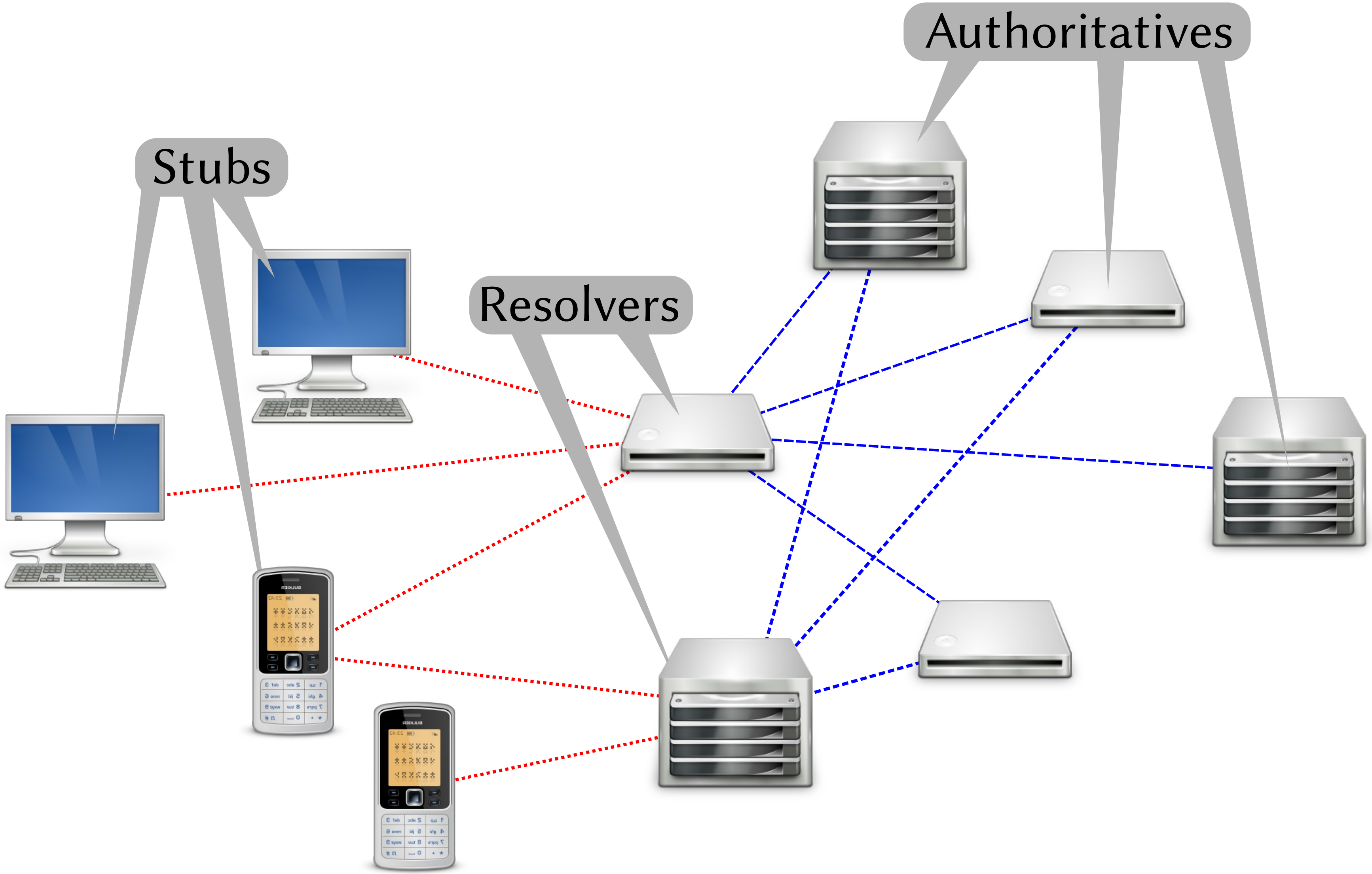
NDSS DNS Privacy 2021

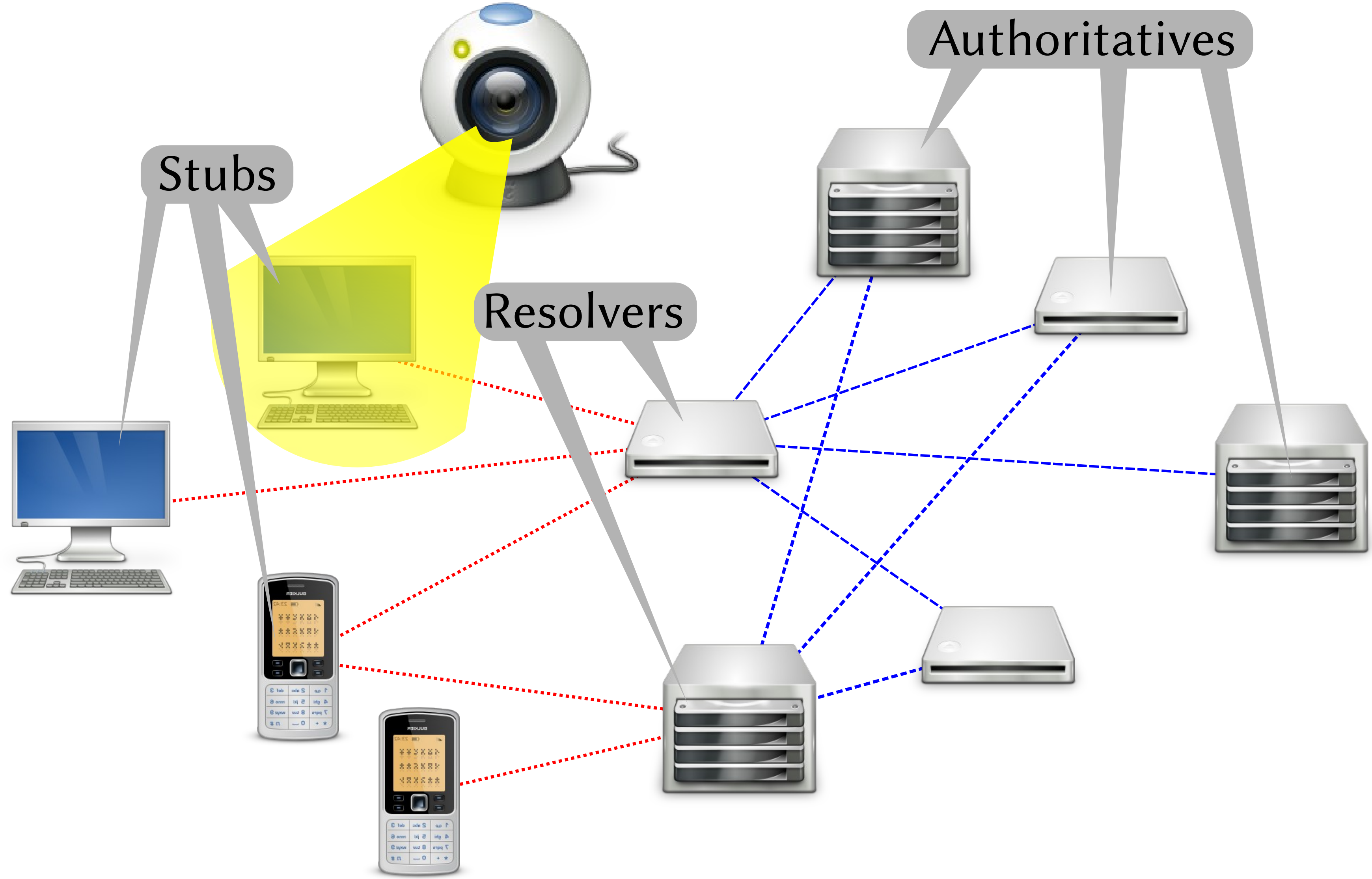
Daniel Kahn Gillmor
dkg@aclu.org

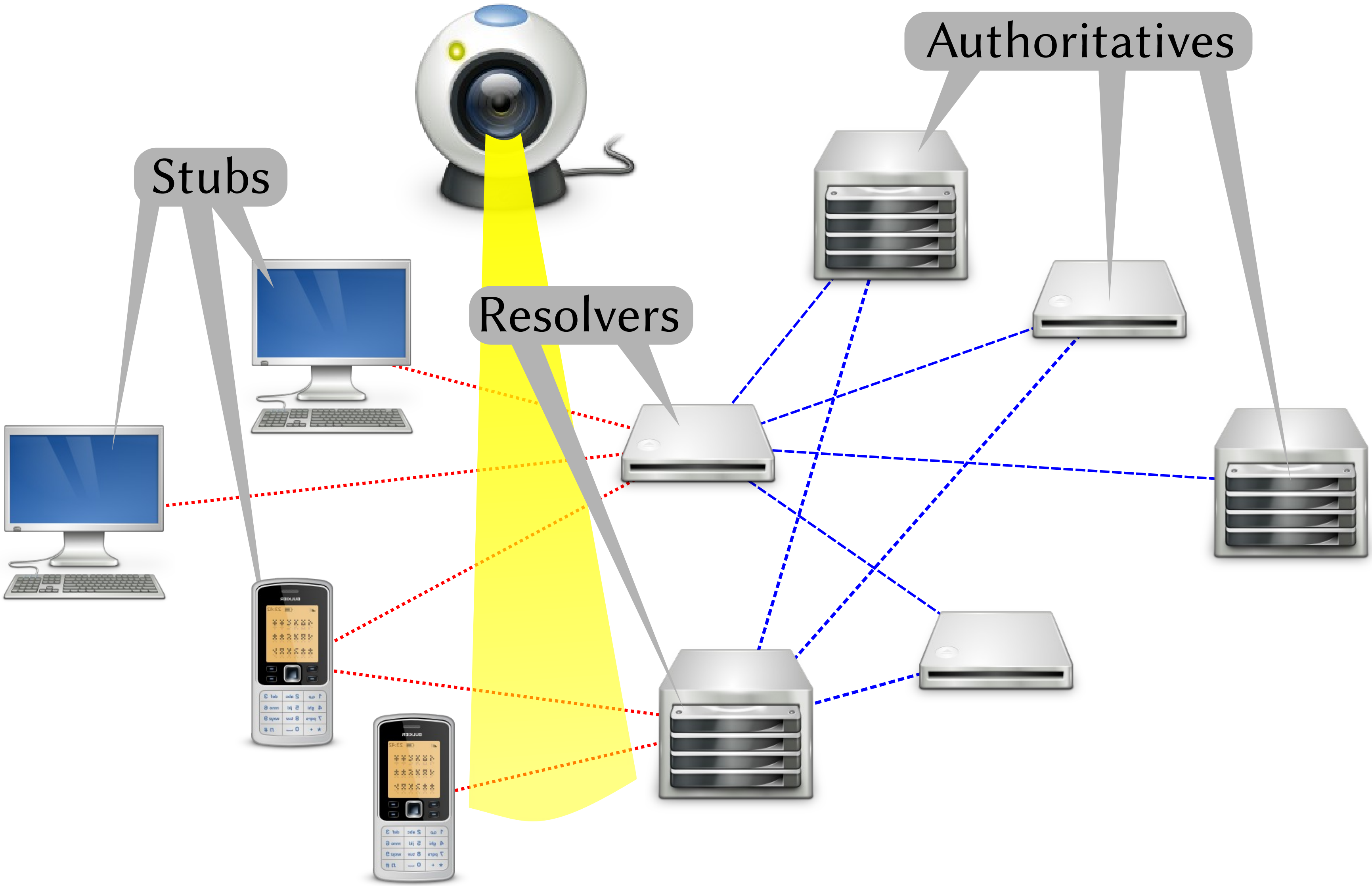
Protecting the Back Half of the Camel

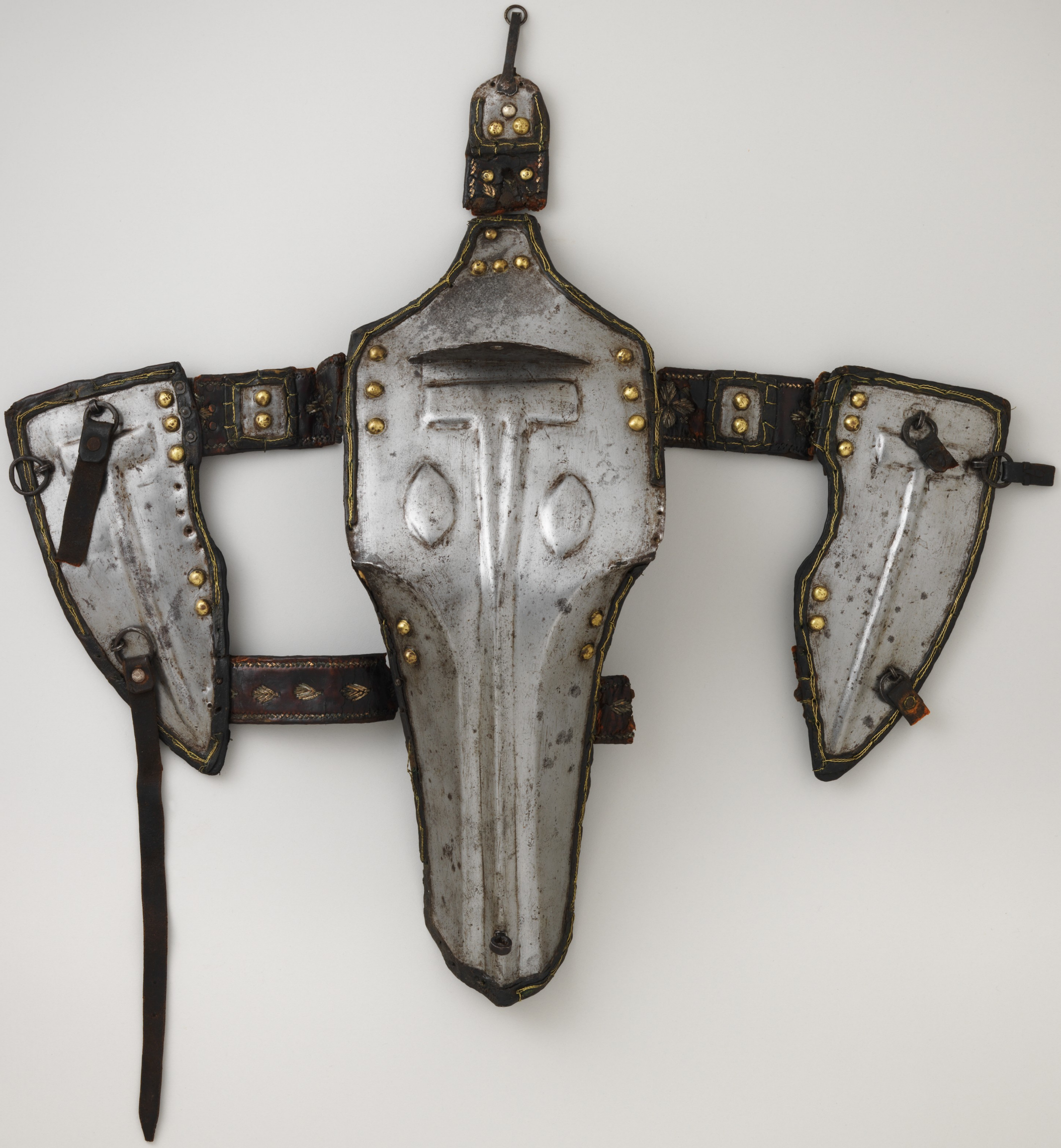
Stub to Recursor

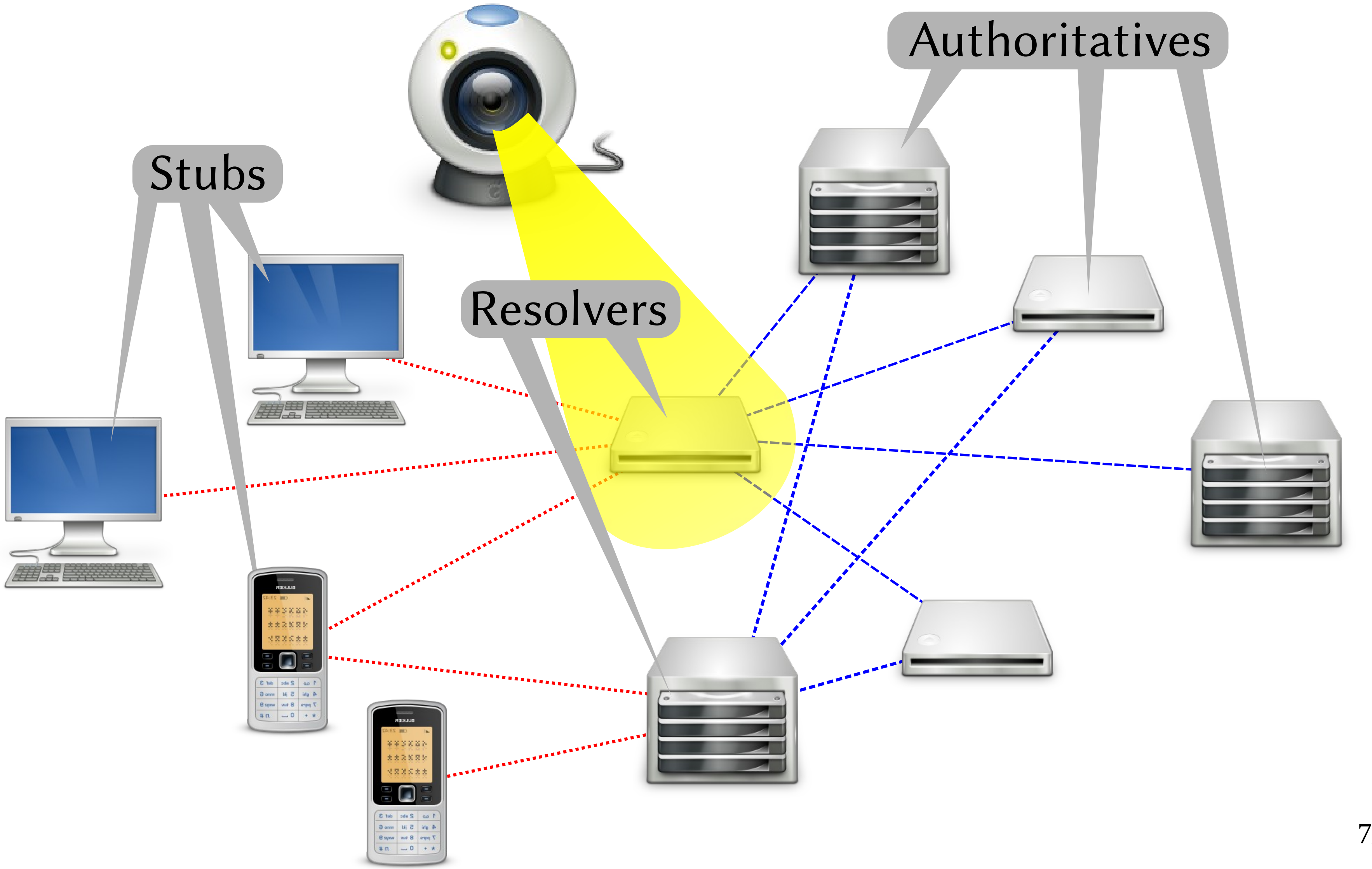
Recursor to Authoritative


Stubs
Resolvers
Authoritatives


Authoritatives
Stubs
Resolvers

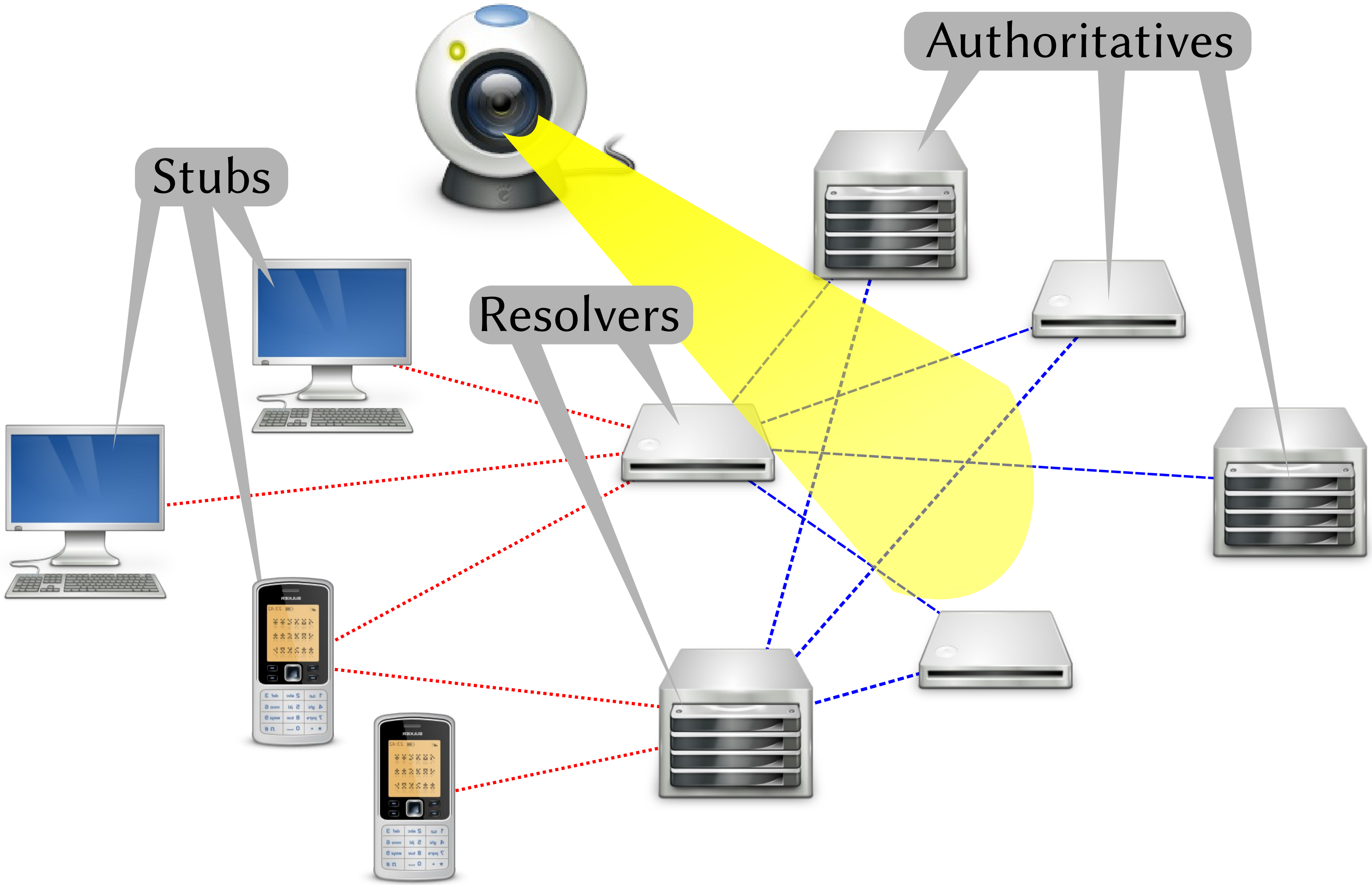

Authoritatives
Stubs
Resolvers



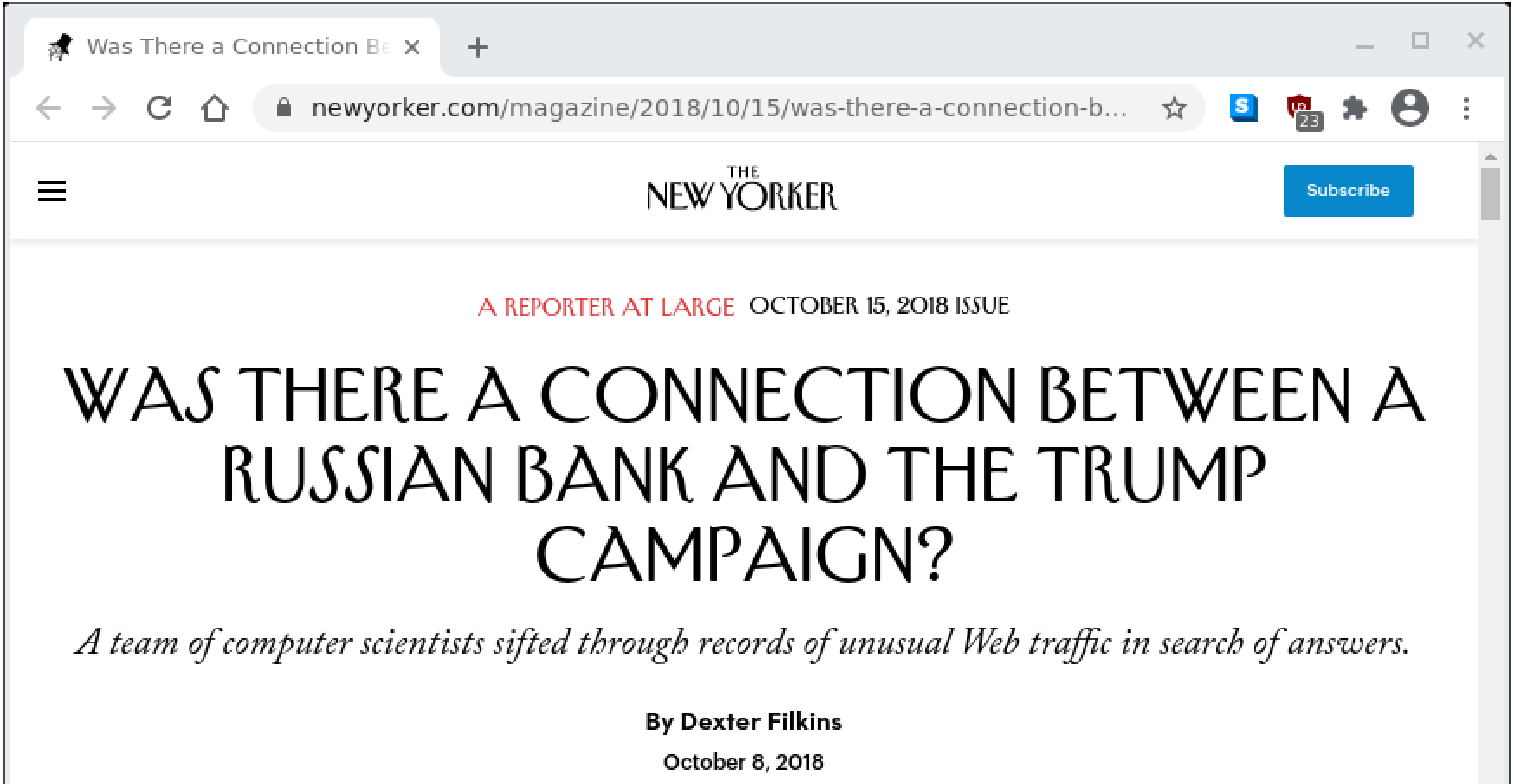

Authoritatives
Stubs
Resolvers

Resolver Operators are Stewards of Client Activity

- Timing analysis
- Traffic size analysis
- Correlations


Authoritatives
Stubs
Resolvers

Associational Metadata


Was There a Connection Be
newyorker.com/magazine/2018/10/15/was-there-a-connection-b...
23
THE NEW YORKER
Subscribe

A REPORTER AT LARGE OCTOBER 15, 2018 ISSUE

WAS THERE A CONNECTION BETWEEN A RUSSIAN BANK AND THE TRUMP CAMPAIGN?

A team of computer scientists sifted through records of unusual Web traffic in search of answers.

By Dexter Filkins

October 8, 2018

Non-encryption Mitigations

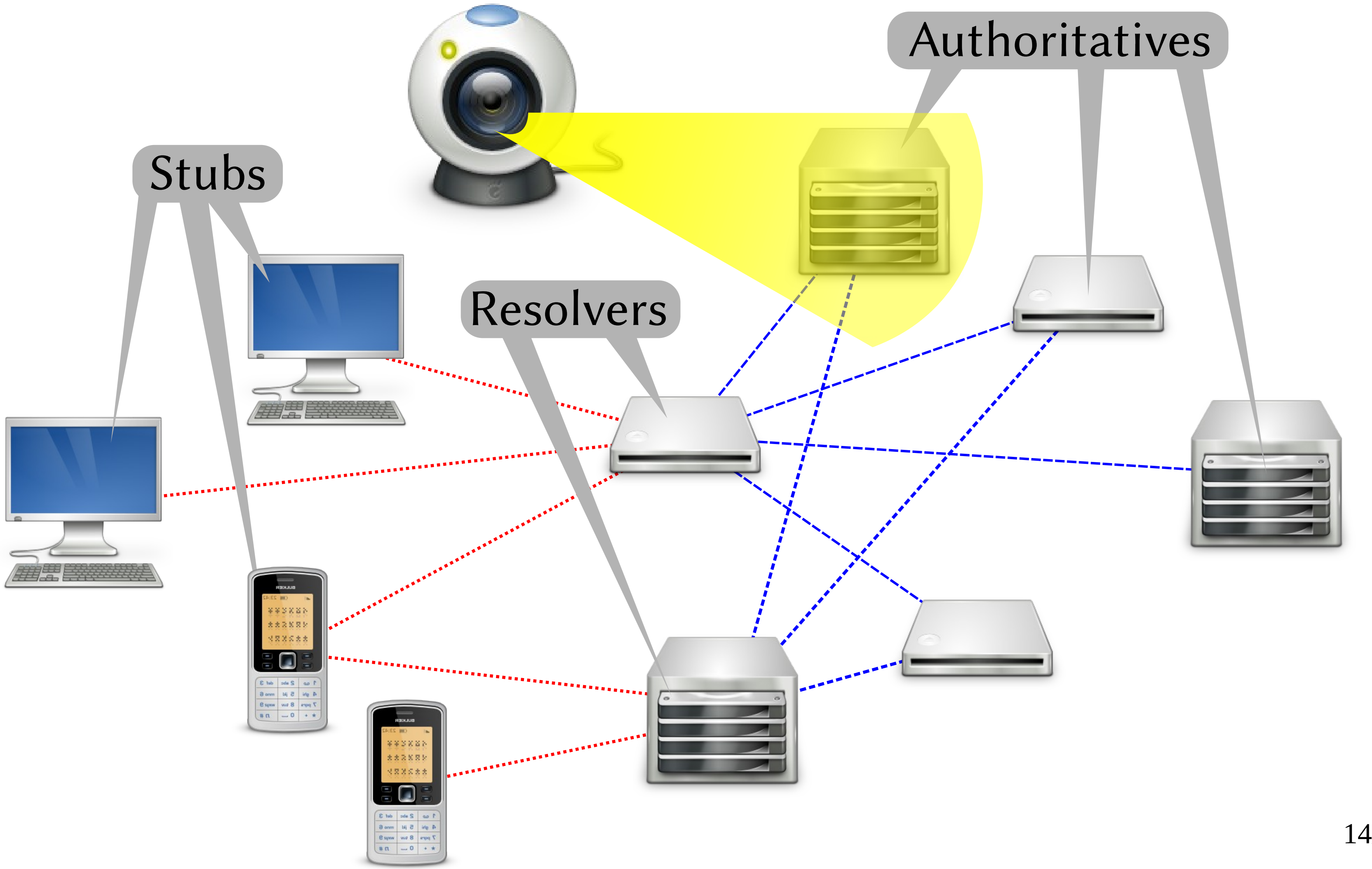
- QNAME Minimization
- NXDOMAIN synthesis (RFC 8198)
- NXDOMAIN cuts (RFC 8020)
- Pre-fetching
- Request pooling (delays)
- ...

Even Second-level Domains can be Sensitive

- **`falundafa.org`**
- **`nra.org`**
- **`plannedparenthood.org`**
- **`parler.com`**
- **`disruptj20.org`**
- …

Resolver Operators are at Risk

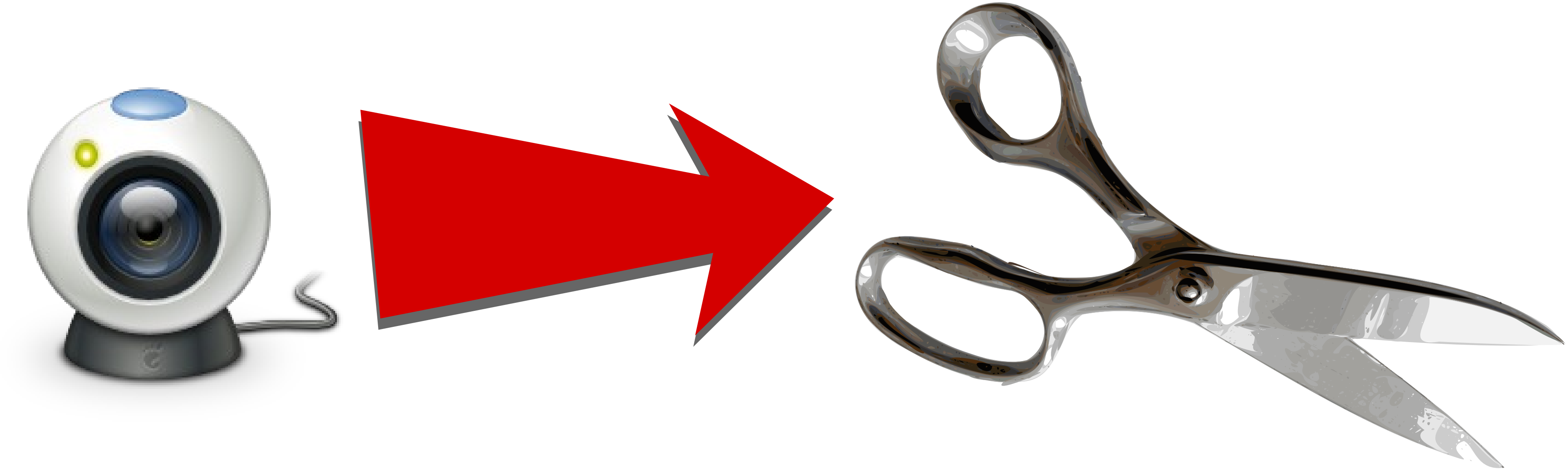
- Legal demands
- Extralegal investigation


Authoritatives
Stubs
Resolvers

Resolver Operators are Stewards of *Subject* Activity

Beyond IP address lookups...

- SMIMEA
- OPENPGPKEY
- DNS UPDATE
- TXT (e.g., DKIM selectors)
- ...



Surveillance enables Censorship

- Tampering
- Blocking
- *Affects subject, regardless of querier*

What can we do?

How to get there (easy/unilateral)

- Augmenting Authoritatives (DoT? DoQ? DoH?)
- Opportunistic strategies for resolvers: probing, pooling
- Resource management (resolvers & authoritative)

How to get there? (riskier, needs coordination)

- Authentication (WebPKI or DANE)
- Who signals? (Nameserver or Domain)
- How to signal? (special NS label or separate record)
- What to signal? (Avoid, Report, Require)

Questions?

Daniel Kahn Gillmor
dkg@aclu.org

dns-privacy@ietf.org