horizon
DIGITAL ECONOMY RESEARCH

Lessons from home

Derek McAuley

January 2019

The University of Nottingham

Research Councils UK Digital Economy Transforming Business and Society

Horizon and Personal Data

Data about us:

- Digital footprint, inferences

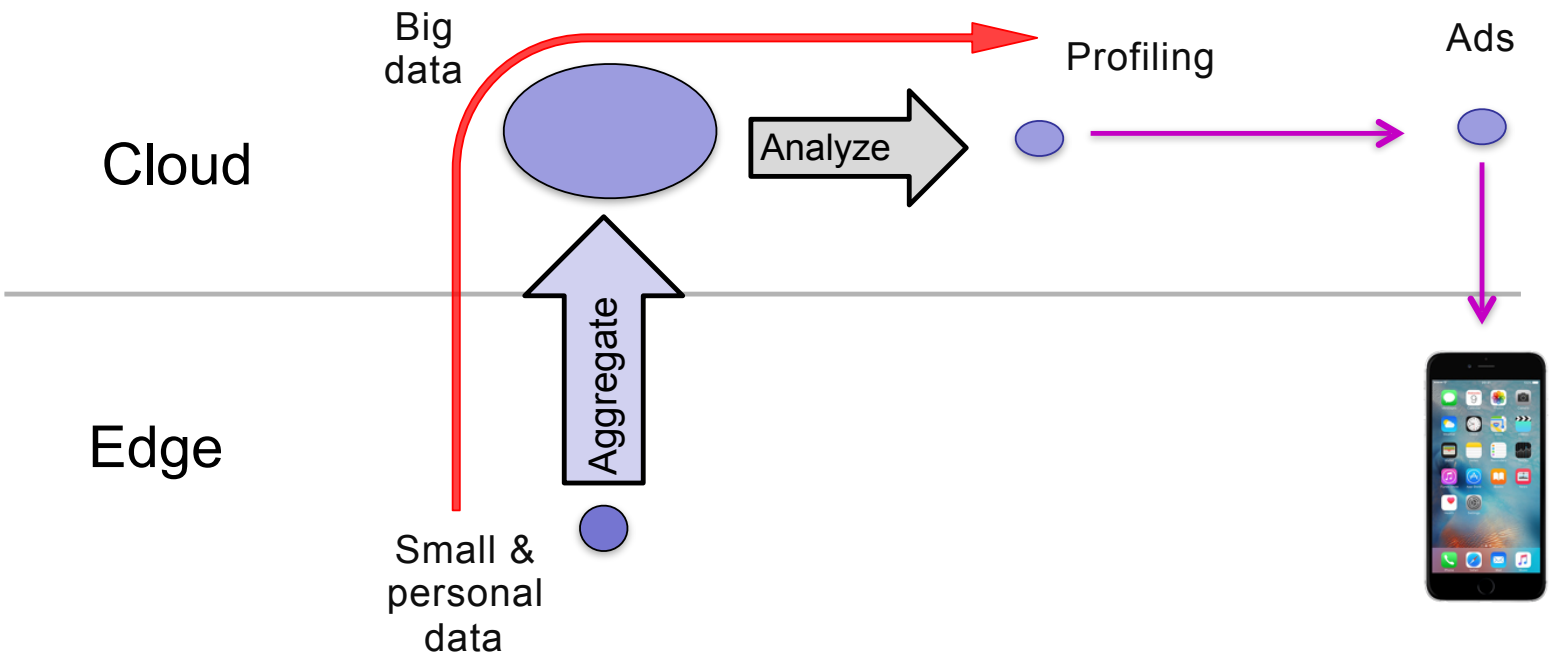
Data generated by us:

- Social media, wearables, smartphones

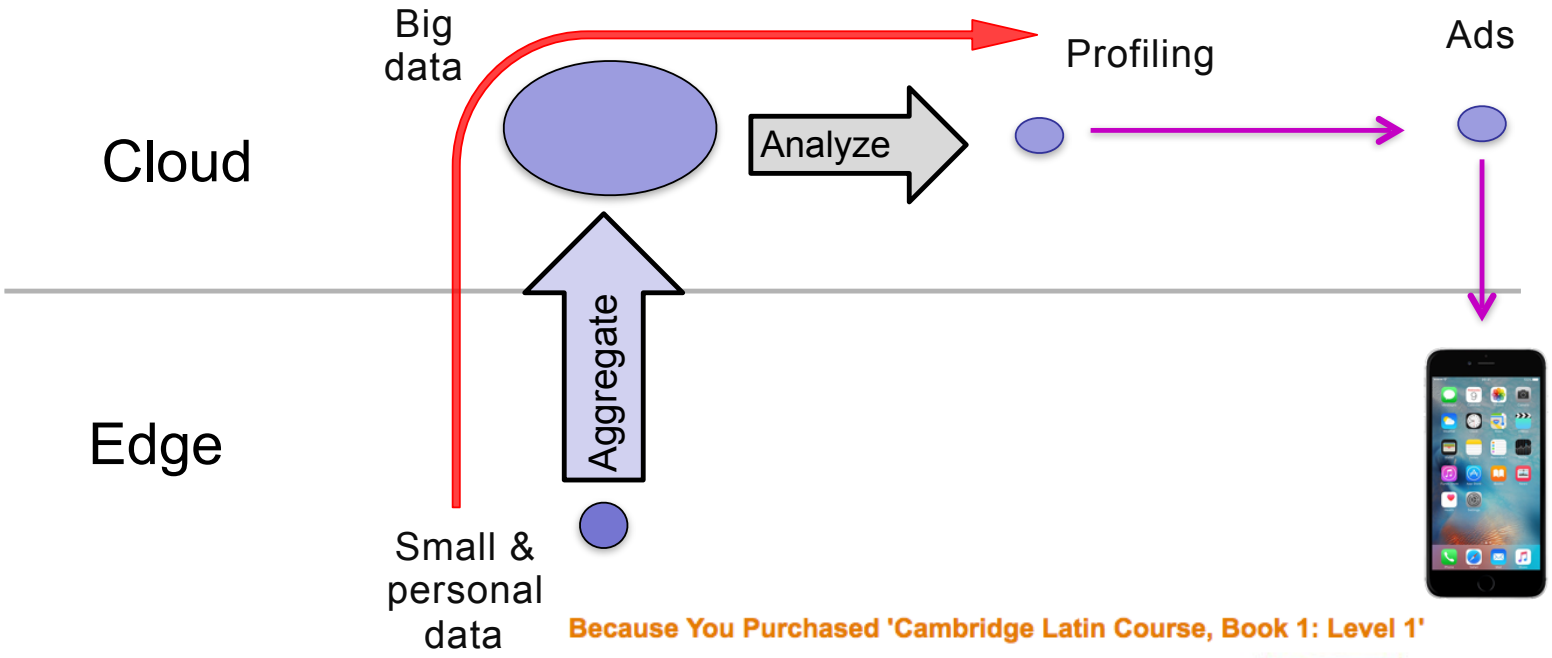
Data around us:

- IoT devices, EHRs

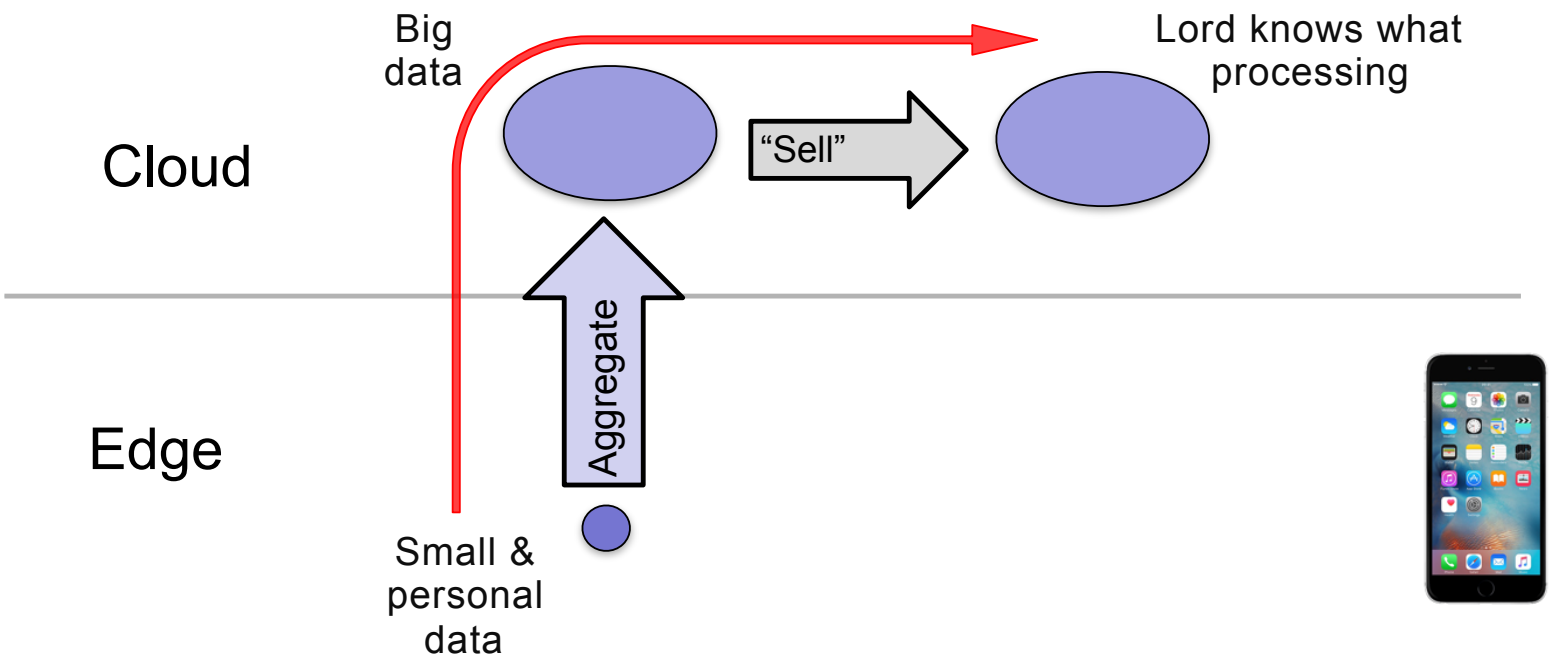
Advertising data



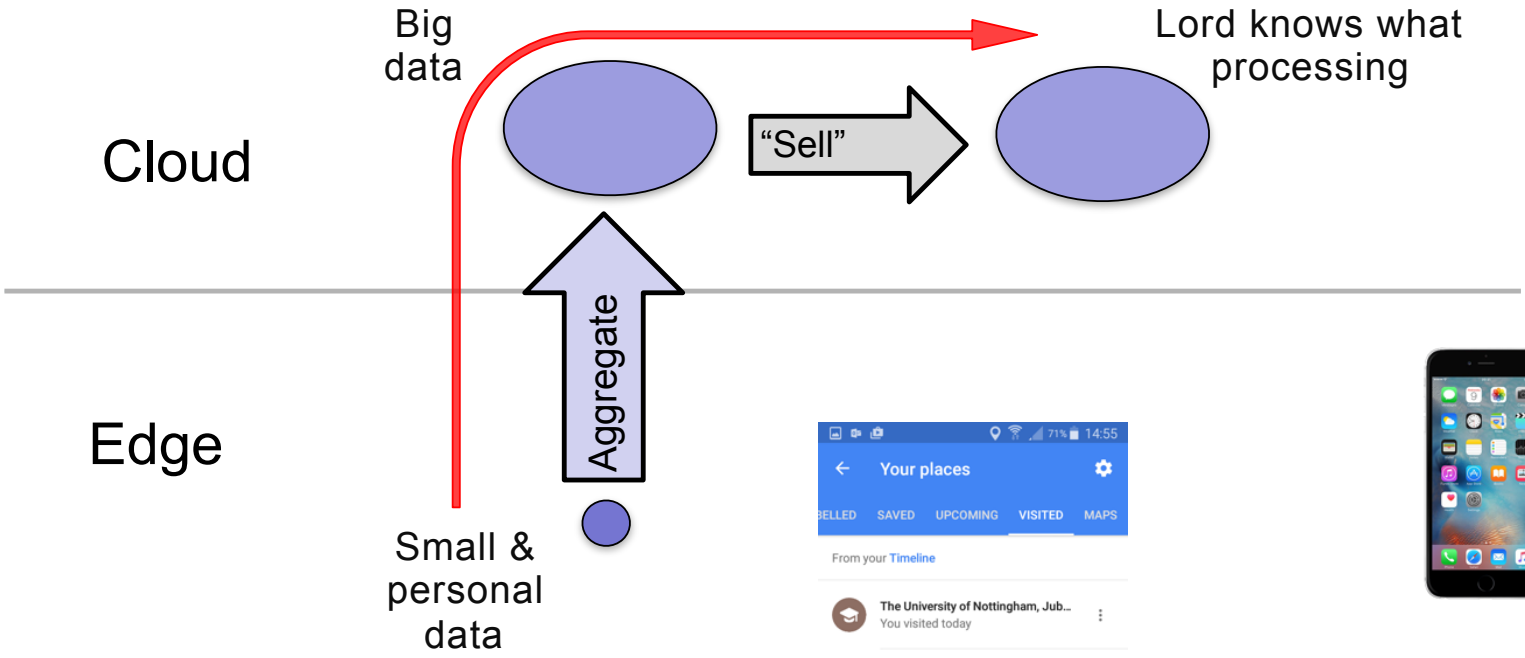
Advertising data

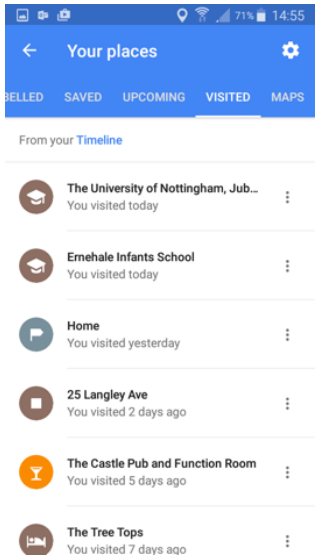


Data reuse by license

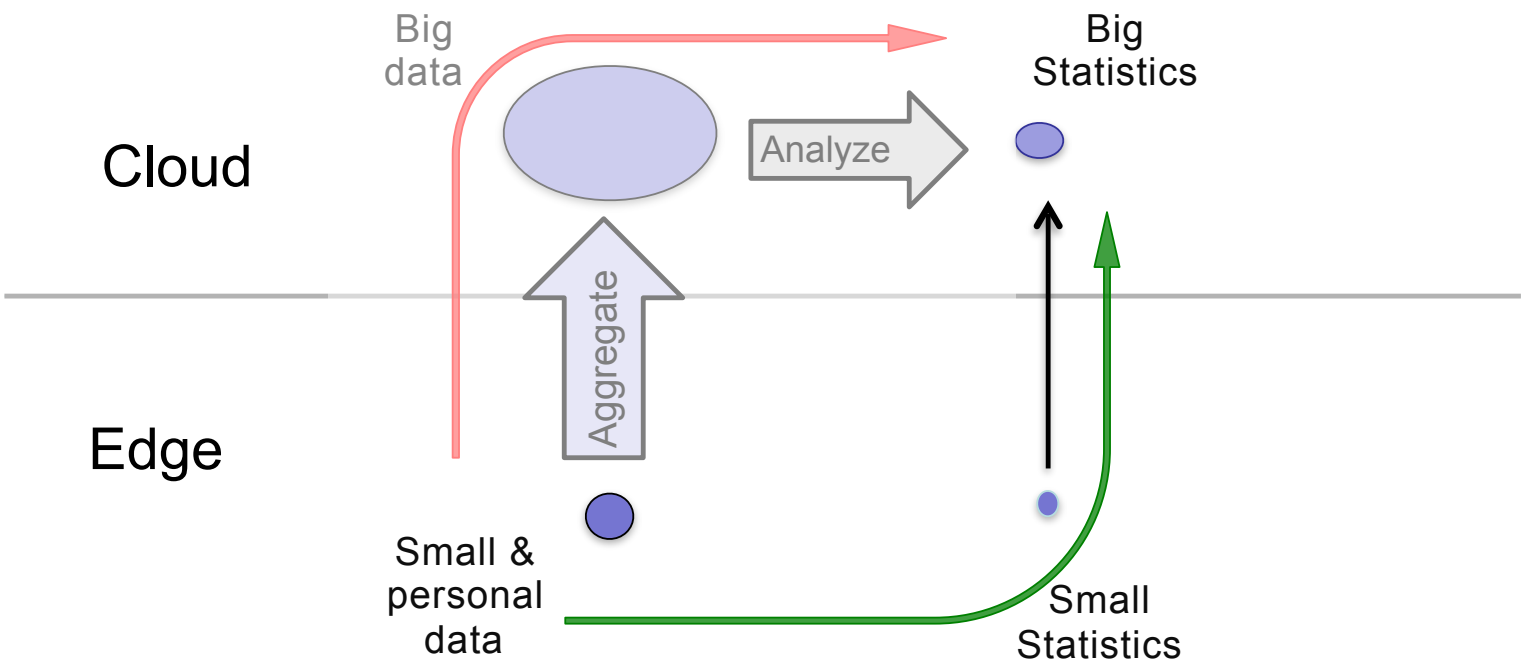


Data reuse by license





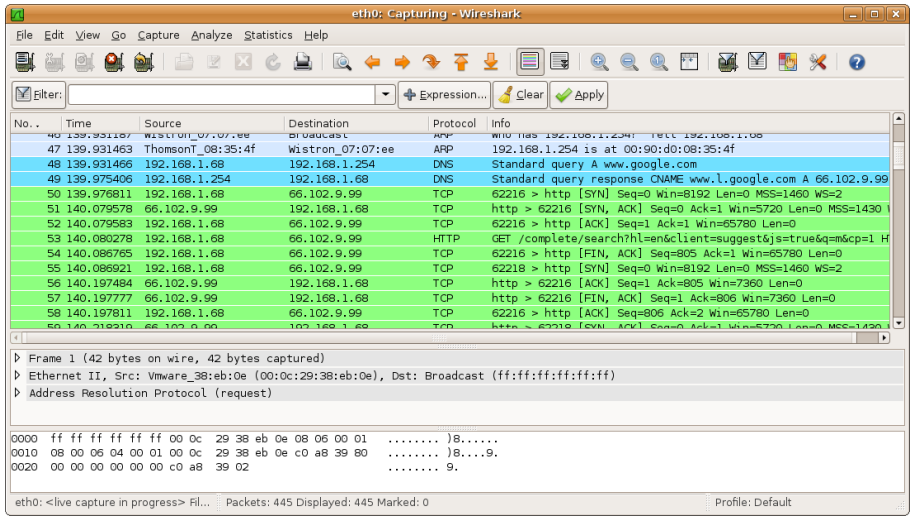
The way of small data



Minimal Sufficient Statistics

Defence Against the Dark Artefacts

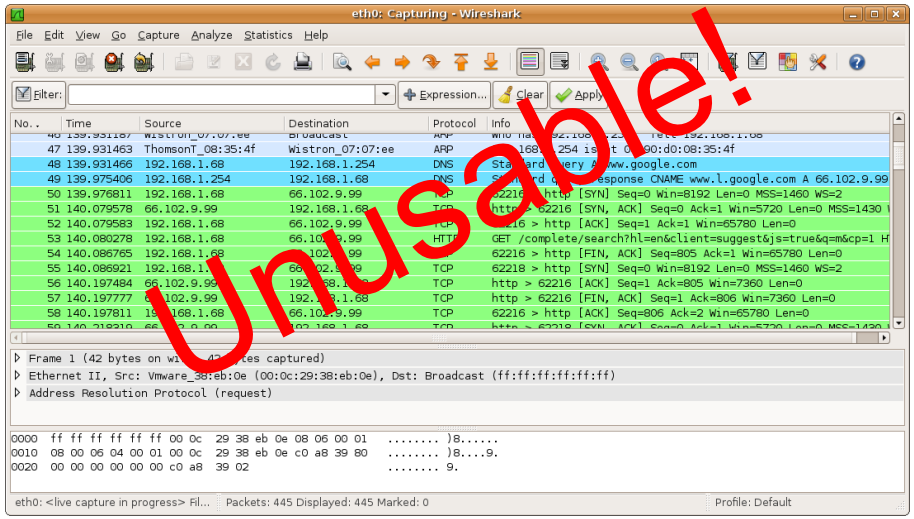
- Network enforcement by traffic control
- Usable by domestic customers
- IoT devices profiled using distributed machine learning
  - *Hamed's talk coming up!*
- Shared profile service



KEEP
CALM
AND
DISARM
THEM

Defence Against the Dark Artefacts

- Network enforcement by traffic control
- Usable by domestic customers
- IoT devices profiled using distributed machine learning
  - *Hamed's talk coming up!*
- Shared profile service



KEEP
CALM
AND
DISARM
THEM

Traffic control history test

An experimental general topology local area network based on [redacted] is described. This network is intended to be used to support multiservice traffic. Thus provision of guarantees of quality of service to various traffic types is an important feature of the network. In order to carry on quality of service experiments, one must have both a network which is inherently manageable, and the flexibility to provide different management strategies.

Traffic control history test

An experimental general topology local area network based on Asynchronous Transfer Mode (ATM) is described. This network is intended to be used to support multiservice traffic. Thus provision of guarantees of quality of service to various traffic types is an important feature of the network. In order to carry on quality of service experiments, one must have both a network which is inherently manageable, and the flexibility to provide different management strategies.

"Fairisle: An ATM network for the local area"
I Leslie, D McAuley
ACM SIGCOMM Computer Communication Review, 1991

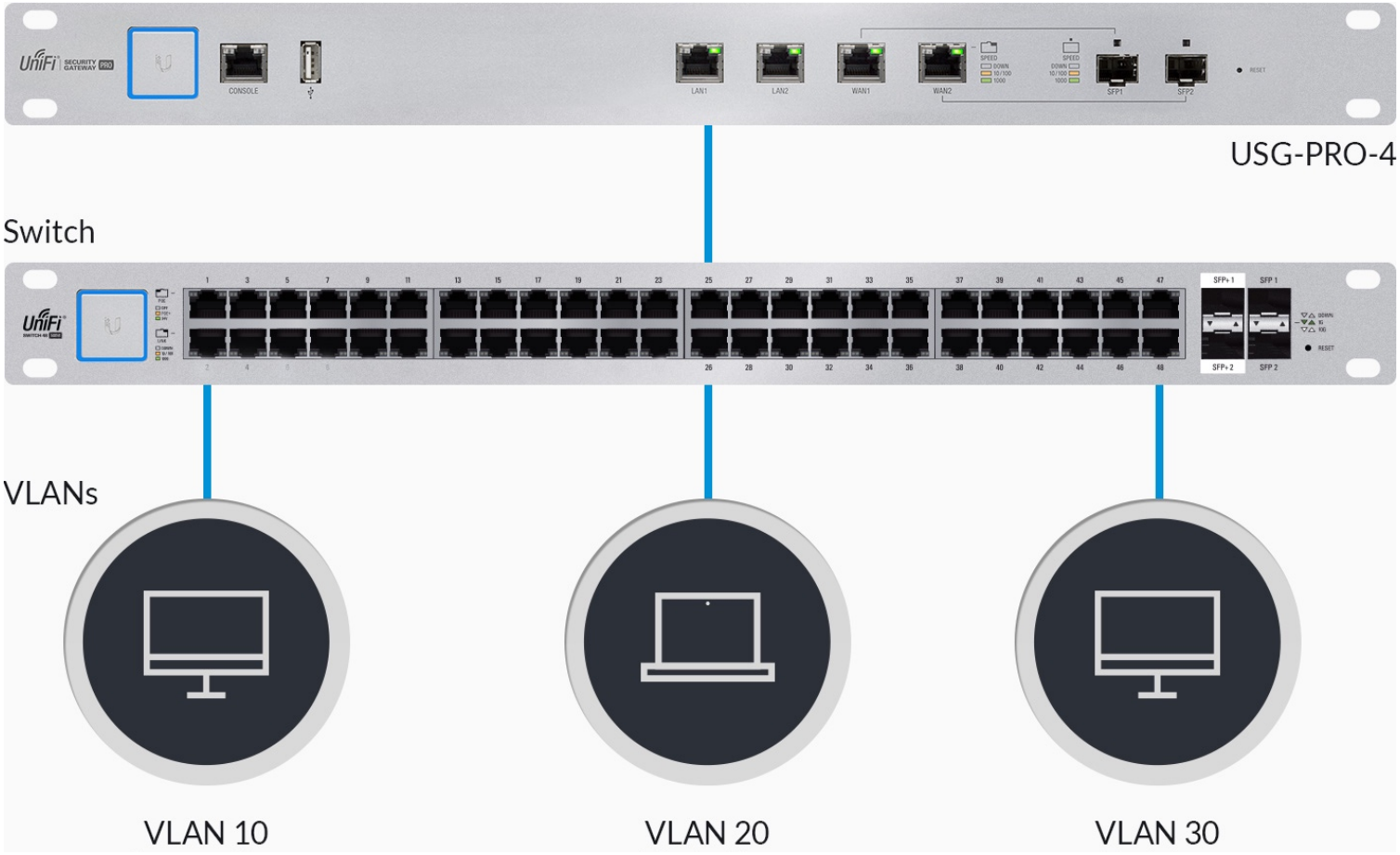
Traffic control history test

An experimental general topology local area network based on Asynchronous Transfer Mode (ATM) is described. This network is intended to be used to support multiservice traffic. Thus provision of guarantees of quality of service to various traffic types is an important feature of the network. In order to carry on quality of service experiments, one must have both a network which is inherently manageable, and the flexibility to provide different management strategies.

"Fairisle: An ATM network for the local area"
I Leslie, D McAuley
ACM SIGCOMM Computer Communication Review, 1991

A topic beaten to death for over 25 years… but…

....but


USG-PRO-4
Switch
VLANs
VLAN 10
Secure
VLAN 20
IoT / LoT
VLAN 30
Kid's Friends

IoT traffic

- MAC address tags all IoT traffic
- Not a general purpose computer work load
- Classification simplified
- Protection in depth - edge network equipment function

- But I have only one…

Experiment in Progress
Please Don't Touch :)

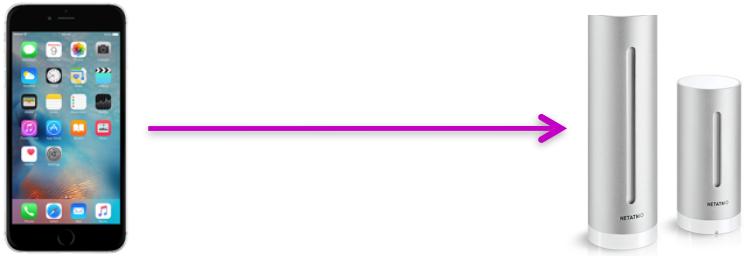
End-to-End design

END-TO-END ARGUMENTS IN SYSTEM DESIGN

J.H. Saltzer, D.P. Reed and D.D. Clark*

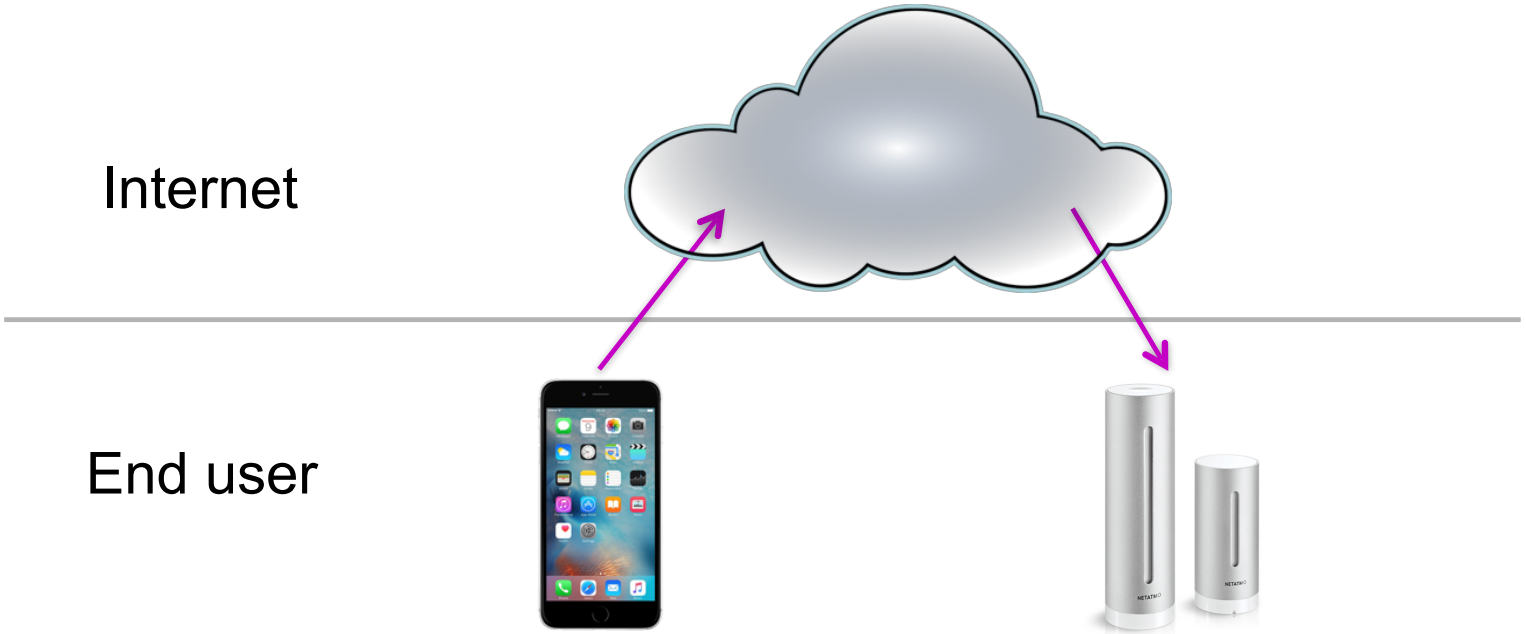
M.I.T. Laboratory for Computer Science

This paper presents a design principle that helps guide placement of functions among the modules of a distributed computer system. The principle, called the end-to-end argument, suggests that functions placed at low levels of a system may be redundant or of little value when compared with the cost of providing them at that low level. Examples discussed in the paper include bit error recovery, security using encryption, duplicate message suppression, recovery from system crashes, and delivery acknowledgement. Low level mechanisms to support these functions are justified only as performance enhancements.



Saltzer, J. H., D. P. Reed, and D. D. Clark (1981) "End-to-End Arguments in System Design". In: Proceedings of the Second International Conference on Distributed Computing Systems. Paris, France. April 8–10, 1981. IEEE Computer Society, pp. 509-512.

End-to-end in the Internet



End-to-end in the Internet

Internet

End user

End-to-end in the Internet

Beyond hope

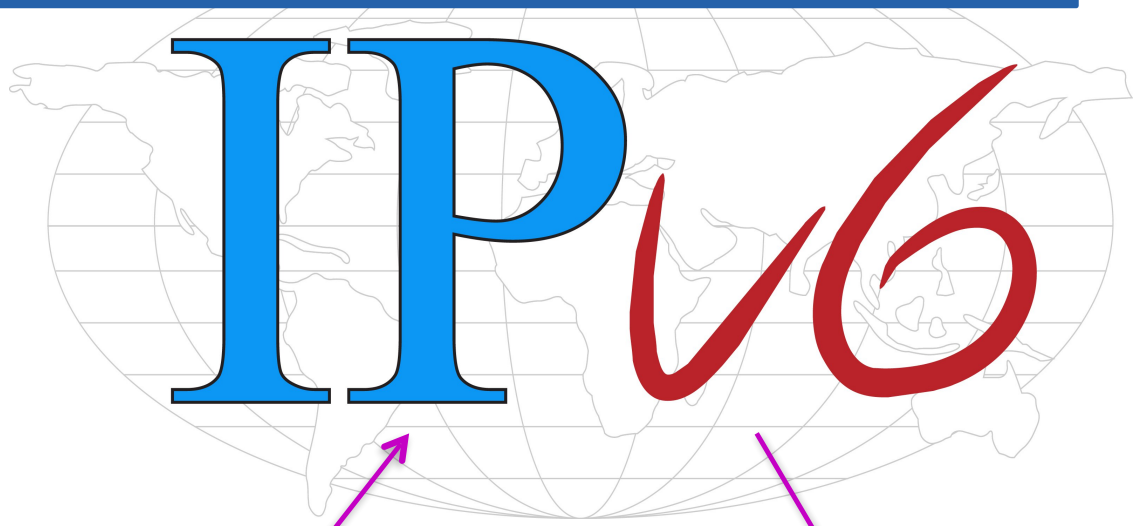
Hard work

Internet

X

End user

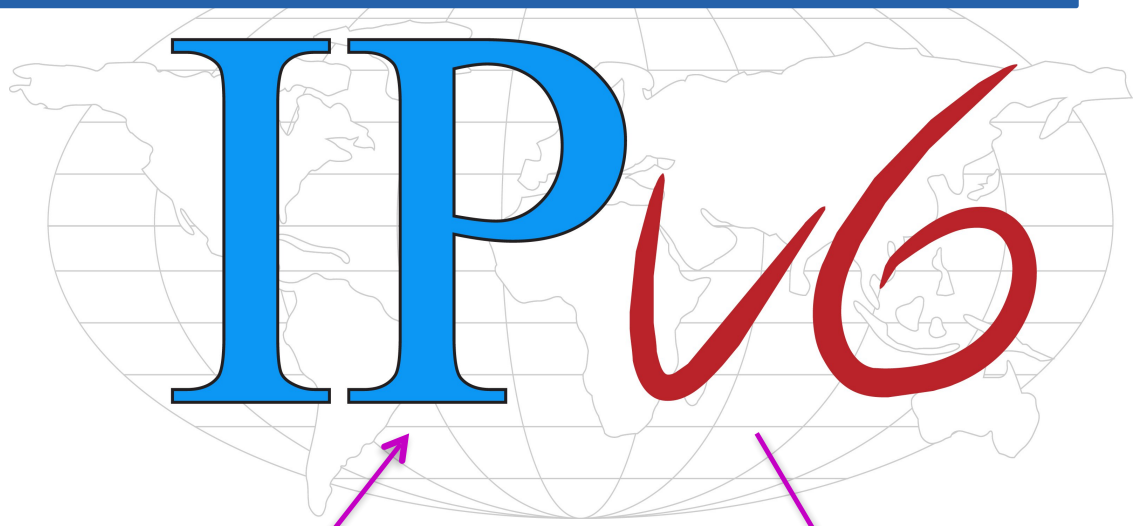
If only…



Internet

End user

If only…

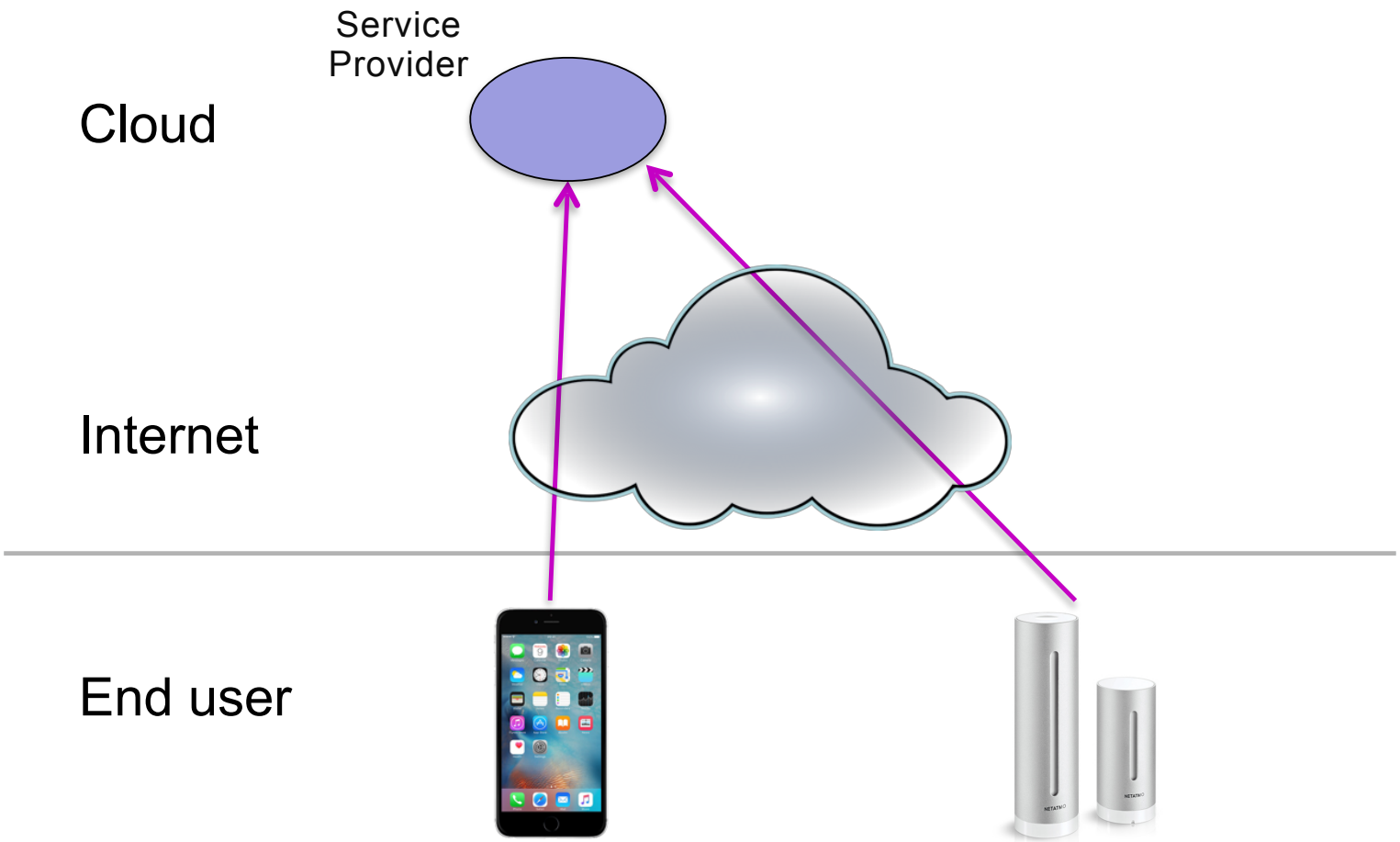


Internet

End user

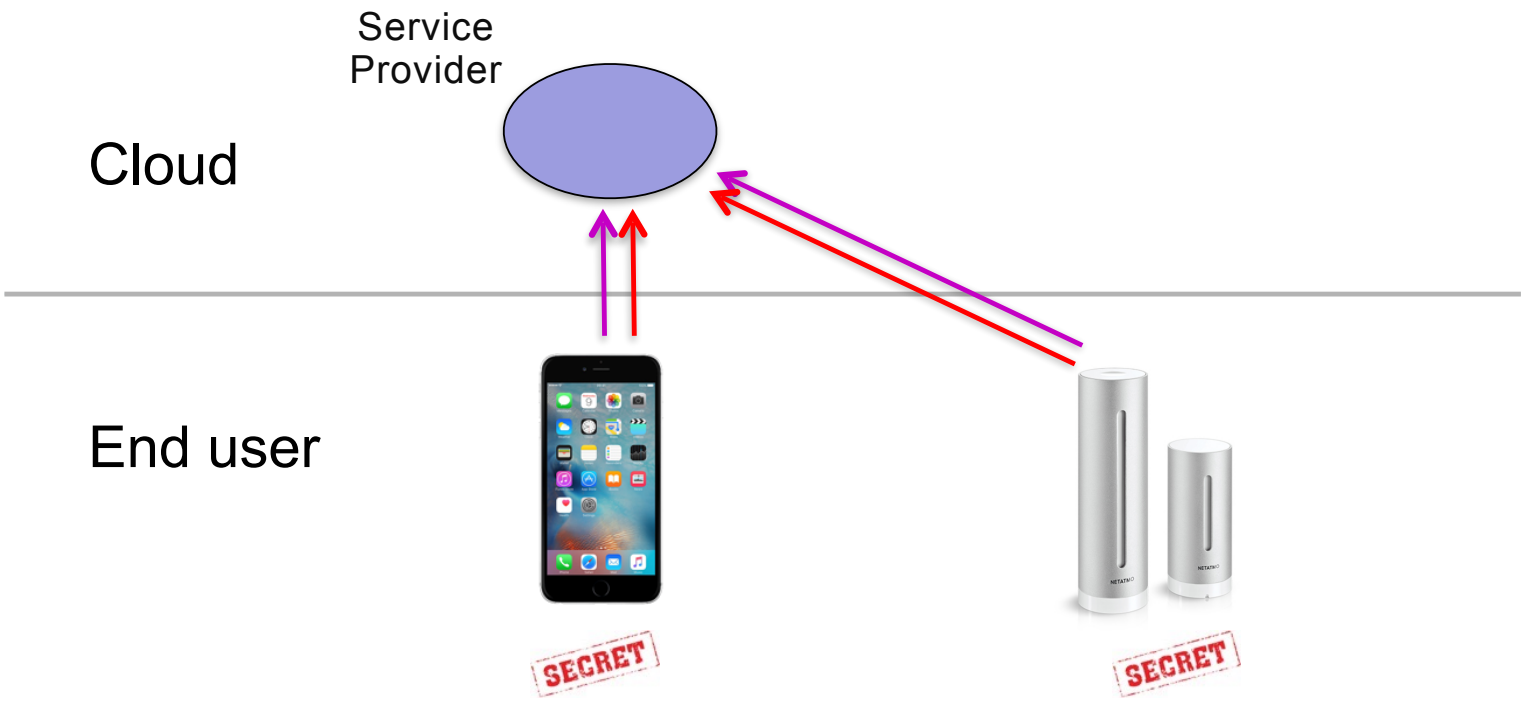
Need easy to use IPv6 VPN

End-to-end failure



The temptation of (fools) gold

End-to-End encryption



SIGNAL
Most Secure Messaging App

WhatsApp

. . .

Devices - qualitative observations

- Covert channels:
  - Built in DNS servers (in China)
  - Built in NTP servers (.ru .az .cn)
- Cloud services
  - Polling every second to the cloud service per device
  - Reverse connection from cloud to device every 236s
  - Random AWS service name
  - Connection to cloud even when in “local only” mode
  - Mobile to device always via Cloud
- Chained XOR “encryption”
- ”Motion detection” is image change detection
  - That’ll be leaves rustling…

Devices - qualitative observations

- Covert channels:
  - Built in DNS servers (in China)
  - Built in NTP servers (.ru .az .cn)
- Cloud services
  - Polling every second to the cloud service per device
  - Reverse connection from cloud to device every 236s
  - Random AWS service name
  - Connection to cloud even when in “local only” mode
  - Mobile to device always via Cloud
- Chained XOR “encryption”
- ”Motion detection” is image change detection
  - That’ll be leaves rustling…

Sometimes DADA will just say no

Summary

- Databox approaches
  - Privacy preserving analytics
- DADA
  - All IoT devices are considered potential threats
  - Complex profiling and “correct“ profile enforcement

Read @internetofshit

https://www.horizon.ac.uk

Questions?

derek.mcauley@nottingham.ac.uk
@drdrmc

The University of Nottingham

Research Councils UK Digital Economy Transforming Business and Society

horizon DIGITAL ECONOMY RESEARCH

Abstract

The presentation will draw lessons from the DADA (Defence Against the Dark Artefacts) project that seeks to understand how to make use of the key technologies used in securing enterprise networks, such as traffic isolation, monitoring and shaping, and bring them to bear at low cost and in easy to use ways for IoT. DADA focusses on the home and small enterprise, where there is no cadre of network cybersecurity experts to deploy and run the systems, and presumes that most IoT devices will eventually become liabilities due to lack of software upgrades (never mind that some of them will be compromised on delivery), so that the network itself may often need to take on the responsibility of managing them off the network… These sorts of deployment issues will also be prevalent as we move to use of low cost systems in remote sensing, with the additional complexity that attackers may have easy physical access to sensors.