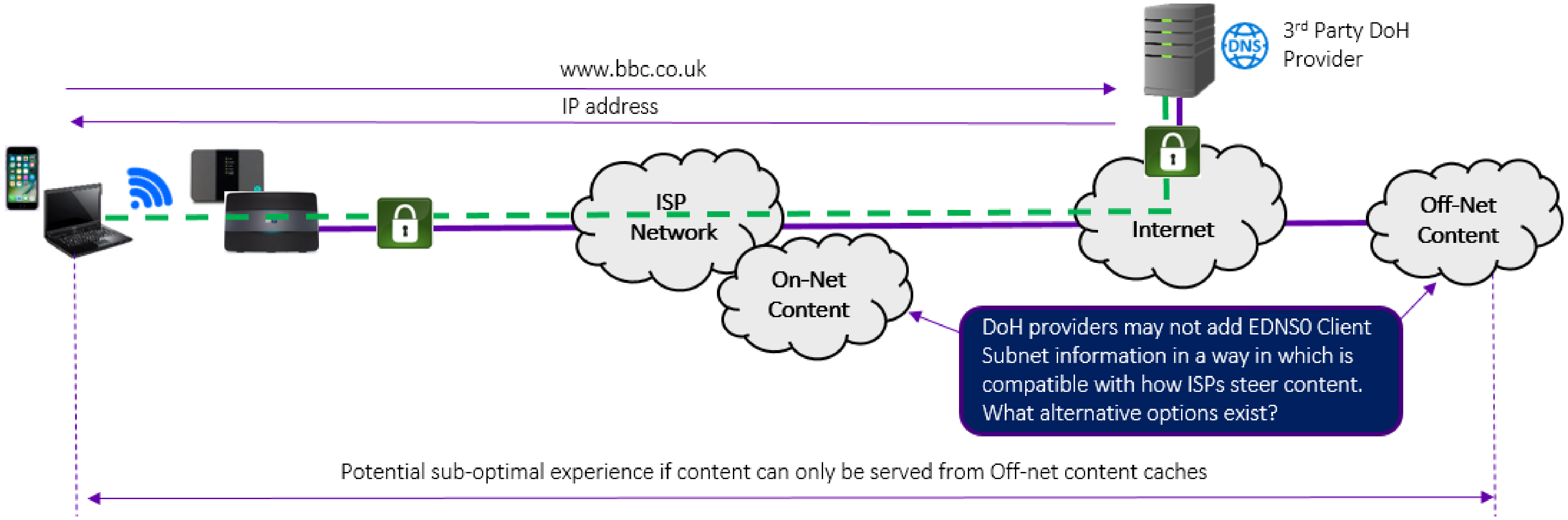
ISP Network

On-Net Content

Internet

Optimal experience as content served from local content cache

- **These Customer Experience and network cost benefits will be impacted if DoH providers block DNS information used by ISPs.**



3rd Party DoH Provider

www.bbc.co.uk

IP address

ISP Network

On-Net Content

Internet

Off-Net Content

DoH providers may not add EDNS0 Client Subnet information in a way in which is compatible with how ISPs steer content. What alternative options exist?

Potential sub-optimal experience if content can only be served from Off-net content caches

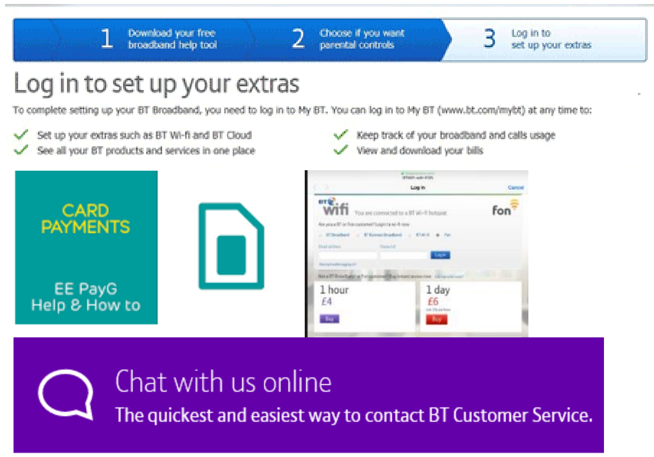
- **Do we risk some users getting less well localised results and a sub optimal experience even if actual DNS resolution is improved?**

# 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**



1 Download your free broadband help tool
2 Choose if you want parental controls
3 Log in to set up your extras

Log in to set up your extras

To complete setting up your BT Broadband, you need to log in to My BT. You can log in to My BT (www.bt.com/mybt) at any time to:

- ✓ Set up your extras such as BT Wi-fi and BT Cloud
- ✓ See all your BT products and services in one place
- ✓ Keep track of your broadband and calls usage
- ✓ View and download your bills

CARD PAYMENTS

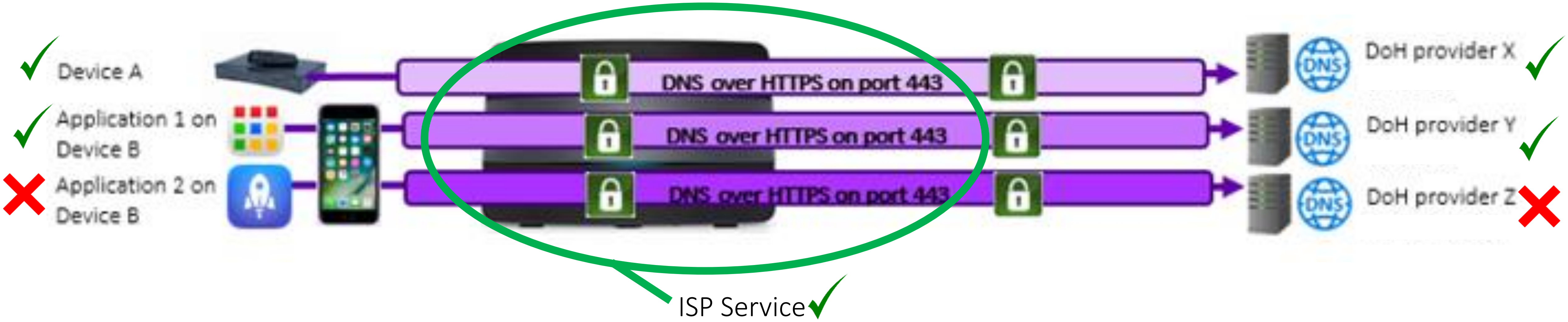
EE PayG Help & How to

Chat with us online

The quickest and easiest way to contact BT Customer Service.

- **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?**



✓ Device A
✓ Application 1 on Device B
✗ Application 2 on Device B
DNS over HTTPS on port 443
DNS over HTTPS on port 443
DNS over HTTPS on port 443
DNS
DoH provider X ✓
DoH provider Y ✓
DoH provider Z ✗
ISP Service ✓

- **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?**

# Impact to Government/Regulatory Blocking & Cyber Security

**Government / Regulator Blocking:**

- **DNS blocking is the most granular tool in the kit box used by ISPs to implement Government / Regulation blocking orders**
- **If 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 country 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?**

# Impact to Privacy: From IETF RFC 8484 [1]

- DNS over TLS [RFC7858] provides similar protections, while direct UDP- and TCP-based transports are vulnerable to this class of attack
- DNSSEC and DoH are independent and fully compatible protocols, each solving different problems
- For HTTP server push extra care must be taken to ensure that the pushed URI is one that the client would have directed the same query to if the client had initiated the request (in addition to the other security checks normally needed for server push)
- HTTPS presents new considerations for correlation, such as explicit HTTP cookies and implicit fingerprinting of the unique set and ordering of HTTP request header fields
- HTTP's feature set can also be used for identification and tracking in a number of different ways
- Mixing DoH requests with other HTTP requests on the same connection also provides an opportunity for richer data correlation

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

# 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?**

# Opportunities for ISPs to reduce DoH implementation risks

- 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]

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 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**

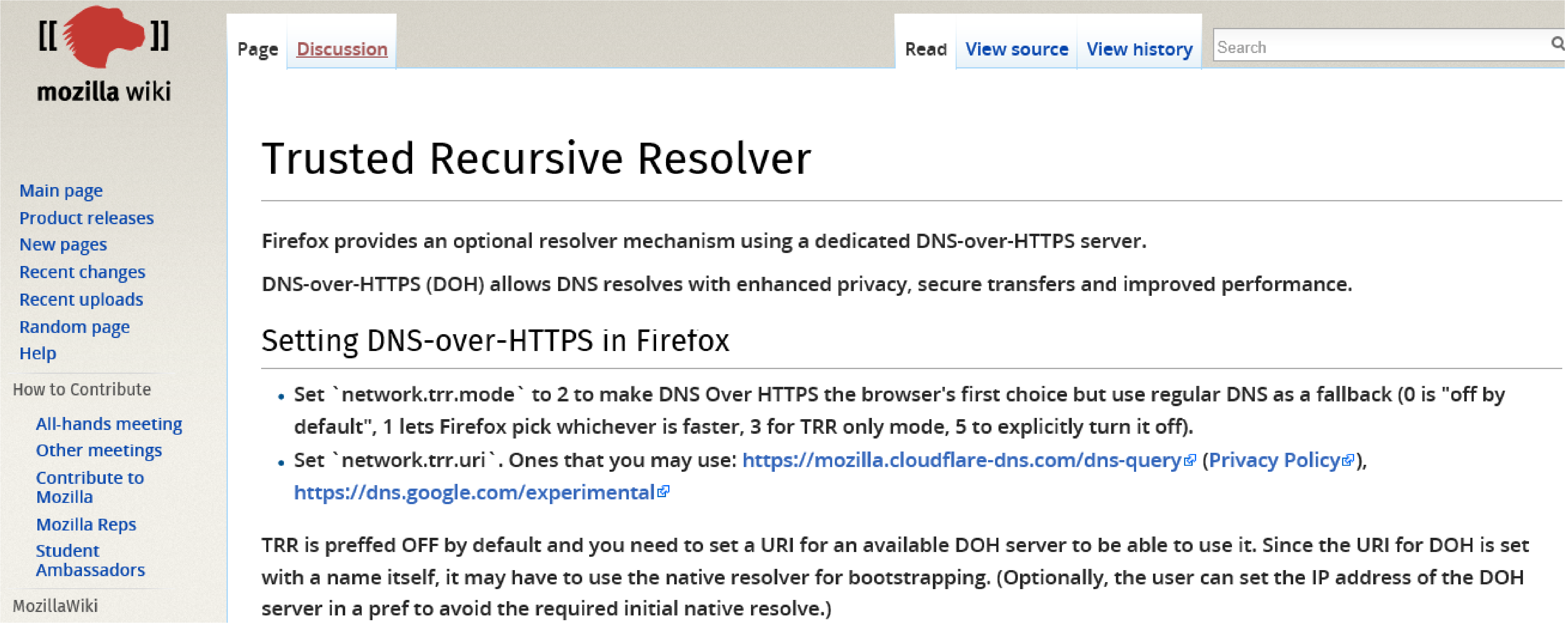
# Recent articles on DoH

- https://www.internetpost.it/dns-over-https-doh/
- https://siamogeek.com/2019/04/dns-over-https/
- https://www.thetimes.co.uk/article/warning-over-google-chrome-browsers-new-threat-to-children-vm09w9jpr
- https://www.forbes.com/sites/zakdoffman/2019/04/22/crisis-as-changes-to-google-chrome-threaten-child-safety-and-cybersecurity/#6261ff8c5704
- https://www.dailymail.co.uk/news/article-6946695/New-version-Google-Chrome-make-harder-stop-computer-users-watching-porn-online.html

https://www.ispreview.co.uk/index.php/2019/04/google-uk-isps-and-gov-battle-over-encrypted-dns-and-censorship.html

**The UK Government, broadband ISPs and the National Cyber Security Centre (NCSC) are set to meet on the 8th May 2019 in order to discuss Google's forthcoming implementation of encrypted DNS (DoH – DNS over HTTPS), which politicians fear could break their internet censorship plans.**

# DoH configuration



## Trusted Recursive Resolver

Firefox provides an optional resolver mechanism using a dedicated DNS-over-HTTPS server.

DNS-over-HTTPS (DOH) allows DNS resolves with enhanced privacy, secure transfers and improved performance.

### Setting DNS-over-HTTPS in Firefox

- Set `network.trr.mode` to 2 to make DNS Over HTTPS the browser's first choice but use regular DNS as a fallback (0 is "off by default", 1 lets Firefox pick whichever is faster, 3 for TRR only mode, 5 to explicitly turn it off).
- Set `network.trr.uri`. Ones that you may use: https://mozilla.cloudflare-dns.com/dns-query (Privacy Policy), https://dns.google.com/experimental

TRR is preffed OFF by default and you need to set a URI for an available DOH server to be able to use it. Since the URI for DOH is set with a name itself, it may have to use the native resolver for bootstrapping. (Optionally, the user can set the IP address of the DOH server in a pref to avoid the required initial native resolve.)

# 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 forum  are most appropriate for these discussions?

- We welcome Operator and Industry collaboration to work on these issues and develop solutions

BT