DNS Privacy Vs.

Confronting Protocol Design
Trade-Offs in the Public Interest

Authors

- Mallory Knodel, Center for Democracy & Technology
- Shivan Sahib, Salesforce

Goals

I. Confront tensions between privacy protection and other public interest principles.

II. Inform public interest advocates of these tensions with technical rigour.

III. Begin to ease tensions by building consensus on shared goals amongst public interest advocates.

IV. Identify research gaps.

Abstract

This short paper attempts to catalogue and briefly treat the predominant emerging tensions that impact the public interest, introduced by DNS privacy measures.

Making DNS lookup more private for the user affects internet measurements, consolidates service provision, makes abuse mitigation harder and risks internet shutdown for some users…

… And yet it is in the public interest and the interest of the internet protocol standards community to properly research these emerging tensions with data, informed as much as possible by the effects on end users.

This paper points toward additional research in order to better mitigate the possible negative effects of DNS privacy on the public interest.

Table of Contents

1. Introduction
2. Vs. Measurement
3. Vs. Consolidation
4. Vs. Abuse
5. Vs. Shutdowns
6. Conclusions

DNS PRIVACY

1. Introduction

Two foundational documents:

1. RFC 6973 -- Makes the case for DNS and other internet protocols to be designed to protect end user privacy.

2. RFC 8280 -- Establishes how human rights, including the right to privacy are impacted.

MEASUREMENT

2. Measurement

Public interest benefits: 1) Knowledge of network performance and operation are critical for access, 2) Empowering users as consumers, and 3) Monitoring of behaviours that might impact human rights, such as freedom of expression.

But: 1) Measurements can come at the cost of user privacy and 2) Measurement becomes more difficult when user data is more private.

So:

- Can research methodologies simply incorporate private DNS resolution?
- What research methodologies **cannot** be used when DNS lookup is private?
- Does user choice have an impact, eg DoT in OS vs DoH in apps?

CONSOLIDATION

3. Consolidation

Public interest concern: Consolidation of internet service provision 1) Is economically detrimental, 2) Degrades quality of service for users, 3) Slows innovation, 4) Creates single points of failure, 5) Facilitates mass surveillance, 6) Complicates regulatory jurisdiction.

But: 1) The ubiquity and large market share of a few browsers and operating systems presents an opportunity for fast, at-scale adoption of private DNS and 2) Early adopters have made privacy a viable business model.

Yet: 1) Private DNS is not monolith and the details that consolidated services make matter, 2) Diversity is at risk when trust and privacy are transactional.

So:

3. Consolidation (continued)

So:

- How do deployment models, from protocol to default settings, compare with respect to consolidation?
- Do trust models centre the user or the intermediary?
- In what ways is this tension between privacy and diversity fundamental to the DNS itself?
- How are users best empowered to change that default and help them make a meaningful decision respecting their own privacy threat model?
- **Does ubiquitous adoption of private DNS really resolve consolidation?**

ABUSE

4. Abuse

Public interest benefit: Mitigating abusive behaviour and legitimate restrictions at the content layer 1) serves end users and 2) is critically necessary in the human rights framework.

But: 1) Privacy enhancing technologies can have the unintended consequence of making abuse mitigation harder to track. 2) Losing the ability to mitigate abuse on a network is a loss in the public interest. 3) An overly complicated and interdependent grouping of private DNS protocols might lead an operator or implementer to make mistakes.

4. Abuse (continued)

So:

- How useful is DNS-based abuse prevention?
- What resources are required for traffic analysis of encrypted DNS for targeted mitigation?

SHUTDOWNS

5. Shutdowns

Public interest concern: Internet shutdowns violate the rights to free expression, access to information, and assembly.

But: Authoritarian governments are sufficiently motivated and resourced and over time wield digital technology in their favour, **or they control it**, to surveil users and censor information.

Yet: Response to the initial deployment of new DNS privacy has been to effectively shutdown volumes of traffic based on protocols, rather than content or user data, thus casting a much wider net on populations in China, Russia, etc.

So: What happens when DNS blocking is no longer used by authoritarian governments?

MOAR NOT LESS

6. Conclusions

- Resolving tensions with measurement and abuse: Ubiquity solves the problem of consolidation on its surface, although more research is needed to understand the more hidden and knock-on effects of early leadership by a small number of DNS privacy providers.
- Tensions of consolidation and shutdowns (and usability):
  - Implementations at the app level center intermediaries,
  - Who then have greater control over user choice.
- In general: At minimum what is needed is a set of best practices for implementers
  - To grow a robust ecosystem of DNS privacy provision that attempts to resolve these tensions.
  - Normative guidance that recommends for DNS operators and application developers on options.
- Also: The authors open a call for research that considers more deeply the four trade offs, as well as if there are other tensions not considered.

Next steps

1. Put document in GitHub and call for PRs, issues
2. Include “Vs Usability and Accessibility”
3. Make more nuanced distinctions between DoH, DoT, and other DNS privacy measures
4. Find appropriate venue for publication.