Governance of (and by) FL

Jon Crowcroft

24/10/2025

Federated Digital Systems over 50 years…

- E-Mail
- DNS
- BGP
- Social Media

- Now Machine Learning…in the form of Federated Learning

Why Federated/Decentralized (now?)

- In the UK, in the last 6 months, centralized systems at
  - Tescos, Coop, Airport checkin, Nursery Schools,
  - And Jaguar/Rover/Landrover
  - And others not so public…
- Bought to a standstill be ransomeware
- Decentralized/Federated systems might be less vulnerable

Added

- E-Mail – DMARC, DKIM
- DNS – CA, CT
- BGP – Route Registries
- Social Media – Id/attribute verification

- Now Machine Learning…in the form of Federated Learning

Coordination

- Without central agency?
  - Both easier…
    - …and harder
  - Without a centralized agency
    - Trust models….

Defence against the Dark - Challenges

- Distributed
  - Consensus – learn clusters of similar policy
  - Reputation – distributed ledgers?
  - What does the adversary look like in practice?
- Policy structures
  - Customer/provider v. peer-peer (as in BGP)
  - Other more unstructured (as in BlueSky moderation)
  - New?

Whither AI in Federated Policy?

- Can we learn model of federated trust?
- Can we learn in a decentrazed way?
  - Multi-agent systems?
  - Do LLMs help? (note can be decentralized themselves)

Challenges

- Complex Systems…
- …emergence
- Decentralization tendency…
- ….to recentralize

Q&A