Surveillance and Control Risks Arising from Outsourced DNS

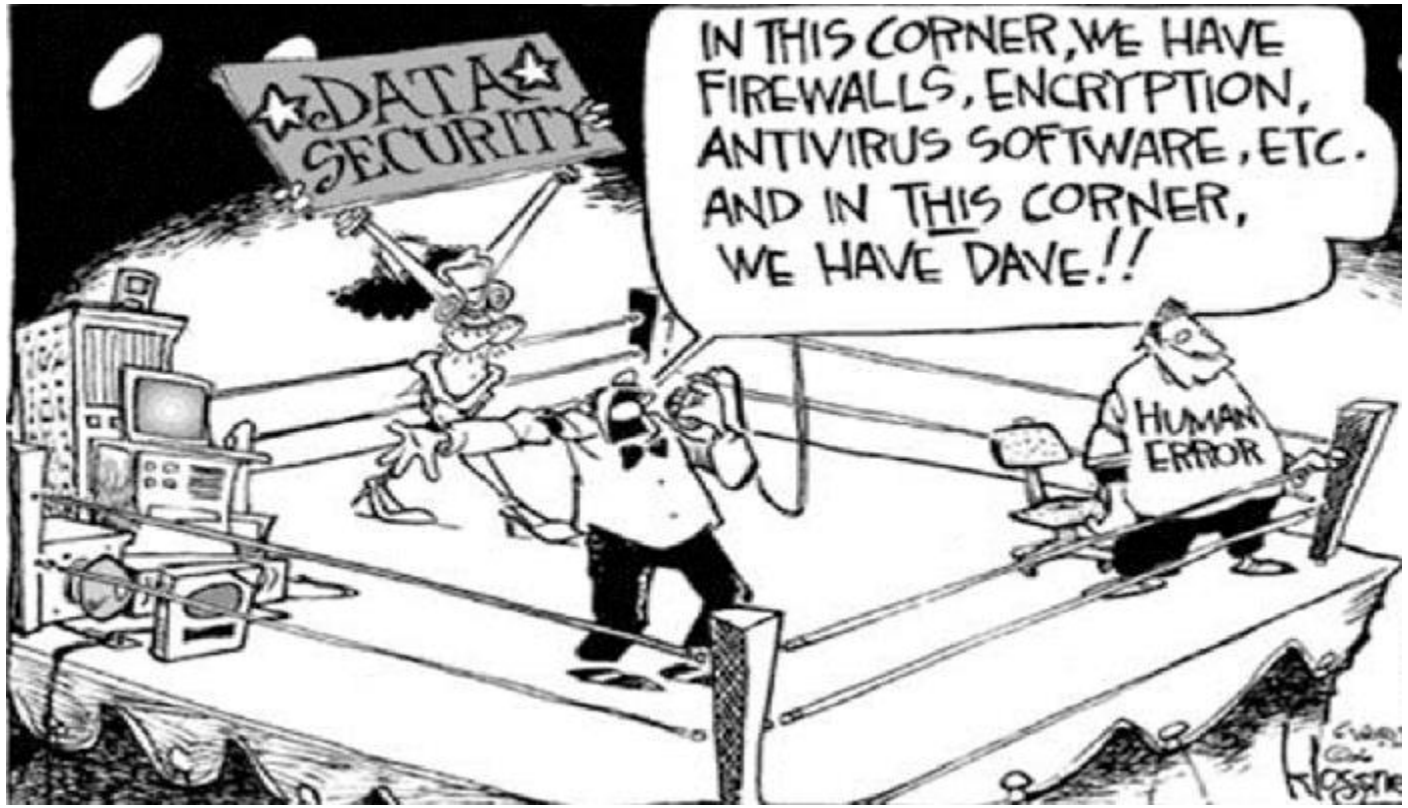
Dr. Paul Vixie, CEO
Farsight Security, Inc.

2019-03-26

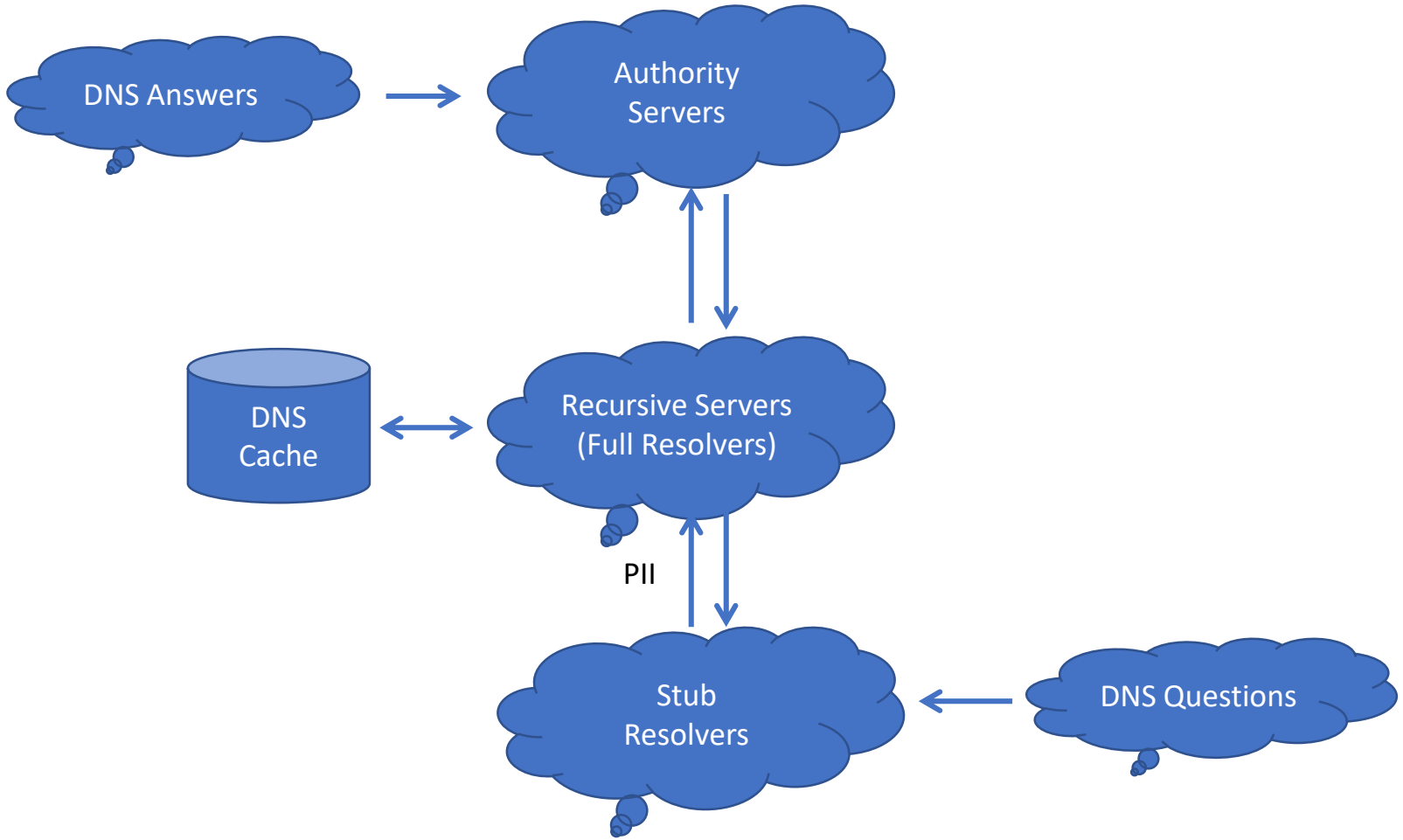
Abstract

- Silicon Valley has insinuated itself into the Domain Name System (DNS) resolution path, simply by providing a free service and waiting for the inevitable madness of crowds to drive traffic to that service. Since almost all Internet activities begin with a DNS transaction, this provides dangerous insight to noncontracted parties who have no limits to their use of our data. In this lecture, Dr. Vixie explain the basic technology involved, and the history of the last 15 years of surveillance capitalism's DNS agenda. The recent DNS Over HTTPS (DOH) standard will be described, and recommendations will be made for individuals, families, and businesses as to restoring and retaining control over their digital exhaust.

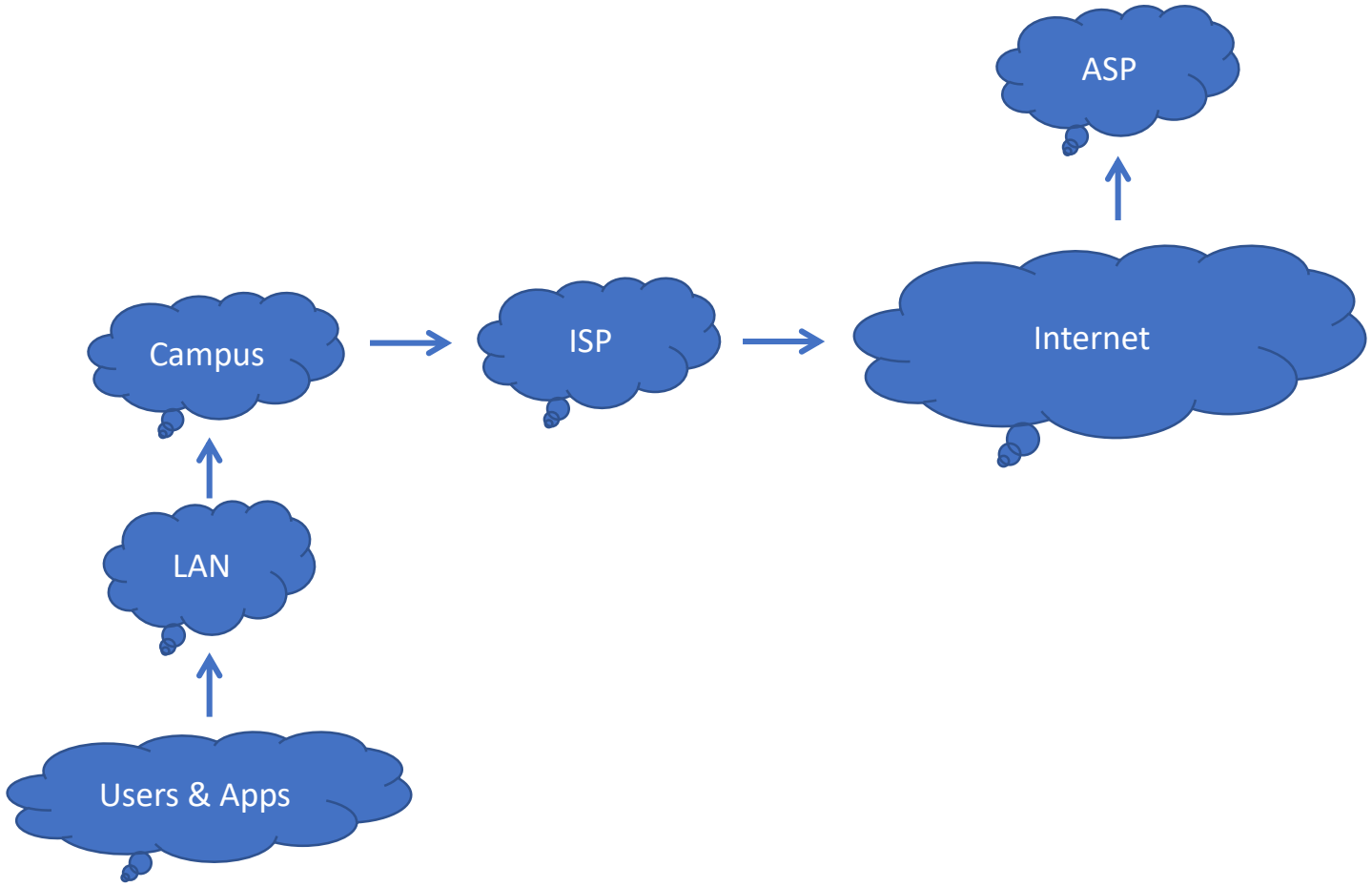
CSO … CIO … CISO



DNS System Architecture



Internet System Topology



Commercialization and Privatization (~1994)

- As the Internet began to outgrow its academic/government origins:
  - The number of connected networks doubled every month for quite a while
  - Most of these new networks did not speak BGP or connect to an IXP
  - Businesses such as WorldNet were created to service this new market
- Non-technical businesses were never told to run their own RDNS
  - RDNS thus moved away from the LAN/Campus and into the local ISP
  - ISP's interests were well aligned: caching meant less upstream traffic
  - Nevertheless, running a LAN or Campus RDNS was still common

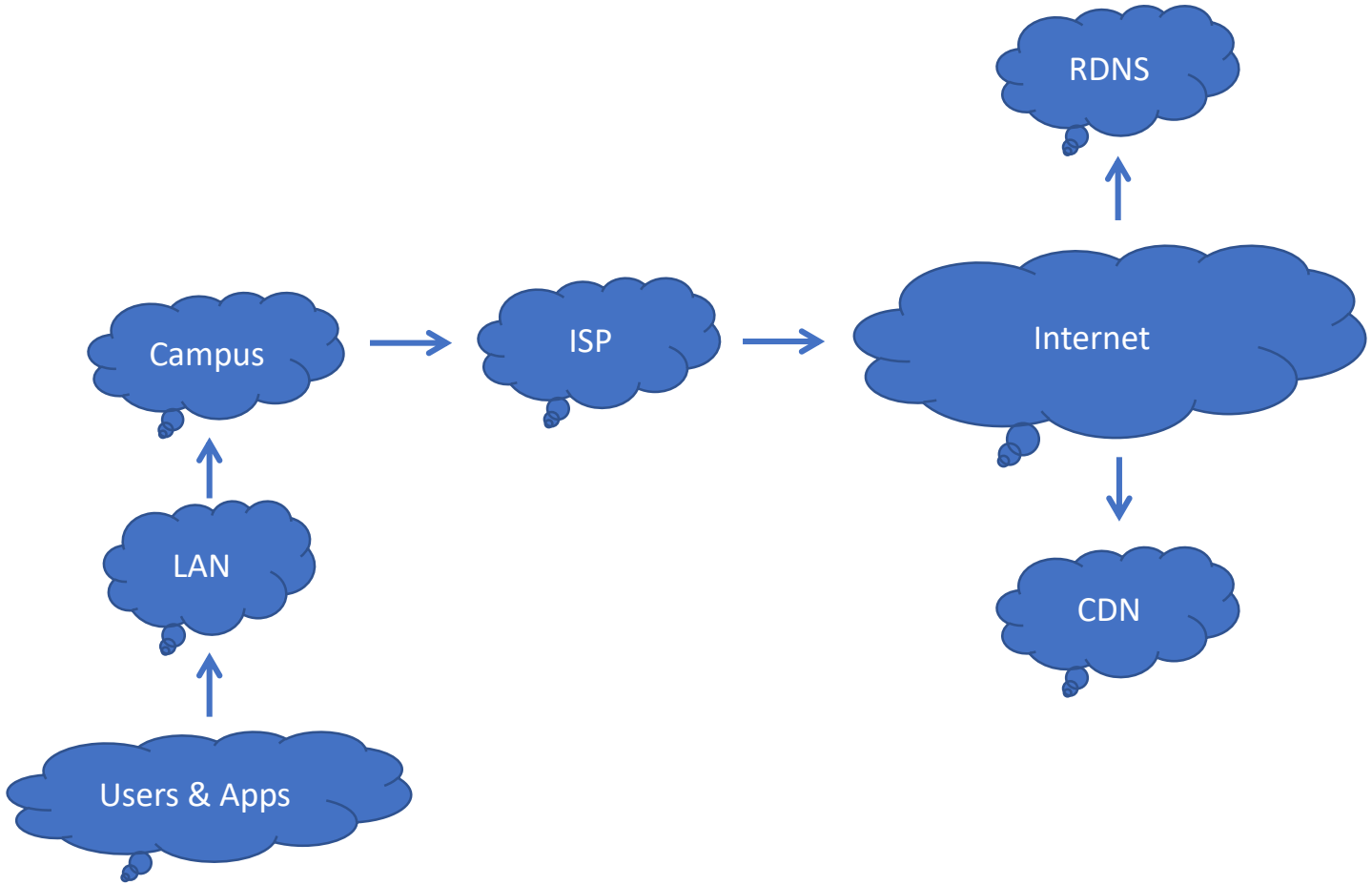
Economic Products of Centralization

- End systems (hosts, routers, gateways) are rarely upgraded
  - Creates a “long tail” problem which limits systemic innovation
  - Makes deliberate first- or last-mover policies practical
- ISP and ASP systems are rapidly and often upgraded
  - Makes protocols like IPv6, EDNS and DNSSEC more deployable
  - Creates opportunities for abuse of power (surveillance; ad insertion)
- There isn’t a simple, timeless, or universal winning position
  - Like all build vs. buy decisions, centralization is a case by case matter
  - Mistakes will be made; tension will exist; powers will be abused

Anycast RDNS (~2005)

- OpenDNS was created to provide RDNS services to the whole Internet
  - This was seen as innovative and/or controversial at the time
- Early business model included NXDOMAIN redirection
  - So a typographic error in a web browser led to an advertising page
- They also intercepted lookups for www.google.com
  - Each search was redirected to Google after keywords were extracted
  - This led directly to Google's investment in RDNS which became 8.8.8.8

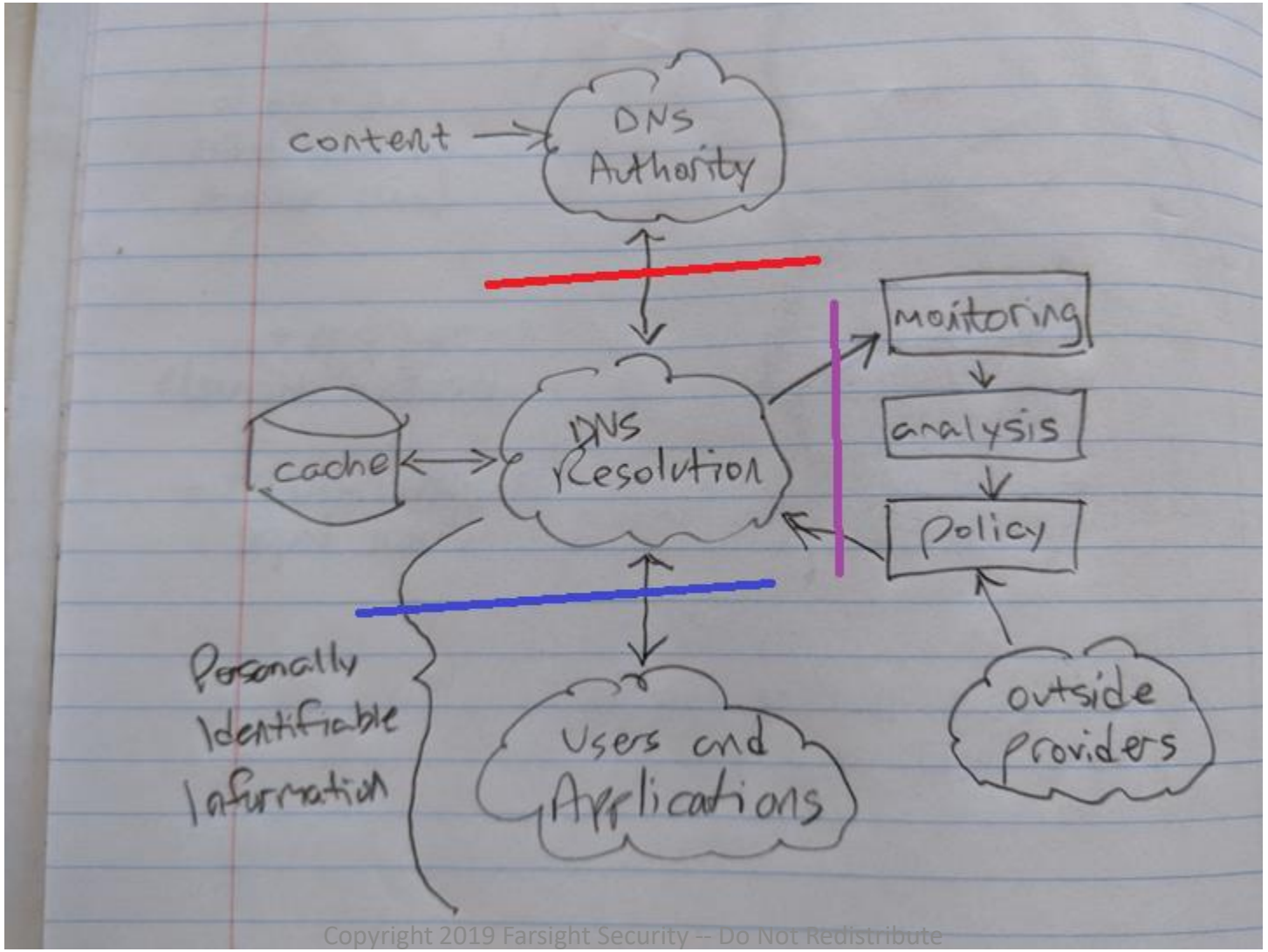
Internet System Topology, Extended



Enter Several Kinds of DNS Privacy

- RDNS path surveillance and intermediation was widely abused
  - Thus, DNS Privacy technologies have come along every few years
- Then there was DNS Over TLS (DoT), which is being deployed now
  - This is a new transport for any/all DNS transactions, above or below RDNS
  - This is TCP/853, is better than TCP/53, and sometimes better than UDP/53
  - Network operators can forbid, but cannot surveil or intercept, DoT
- Finally there is DNS Over HTTPS (DoH), also being deployed now
  - This is a new transport for stub-to-RDNS, so, a lot like DNS Crypt
  - Since it uses TCP/443, a network operator will “think twice before blocking it”
  - DoH disintermediates parental controls at home, and company policy at work

DNS System Architecture, Extended



Problems with DoH, part 1

- It's a political project, not a technical one
  - Encrypting stub-to-RDNS but not subsequent flows adds no actual privacy
  - An eavesdropper can guess answers based on what happens afterward
  - Guessing the questions once you know the answers is trivial data science
- To stay out of jail in an authoritarian regime, you need a VPN
  - And once you have a VPN, what value would DoH add?
- Also note, many names are resolvable locally but not remotely
  - Most companies have their own internal-only TLD's like .CORP or .GOOG
- The web is not the whole Internet; browsers can launch helper apps
  - Helper apps will use the normal stub resolver, getting different DNS answers

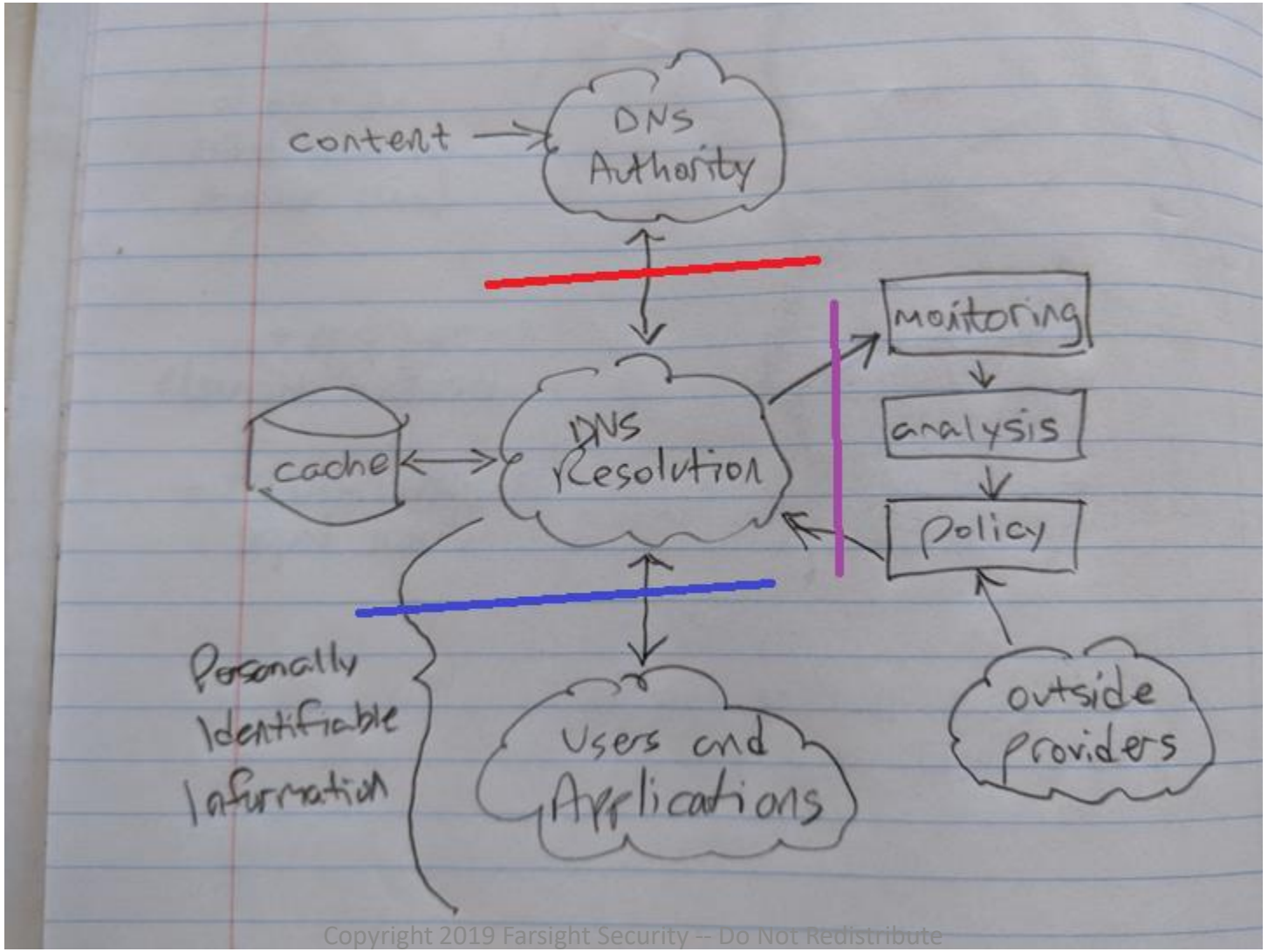
Problems with DoH, part 2

- DoH cannot differentiate between these network operators:
  - Parents, who use RDNS filtering as part of their family Internet controls
  - Sysadmins, who use RDNS filtering to block spam and malware
  - Security teams, who use RDNS monitoring to detect new malware infections
  - Authoritarian government, who uses RDNS for “thought control”
- It’s going to become broadly necessary to control TCP/443 (HTTPS):
  - Service networks will proxy or whitelist known-safe external API servers
  - Access networks will add HTTPS MITM, or simply require SOCKS for outbound
  - Any CDN IP who offers DoH will have to be blacklisted, because of malware
  - This increases complexity, cost, and vulnerability for almost every network

Inevitability of DoH

- The Web community has embraced DoH
  - Browsers and mobile OS will support it (“DNS Privacy?”)
  - DoT, by offering privacy but also cooperation, does not excite
- The rest of us can either embrace, or retire
  - Servers we run (Host, Lan, Campus, ISP) must support DoH
  - This capability must be well-advertised to our user communities
- DoH will be widely abused by non-cooperators
  - Intruders, bots, malware, teenagers, supply chain poisoners
  - Therefore a secure network must use SOCKS for outbound HTTPS
- This is the collective cost of long term abuse of RDNS position

DNS System Architecture, Extended



Conclusions

- RDNS need not be far away
  - (Host ≥ LAN ≥ Campus ≥ ISP ≥ ASP)
- RDNS is not expensive or complicated
  - Unbound, BIND, Knot, PowerDNS, PiHole
- RDNS is extremely sensitive
  - Contains PII (user + intent)
  - Deserves its own firewall
  - Requires contracted operator
- Port-based firewalls are powerless against DoH
  - Therefore, expect to proxy all outbound HTTPS