# DNS Privacy - The Problem

## Why is DNS a privacy concern?

Some of the issues in simple terms:

- Almost every activity on the Internet starts with a DNS query (and often several).
- Those queries can reveal not only what websites an individual visits but also meta data about other services such as the domains of email contacts or chat services.
- Whilst the data in the DNS is public, individual transactions made by an end user **should not** be public.
- However DNS queries are sent in **clear text** (using UDP or TCP) which means passive eavesdroppers can observe all the DNS lookups performed.
- The DNS is a globally distributed system that crosses international boundaries and often uses servers in many different countries in order to provide resilience.
- It is well known that the NSA used the MORECOWBELL tool to perform mass surveillance of DNS traffic.
- Some ISPs embed user information (e.g. a user id or MAC address) within DNS queries that go to the ISPs resolver in order to provide services such as Parental Filtering. This allows for fingerprinting of individual users.
- Some CDNs embed user information (client subnets) in queries from resolvers to authoritative servers (to geo-locate end users). This allows for correlations of queries to particular subnets.
- Some ISPs log DNS queries at the resolver and share this information with third-parties in ways not known or obvious to end users.

> The DNS is one of the most significant leaks of data about an individuals activity on the Internet.

For an expert review of this topic recommended reading is DNS Privacy Considerations.