

# When DNS goes dark: Understanding privacy and shaping policy of an evolving protocol

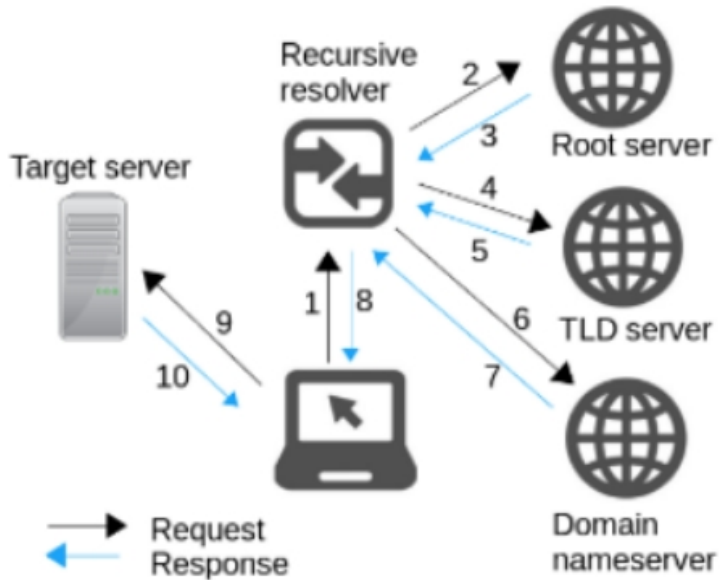
Vijay K. Gurbani, Cynthia Hood, Anita Nikolich, Henning Schulzrinne, and Radu State

vgurbani@iit.edu

DNS Privacy Workshop, NDSS 2021 Symposium  
February 21, 2021



# Introduction



Gurbani, Vijay and Hood, Cynthia and Nikolich, Anita and Schulzrinne, Henning and State, Radu, When DNS Goes Dark: Understanding Privacy and Shaping Policy of an Evolving Protocol (December 16, 2020). Available at SSRN: <https://ssrn.com/abstract=3749764> or <http://dx.doi.org/10.2139/ssrn.3749764>

- DNS: What it is and how it works.
- Traditionally, DNS traffic has been cleartext, recently encrypted.
- Protocol is evolving.
  - Early work on security focused on infrastructure
    - DNSSEC (March 1999)
    - EDNS0 (August 1999)
  - Later (current) on privacy:
    - DNSCrypt (not standardized)
    - DoT (2016)
    - DoH (2018)
    - ODoH (2020, Internet-Draft)
    - Resolver-less DNS (not standardized)

# We are interested in ...

- **As the protocol evolves, do the privacy-preserving extensions enhance user privacy?**



# Why protect DNS queries?

- DNS has a privileged position in the network.
- **Traffic analysis**: prevent tracking.
- **Ads**: Make it harder for ISPs to sell user data.
- **Increase faith in the system**: Protect against destination re-targeting.

Despite DoH, DoT, ODoH, *someone* has access to a user's DNS lookups!

# DNS and PII: Privacy of the user

- Is an IP address PII?
  - US FTC 2016: “...when it can be reasonably linked to a particular person, computer or device.”
  - CCPA: “... [if it] identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”
  - Article 2(a) of Directive 95/46/EC EU Directive: IP address can be considered PII if “directly or indirectly”, the IP address can be correlated with contextual information to allow the identification of an individual.
    - Breyer v. Germany, 2016 upheld this view on the ground that the ISP had enough contextual information to link IP address to individual.

# User privacy and DNS providers

- Examined 12 DNS providers:
  - Google Public DNS, Cloudflare, Quad 9, OpenDNS, NextDNS, Comcast, Yandex, Comodo, Verisign, OpenNIC, Free DNS, dnswatch.info.

# User privacy and DNS providers

- Examined 12 DNS providers:
  - Google Public DNS, Cloudflare, Quad 9, OpenDNS, NextDNS, Comcast, Yandex, Comodo, Verisign, OpenNIC, Free DNS, dnswatch.info.
    - 9 had privacy policies, 3 did not.

# User privacy and DNS providers

- Examined 12 DNS providers:
  - Google Public DNS, Cloudflare, Quad 9, OpenDNS, NextDNS, Comcast, Yandex, Comodo, Verisign, OpenNIC, Free DNS, dnswatch.info.
    - 9 had privacy policies, 3 did not.
    - Of 9 that had privacy policy, 6 had DNS specific policies.
- Next, examine the providers under the lens of 6 GDPR articles.



# User privacy and GDPR

- GDPR Article 5(b): Purpose Limitation
- Taxonomy of reasons for collecting data:
  - 1) Security and visibility into DNS traffic. (OK)
  - 2) Improving services. (OK)
  - 3) Data sharing with affiliates for
    - (i) profit (??)
    - (ii) research in the public good (OK)
  - 4) Marketing (??)
  - 5) Contractual and legal obligations (OK)

# User privacy and GDPR

- GDPR Article 5(c): Data minimization.
  - DNS specific policies fare better than general policies.
    - Enumerated what is being collected or logged.
    - NextDNS: no data logged, but retention (of what?)
  - General policies:
    - Too broad, as they cover all services, not only DNS.
    - Defer to third party privacy policies if a third party feature used in a service.

# User privacy and GDPR

- GDPR Article 5(e): Storage limitation.
  - DNS only privacy policies far more stringent than general privacy policies.
    - Most delete data after 24-48 hours.
    - Some sample data for permanent storage, but anonymize IP addresses or keep data at “city/metropolitan area” level.
    - OpenDNS and NextDNS allow user to delete their data, but not clear how user will exercise this preference.

# User privacy and GDPR

- GDPR Article 7: Conditions for consent.
  - Genuine consent should put user in charge, allowing user to withdraw consent at any time.
  - “Notice and consent” does not work for DNS
    - Does configuring host to use Cloudflare’s resolver constitute consent?
  - Most all of the providers do not require explicit consent to collect user’s DNS information.
    - Consent is given when service is used.
    - One allows account to be created, and associate policies with collection.
  - Withdrawal of consent ambiguous still.
    - Some policies allow withdrawal of consent, but don’t specify the means of withdrawal.
    - Verisign allows “written notification”.

# User privacy and GDPR

- GDPR Article 15: Right of access by data subject.
  - Broad rights to user about purpose limitation and storage limitation (covered earlier).
  - Article 15(e): rectification or erasure of personal data, or restriction of processing of personal data.
    - May impose a burden on the DNS provider, not clear consent is well defined to allow a specific user's records to be traced and purged.
    - IP address may change over time, making tracing time consuming.

# User privacy and GDPR

- GDPR Article 45: Data transfers on the basis of adequacy.
  - What are the obligations of a DNS provider when user's reside outside of the provider's jurisdiction?
  - Primary framework for cross-Atlantic data protection (Privacy Shield) is now invalid (July 16, 2020, EU Court of Justice ruling).
    - Signed signatories must still adhere, new signatories will need bi-lateral agreements.
  - None of the providers had any data transfer information in their DNS-specific policies.

# Policy & standard recommendations

- Standardized disclosure of DNS privacy policies
  - Jurisdiction, data residency, retention, delete data on request, ...
- Make it easy for users to configure the DNS service.
- Enhance regulatory clarity:
  - Should ISP-provided resolver service be treated as an adjunct service?

# Policy & standard recommendations

- Role of standards bodies, especially IETF.
  - Unique position to specify protocol behaviour.
    - The Raven document (RFC 2804).
  - Should continue to engage in more robust user-centric privacy threat modeling.
    - RFC 8932 is a laudable step.
      - Recursive operator Privacy Statement (RPS) forces DNS providers to focus on user-centric privacy.



# Policy & standard recommendations

- User centric privacy policies.
  - RFC 8932 good example.
  - Simplified purpose limitation statement.
  - Transparency on retention.
  - Transparency on consent.
    - Re-configuring */etc/resolv.conf*: Is this consent?
    - Should DoH be opt-in?
    - How to stop consent?
  - Transparency in adequacy decision.

# Policy & standard recommendations

- Shaping the protocol evolution.
  - Early DNS extensions aimed at infrastructure privacy (DNSSEC).
  - Later ones improved user privacy: DNSCrypt → DoT → DoH → ODoH → ??
  - If viewed as a game between rational actors (privacy advocates and market forces), does the user benefit?
    - Pursuing dominant strategy will result in user privacy being the casualty (Resolverless-DNS).
  - What's the answer?
    - Light hand of regulations?
    - Industry regulations (Mozilla TRR Program)?

# Conclusions

- DNS has a privileged position in the network ecosystem.
- Most users unaware of DNS.
  - “Privacy by default” should be the de-facto mode.
- Public resolvers gaining traction.
  - A single public resolver could achieve monopoly status under certain conditions.
- Data privacy regulations or self-regulation.
- **Above all, user’s privacy should be the centerpiece.**