European Resolver Policy

ISPCP Membership Session

23rd March 2021

Andrew Campling
Andrew.Campling@419.Consulting

419.Consulting

Background

- Personal Profile
  - 40 years in the tech and telecoms industries
  - Programmer, industry analyst, product management, marketing, public policy and public affairs

- Company Profile
  - 419 Consulting (www.419.Consulting)
  - Public policy and public affairs focused on the tech and telecoms sectors

- Encrypted DNS
  - Documenting practicalities
    - https://datatracker.ietf.org/doc/draft-campling-operator-observations/
    - https://datatracker.ietf.org/doc/slides-108-add-practical-observations-from-encrypted-dns-deployments-by-network-operators/
  - Weekly call

European DNS Resolver Policy

- Developed with input from across the industry
- Recognition that most users do not understand DNS
- Concerns that users are being tracked and their data monetised

It is intended to provide reassurance to end-users and other stakeholders that personal data gained in the operation of DNS resolution services are not used for any other purposes except where required by law or regulation, or with GDPR-level consent of the end-user and where it is clearly documented in the operator's transparency and privacy statement.

Current Policies

- What are the issues?
  - Generally written with a US market perspective
  - No explicit references to applicable legislation and regulations
  - Other requirements can be problematic
  - Applications as gatekeepers, centralisation

- Fragmentation
  - Inconsistency
  - Unhelpful for users

Key Components: Privacy

Except where required or prohibited by law or with GDPR-level consent of the end user[7], operators of DNS resolver services:

- MUST make, document and publish their operational practices to protect the privacy and security of their users' data. The practices documented in the IETF's RFC 8932 ("Recommendations for DNS Privacy Service Operators") SHOULD be adopted for this reason.
- SHOULD NOT retain or transfer to any third party any personal data arising from the use of these services except where anonymised or aggregated data is necessary for cybersecurity, DNS analytics, reporting and research purposes.
- SHOULD NOT directly or indirectly monetise any personal data arising from the use of these services and SHOULD NOT enable other parties to monetise the data either.
- SHOULD NOT use or require HTTP cookies or other tracking techniques when communicating with DNS clients that use HTTP-based DNS transports for resolution.

Key Components: Security and Filtering

- Blocking – must detail categories of material
- Filtering – should be possible to opt in or out
- Cyber intelligence – aggregated material should be shared

Care should be taken in offering DNS resolution without malicious content protection or the blocking of child sexual abuse material as a default option to non-expert end-users such as consumers unless it is unlawful to provide such protections.

Key Components: Transparency

- Transparency and privacy notice – readily accessible, written using plain language, kept up to date
- Clarity on compliance with EU and national legislation
- Details of any personal data that is stored or processed
- Details of data requests from law enforcement agencies – origin and action taken
- Complaints procedure for filtering

Use of the Policy

Full details are available on the website which can be accessed at https://www.EuropeanResolverPolicy.Com.

- Does the new policy cover all types of DNS including the most recent encrypted DNS standards?
  Yes, the policy is designed to be independent of the type of DNS so covers systems using the original DNS standard as well as more recent, encrypted standards including DoT, DoH and DoQ
- What types of organisations are expected to adopt the new policy?
  It is targeted at a range of companies including Internet Service Providers (ISPs) and resolver operators. Other organisations including software developers, membership bodies, industry regulators and legislators may wish to endorse the policy and encourage its adoption.
- How can my organisation adopt the policy?
  Once your processes have been adapted and your transparency and privacy reports updated to reflect the changes, you can contact the team at Enquiry@EuropeanResolverPolicy.Com to confirm that you are committing to remain compliant.
- Are there any charges for companies to adopt the European DNS Resolver Policy?
  No, it is an industry initiative that any organisation is free to join.

419.Consulting

Any Questions?

Andrew.Campling@419.Consulting