What's the DNS, anyway?

DNS-OARC 31

Vittorio Bertola, Head of Policy & Innovation
Austin, 1 November 2019

Stay Open.

This all started at IETF 105…

One main reason

DNS is an effective control point

Not a good reason

DNS ~~is~~ **was** an effective control point

Mozilla's presentation from the ADD BoF at IETF 105, Montreal, 23 July 2019
(the choice of font is theirs)

Even if this is a fallacy…

DNS is NOT an effective control surface

It doesn't always work

≠

It doesn't work!

If the DNS is not a control surface…

…what’s the DNS, anyway?

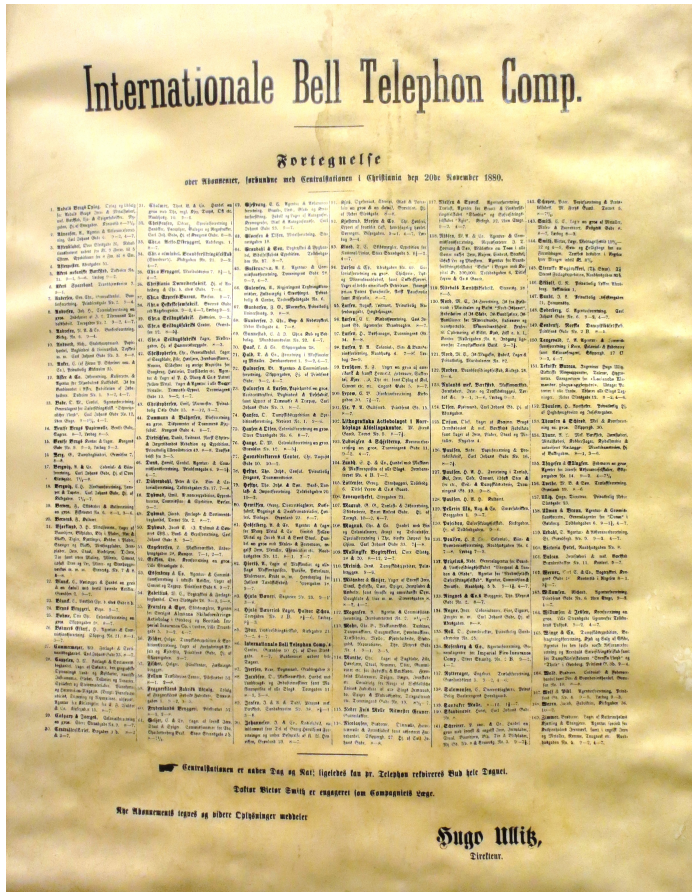
What’s the DNS, anyway?

What’s the DNS, anyway?

- RFC 1034 gives no definition – just a description of its components.
- RFC 8499 («DNS Terminology») starts with «The Domain Name System (DNS) is defined in literally dozens of different RFCs.», but does not provide a pointer to a definition.
- It then says «The Domain Name System (DNS) is a simple query-response protocol whose messages in both directions have the same format.» *(is really the DNS just a protocol?)*
- Namecheap says «The domain name system (DNS) connects URLs with their IP address.»
- PC Magazine says «The Internet's system for converting alphabetic names into numeric IP addresses.»
- Wikipedia says «The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.» *(which is actually a better definition than anything the DNS community has ever produced)*
- DNS gurus, when asked, tend to mention «a distributed database».

What's the DNS, anyway?

Is it really a database?


Internationale Bell Telephon Comp.

Fortegnelse

Hugo Ullitz,

Or is it a direction system?

What's the DNS, anyway?

A database

always gives back the same response when queried for the same key

A direction system

may give different responses when queried for the same key, depending on who you are, where you are and other relevant factors

Which of the two models describes the DNS better today?

Things that cannot exist, but they do

If DNS were a database, we would not have:

- Local-only / private names
- Split DNS
- DNS-based CDNs
- Resolvers blocking malware and bots
- DNS-based parental controls
- DNS-based law-mandated blocks
- DNS-based censorship

All these things are not censorship, except censorship

All these things are widely in use everywhere today

What's the DNS, anyway?

In a database

it doesn't matter whom you ask to,
since everyone
always gives you the same reply

In a direction system

different nodes
may give you different responses,
so whom you ask to
makes all the difference

**If the DNS were a database,
we would not be arguing over
applications choosing a different resolver**

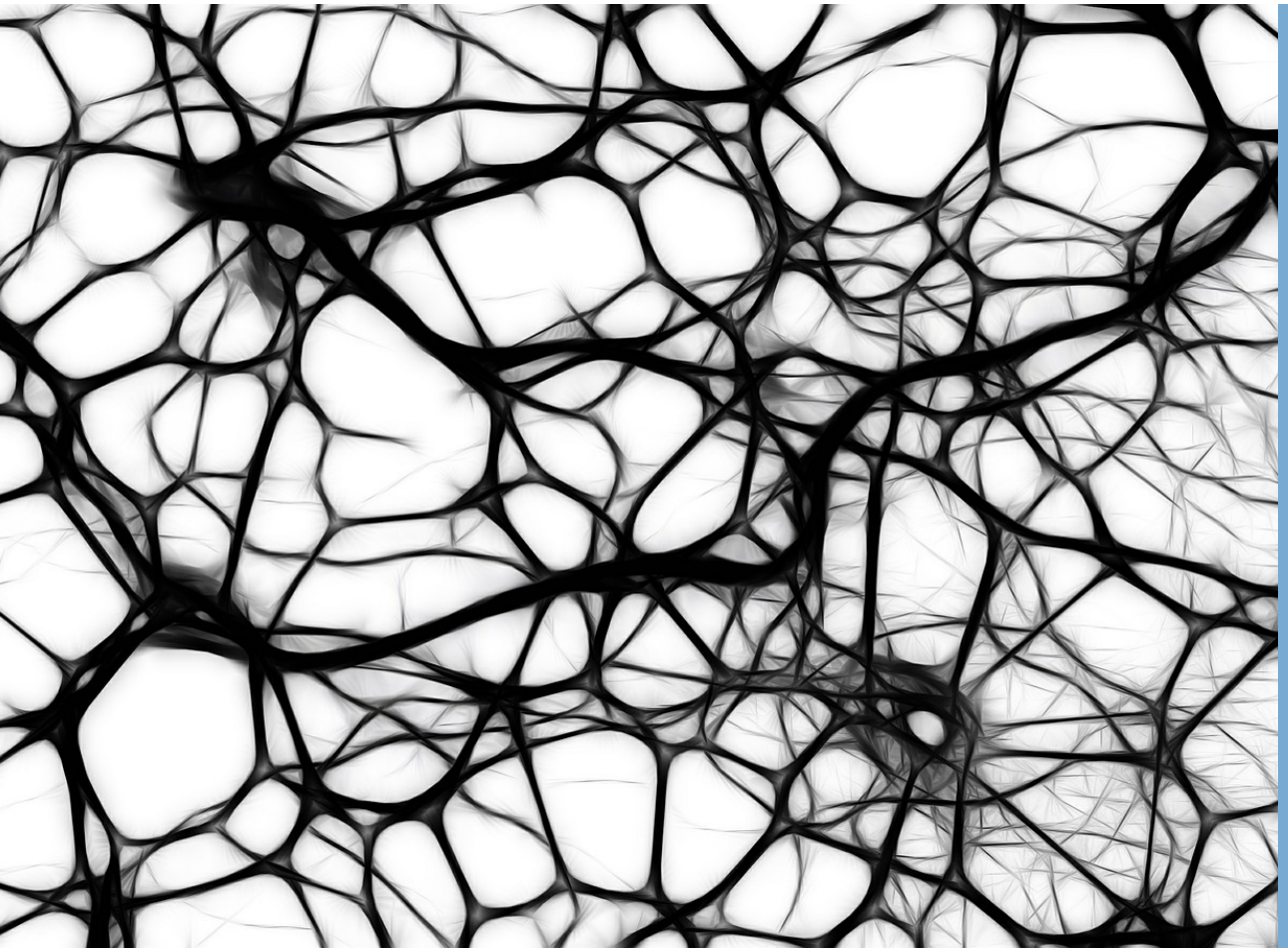
In the beginning, the DNS was a database.

Today, the DNS is a direction system.

(maybe we are not too happy that it is,
but it is)

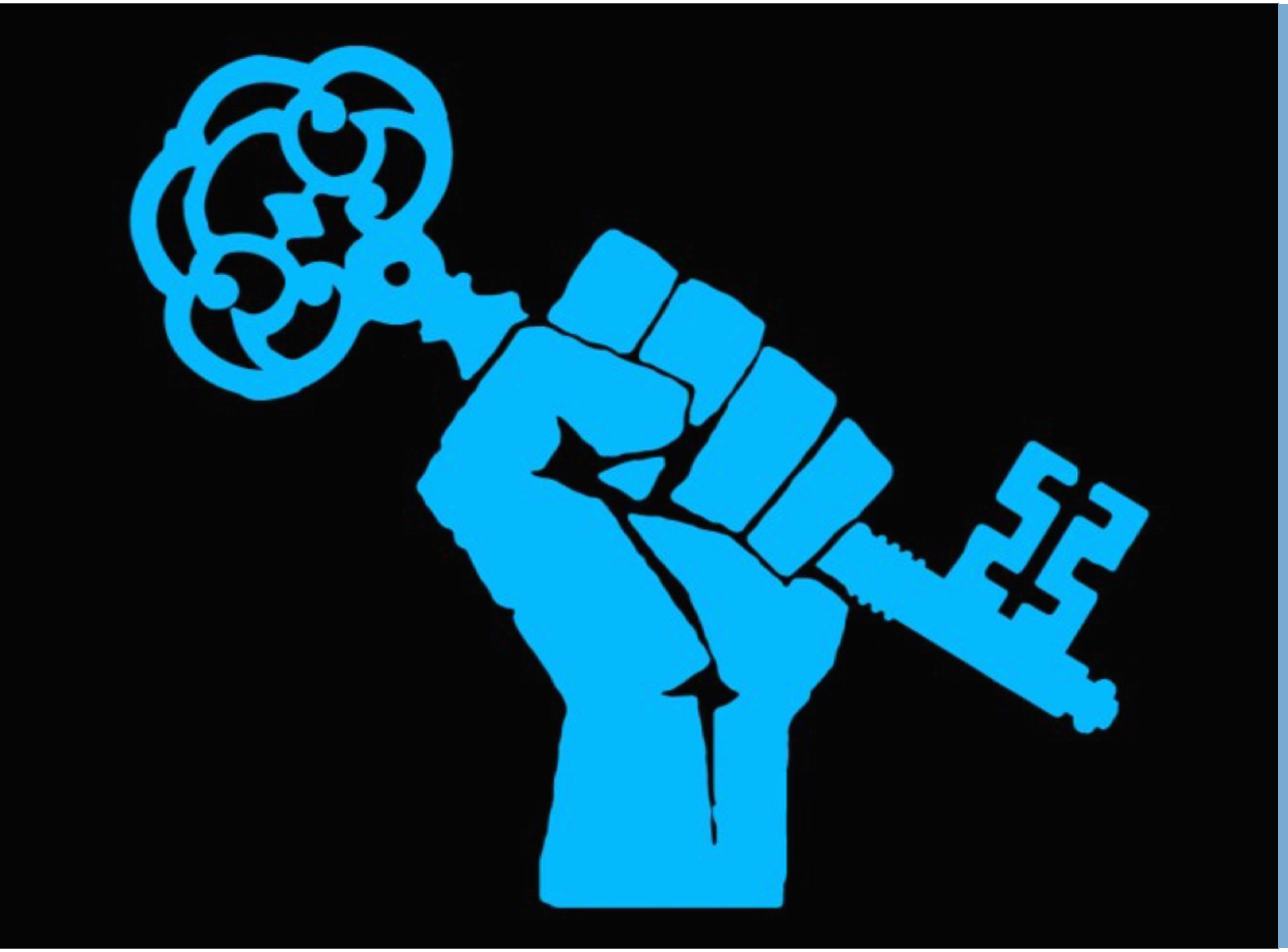
Properties of DNS as a direction system

Resolvers are smart



- Resolvers are increasingly complex and intelligent
- This strains the DNS camel
- They do not fit the «dumb network, dumb pipes» model that the OTTs are pursuing

Channel security is vital



- **Making you talk with a different resolver is an attack**
- **You need a private, authenticated connection to your resolver**

The resolver is the oracle

- There are no lies
- «Truth» is anything your resolver tells you
- The resolver is the source of trust
- The choice of the resolver is super-important

Data integrity in DNS as a direction system

- DNSSEC «to the client» is not necessary any more
  - But it can still be useful, to caution the user against a resolver that should not be trusted
  - But only if implemented in the client application
- DNSSEC is still necessary between the resolver and the authoritatives
  - But only if the resolver wants to abide by the public DNS root
  - And the resolver perhaps could just authenticate the authoritatives in some other way

The resolver is a great control point

- **...since you are bound to accept whatever the resolver says**
- **The resolver knows both you and the Internet pretty well, so tailoring responses is easy**

Local resolvers give you more privacy

(as long that they don't sell your data)

On-device resolvers (running on your own device)

- Make you fully in control of your resolution
- But all queries coming from there are definitely yours
- So it is trivial for an observer to associate all your DNS activities with you

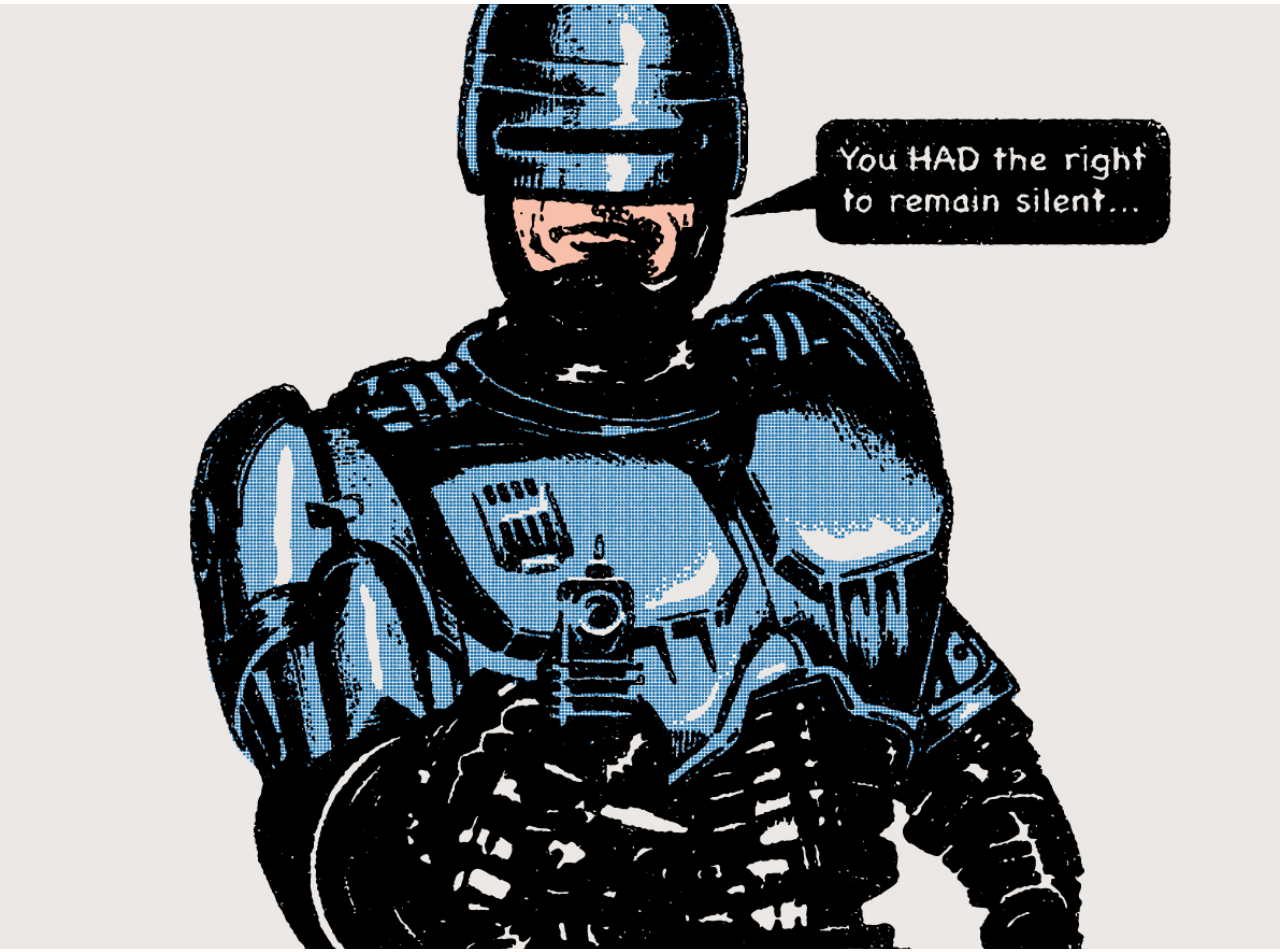
Local resolvers (running on your local access network)

- Can mix your queries among those of others near you
- But can still represent your network position with good accuracy by providing only their own address
- So they can get good directions while making it hard to isolate your queries and associate them with you
- They can also tailor the responses for you without further authentication

Remote resolvers (running somewhere else on the Internet)

- Can mix your queries among those of millions of other people
- But have to disclose your IP address to authoritatives if they are to provide accurate directions for your position
- So they give you less privacy than local resolvers
- They also need you to authenticate to provide tailored services

The resolver is your biggest potential enemy



- You are at your resolver's mercy
- A malicious resolver can deprive you of privacy, phish you, sell you out...

Conclusions for discussion

Consequences of denying reality

By refusing to admit that the DNS is a direction system and not a database:

- We talk past each other, because in our minds we have different concepts for the same thing
- We spend a lot of time arguing about resolver selection, but we cannot really understand why or frame that discussion properly
- We prompt an increasing divide between big resolver platforms with smart capabilities and small dumb resolvers, which will lead to centralization unless the smart features are standardized and made widely available
- We cannot agree on efforts to optimize the DNS for its current reality

In the beginning, the DNS was a database.

Today, the DNS is a direction system.

What do we think it should be tomorrow?

Thank you!

vittorio.bertola@open-xchange.com

Stay Open.