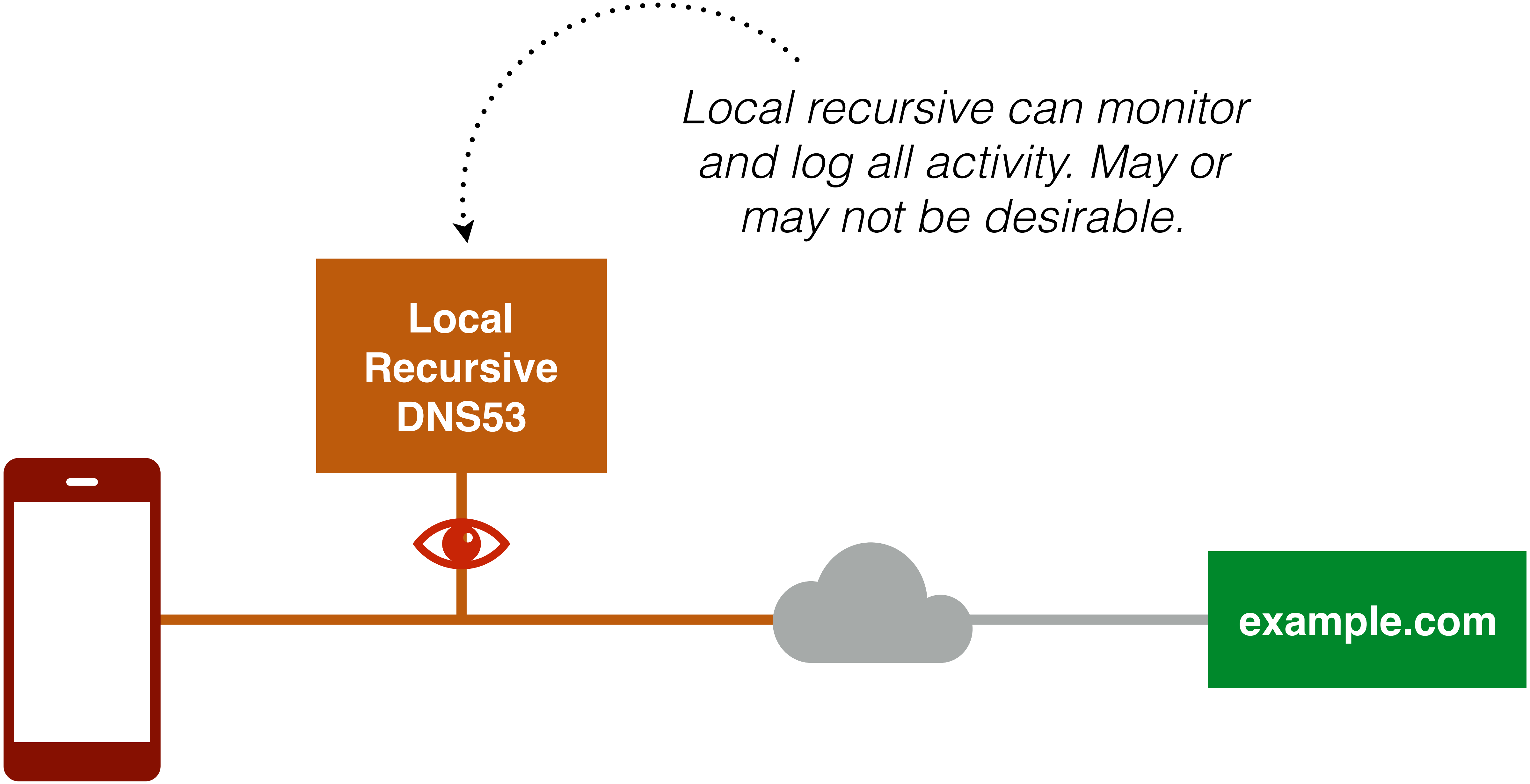
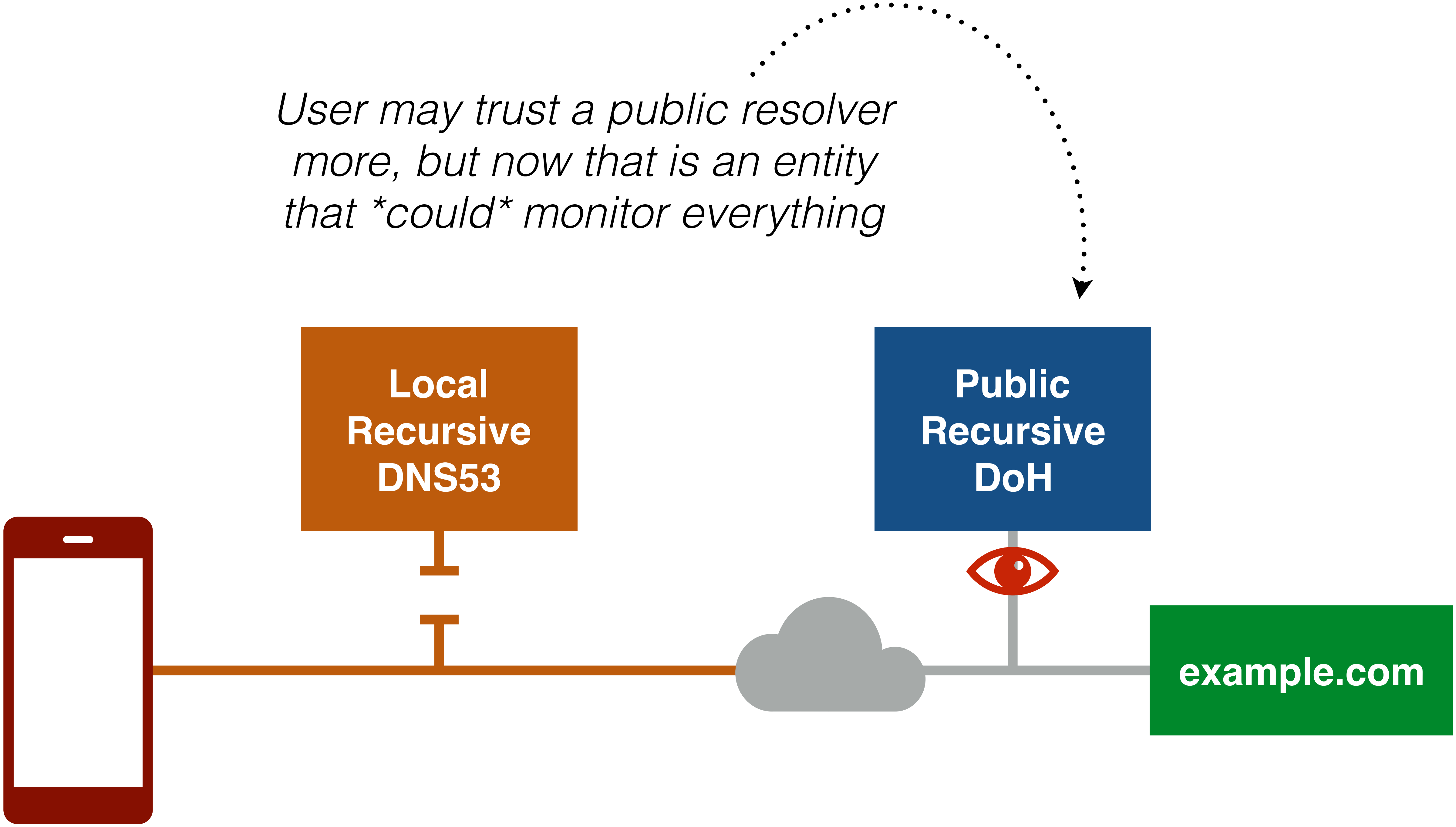
Adaptive DNS Privacy
&
Oblivious DoH

HotRFC
IETF 106, November 2019, Singapore



Local recursive can monitor and log all activity. May or may not be desirable.

*User may trust a public resolver more, but now that is an entity that *could* monitor everything*



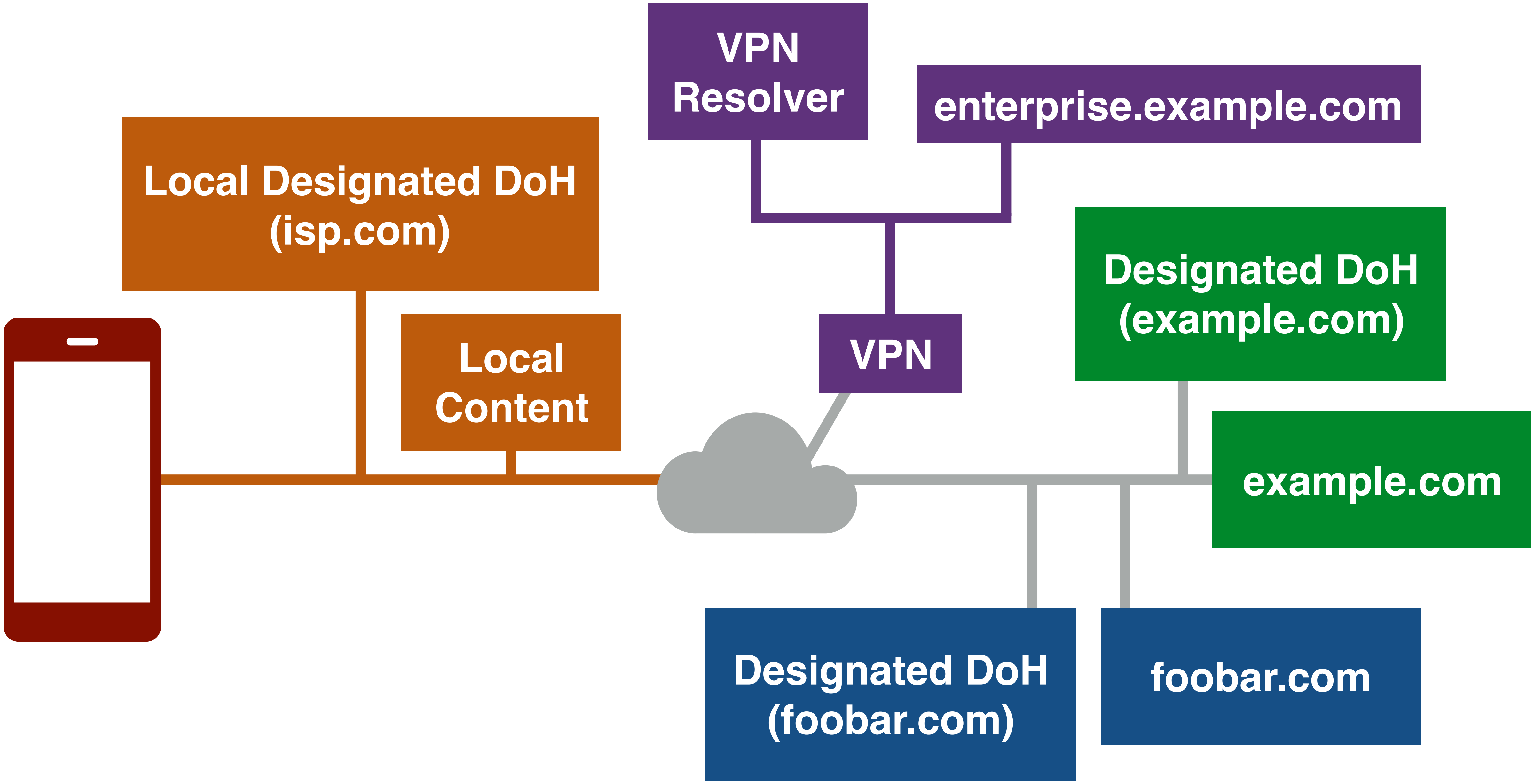
Adaptive DNS Privacy

Discover many different decentralized DoH servers

Designate DoH servers by domain/zone

Discover local DNS policy and server capabilities

Decide which DNS servers to use for queries


VPN Resolver
enterprise.example.com
Local Designated DoH (isp.com)
Designated DoH (example.com)
Local Content
VPN
example.com
Designated DoH (foobar.com)
foobar.com

How do you bootstrap this system
if you don’t trust the local resolver...

...without just trusting one
public resolver instead?

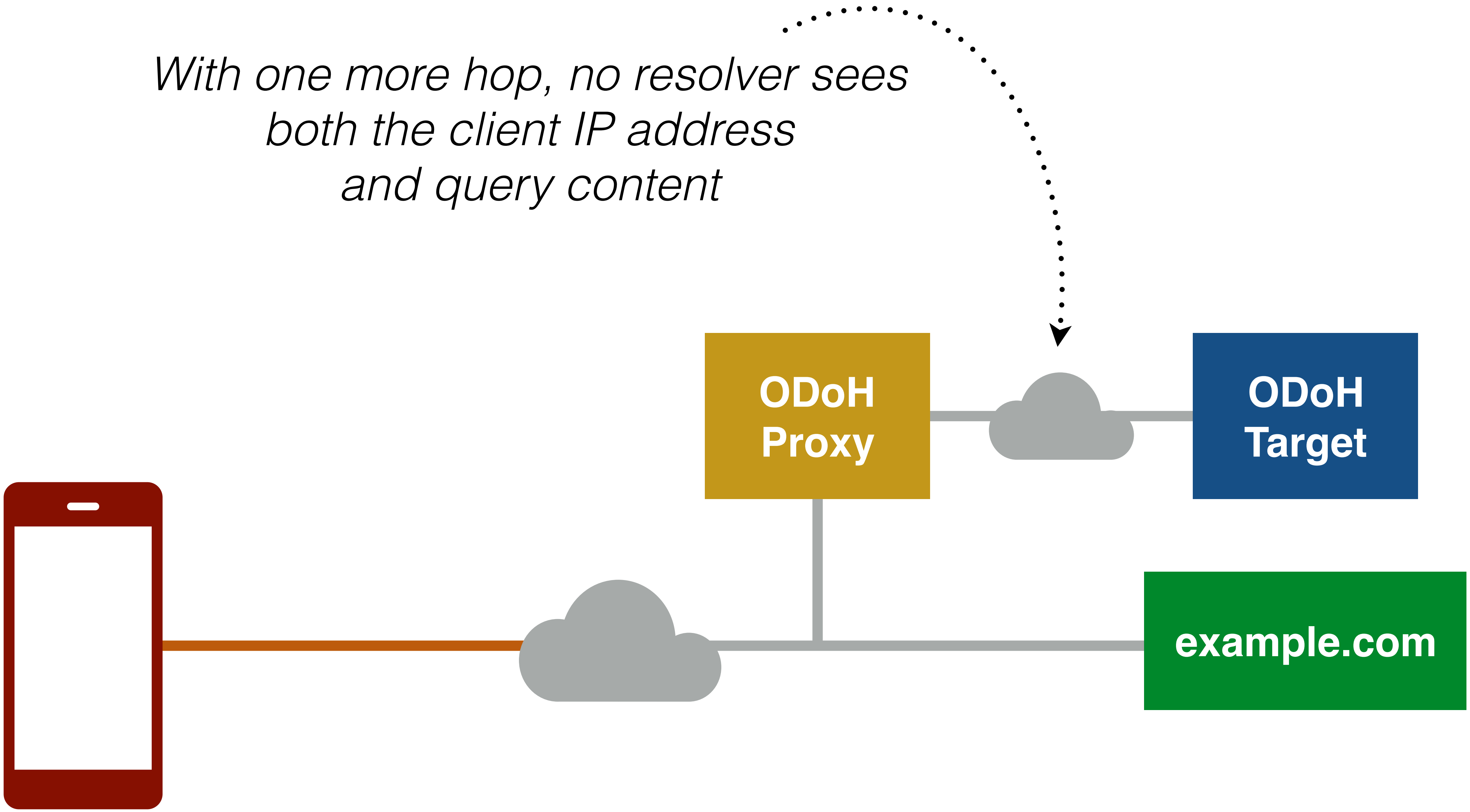
Oblivious DoH

Proxy DoH queries in order to mask client IP address

Encrypt requests with server public key

Encrypt responses with one-time symmetric key

With one more hop, no resolver sees both the client IP address and query content



Get involved!

ABCD BoF

DPRIVE

draft-pauly-dprive-adaptive-dns-privacy-01

draft-pauly-dprive-oblivious-doh-01

https://github.com/tfpauly/draft-pauly-adaptive-dns-privacy