

# DoH Preference Hints

draft-schinazi-httpbis-doh-preference-hints

IETF 105 – Montreal – 2019-07

David Schinazi – dschinazi@google.com

Nick Sullivan – nick@cloudflare.com

Jesse Kipp – jkipp@cloudflare.com

# Using the Right DoH Server

Sending all DNS queries to one DoH provider can be inefficient

Exposes browsing history to that provider

# Proposed Solution

Inspired by HSTS

Let HTTP server tell user agent which DoH server it prefers

Completely optional: user agent free to decide

```
DoH-Preference: "https://dnsserver.example.net/dns-query{?dns}";  
max-age=15768000
```

# Intended Deployment

Browsers ship with list of vetted DoH Servers

Follow DoH-Preference if proposed server is in vetted list

Content providers can provide vetted DoH server

# Fallback

This is a performance feature, not a security feature

Unlike HSTS, fallback is allowed

Fallback to other DoH server or any other DNS mechanism

# There be Dragons: Tracking

DoH Preference is cached – could be used as tracking vector

Needs to be properly double-keyed

Should only allow resolver from trusted list

# DoH Preference Hints

draft-schinazi-httpbis-doh-preference-hints

IETF 105 – Montreal – 2019-07

David Schinazi – dschinazi@google.com

Nick Sullivan – nick@cloudflare.com

Jesse Kipp – jkipp@cloudflare.com