Developments in Encrypted DNS

RIPE DNS Working Group
28 October 2020

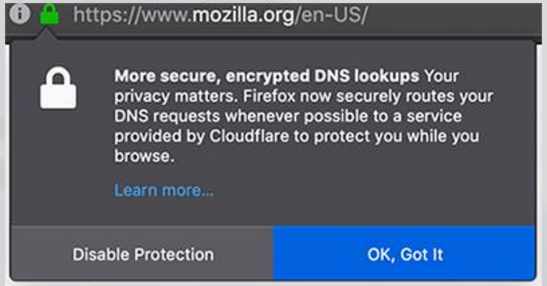
Andrew Campling
Andrew.Campling@419.Consulting

419.Consulting

Background

- Pressure to Encrypt DNS
  - Part of a drive to end-to-end encryption
  - Allegations of abuse of DNS data
- DNS over TLS
  - Available for a while but limited adoption
- Drive to Allow Applications to Access the DNS Directly
- DNS over HTTPS (DoH) Standard Ratified by the IETF
  - October 2018, RFC 8484
  - Just a protocol, no specification to discover or select DoH resolvers
  - Protects DNS queries from being monitored by third parties
  - But can impact illegal content blocking, malicious content filtering, parental controls, CDNs, split-horizon DNS etc

Client Software Support for Encrypted DNS


https://www.mozilla.org/en-US/

More secure, encrypted DNS lookups Your privacy matters. Firefox now securely routes your DNS requests whenever possible to a service provided by Cloudflare to protect you while you browse.

- Firefox (DoH)
  - First major browser to support DoH
  - Implemented by default in the US (Cloudflare then NextDNS, now Comcast too)

- Chrome (DoH)
  - Support from mid May 2020
  - Auto-upgrade facility – doesn't currently work well with the resolvers of many European ISPs

- Apple (DoT and DoH, DNSSEC and ECH to follow)
  - Added in IoS / iPadOS 14 and MacOS Big Sur – first announced at WWDC 2020
  - Configuration options for enterprises, individuals and applications

- Windows 10 (DoH)
  - Support in beta (Windows Insider programme)
  - Auto-upgrade facility – doesn't currently work well with the resolvers of many European ISPs
  - Full release first half 2021?

The IETF ADD Working Group

- Adaptive DNS Discovery Working Group
  - Formed February 2020
  - “This working group will focus on discovery and selection of DNS resolvers by DNS clients in a variety of networking environments, including public networks, private networks, and VPNs, supporting both encrypted and unencrypted resolvers.”
  - Recent discussions have been focused on agreeing use cases and associated requirements
  - Not all the proposed discovery methods reflect the way that the Internet ecosystem functions, especially outside the US

The IETF ADD Working Group

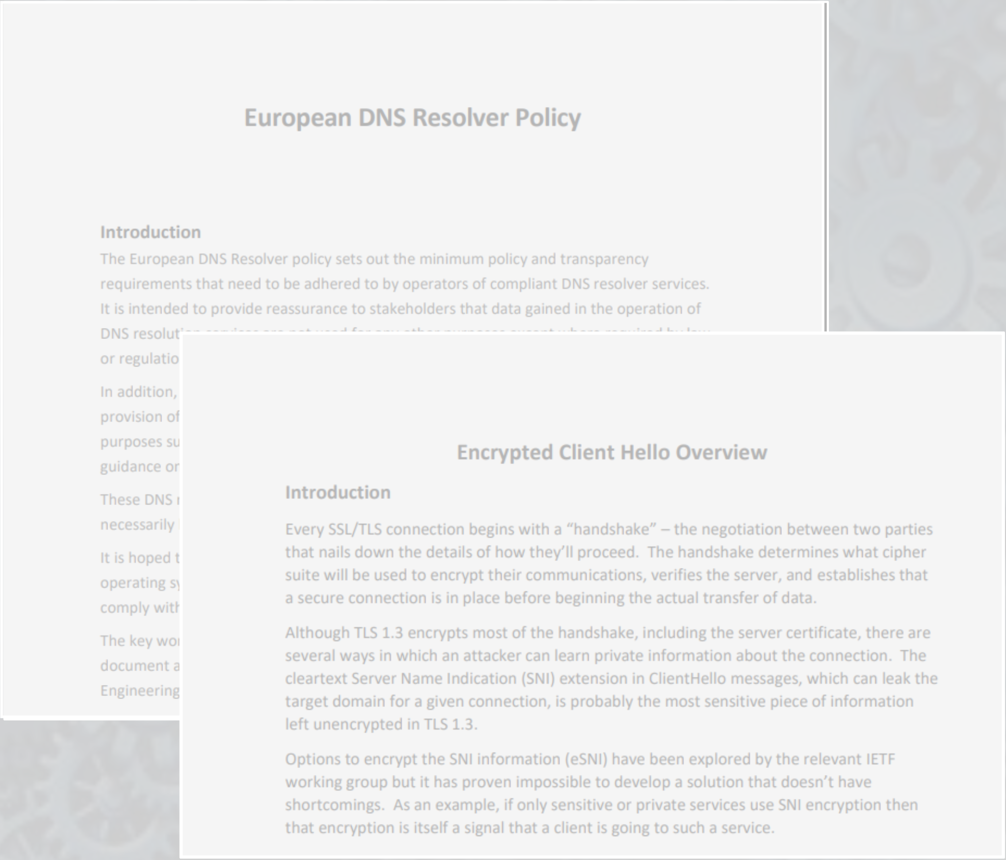
- What About Policy Matters?
  - [The ADD Working Group] "…is chartered solely to develop technical mechanisms. **Making any recommendations about specific policies for clients or servers is out of scope**."
- Related IETF Documents
  - RFC 8932 – Recommendations for DNS Privacy Service Operators
- If Not The IETF Then Where?
  - The Internet Governance Forum
  - The EC's High-Level Group on Internet Governance
  - Encrypted DNS Deployment Initiative

Other Developments

- What About ISPs?
  - Comcast (US) – Firefox, Chrome
  - Deutsche Telekom
  - BT Group

- What About Resolver Policy?
  - Mozilla Trusted Recursive Resolver Programme
  - European Resolver Policy

- What Else is Changing?
  - Encrypted Client Hello (ECH)



European DNS Resolver Policy

Introduction

The European DNS Resolver policy sets out the minimum policy and transparency requirements that need to be adhered to by operators of compliant DNS resolver services. It is intended to provide reassurance to stakeholders that data gained in the operation of
DNS resolut
or regulatio

In addition,
provision of
purposes su
guidance or

These DNS r
necessarily

It is hoped t
operating sy
comply with

The key wor
document a
Engineering

Encrypted Client Hello Overview

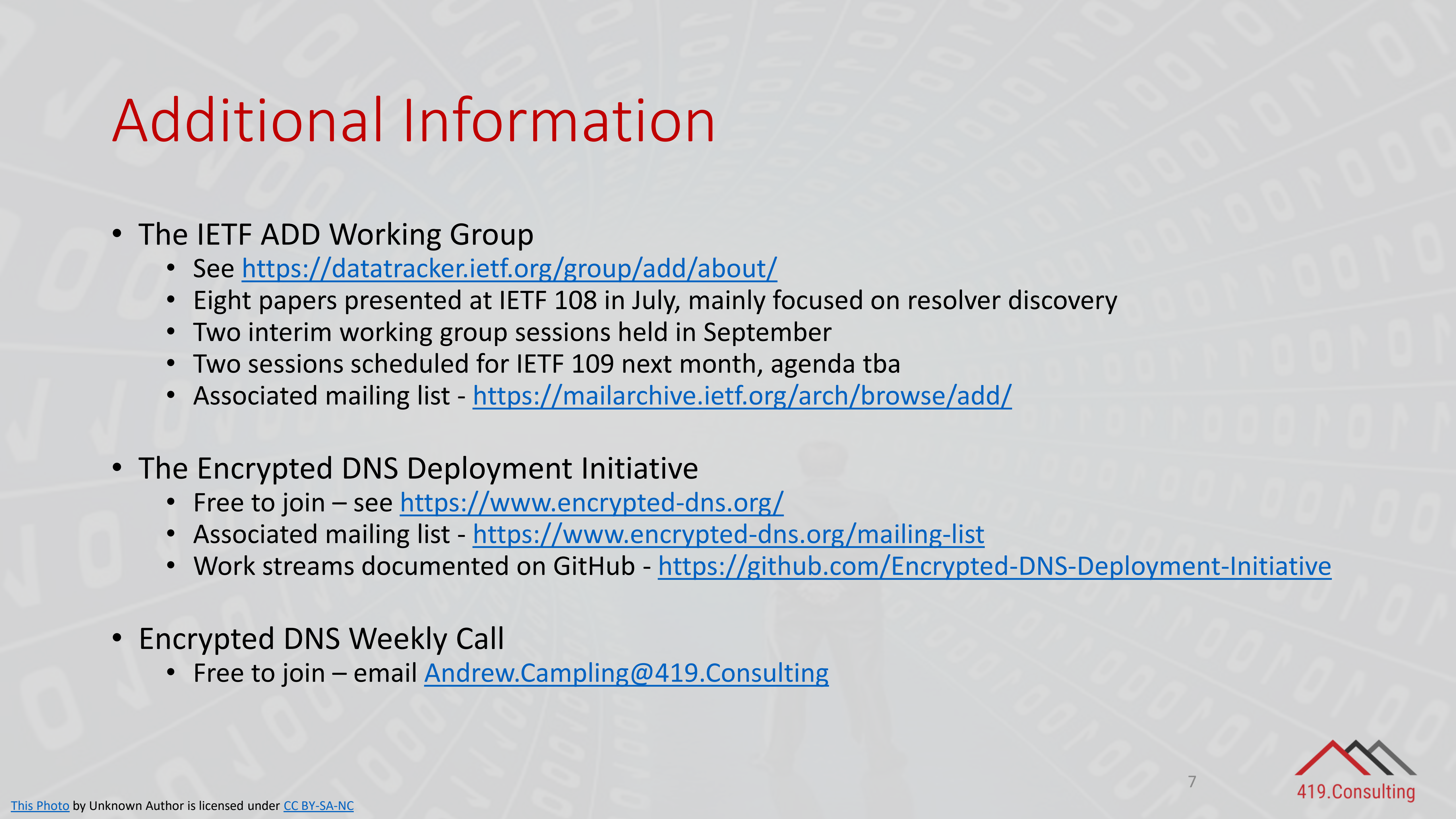
Introduction

Every SSL/TLS connection begins with a "handshake" – the negotiation between two parties that nails down the details of how they'll proceed. The handshake determines what cipher suite will be used to encrypt their communications, verifies the server, and establishes that a secure connection is in place before beginning the actual transfer of data.

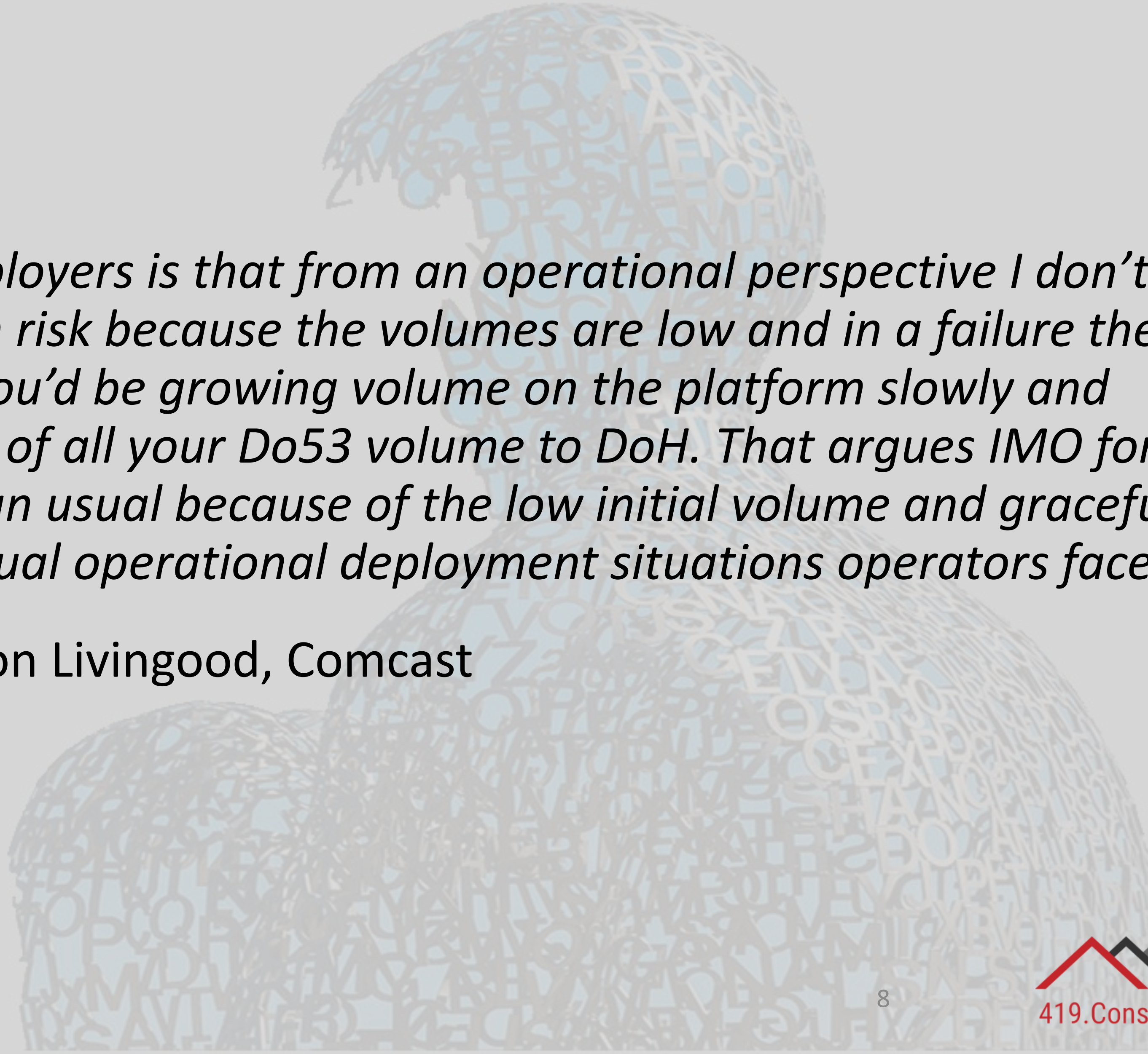
Although TLS 1.3 encrypts most of the handshake, including the server certificate, there are several ways in which an attacker can learn private information about the connection. The cleartext Server Name Indication (SNI) extension in ClientHello messages, which can leak the target domain for a given connection, is probably the most sensitive piece of information left unencrypted in TLS 1.3.

Options to encrypt the SNI information (eSNI) have been explored by the relevant IETF working group but it has proven impossible to develop a solution that doesn't have shortcomings. As an example, if only sensitive or private services use SNI encryption then that encryption is itself a signal that a client is going to such a service.

Additional Information



- The IETF ADD Working Group
  - See https://datatracker.ietf.org/group/add/about/
  - Eight papers presented at IETF 108 in July, mainly focused on resolver discovery
  - Two interim working group sessions held in September
  - Two sessions scheduled for IETF 109 next month, agenda tba
  - Associated mailing list - https://mailarchive.ietf.org/arch/browse/add/
- The Encrypted DNS Deployment Initiative
  - Free to join – see https://www.encrypted-dns.org/
  - Associated mailing list - https://www.encrypted-dns.org/mailing-list
  - Work streams documented on GitHub - https://github.com/Encrypted-DNS-Deployment-Initiative
- Encrypted DNS Weekly Call
  - Free to join – email Andrew.Campling@419.Consulting



“What I say to other potential deployers is that from an operational perspective I don’t think you need to view this as high risk because the volumes are low and in a failure the fallback is to Do53. In essence you’d be growing volume on the platform slowly and organically – this is not a flash cut of all your Do53 volume to DoH. That argues IMO for taking on more operational risk than usual because of the low initial volume and graceful fallback, which is atypical of the usual operational deployment situations operators face“

Jason Livingood, Comcast

419.Consulting

Any Questions?

Andrew.Campling@419.Consulting