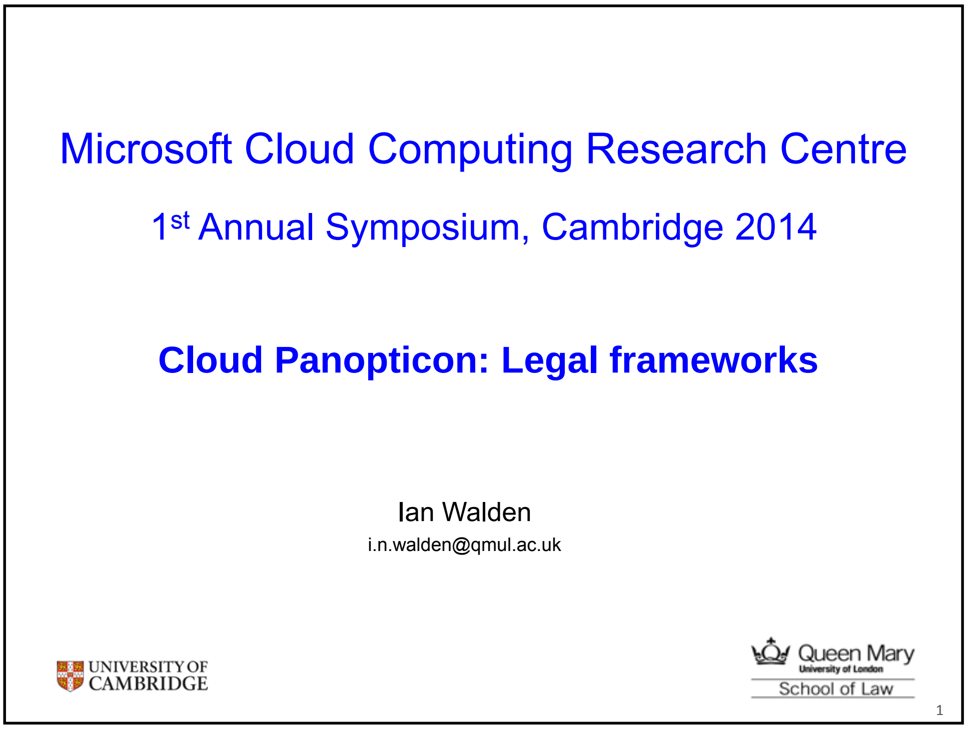


Microsoft Cloud Computing Research Centre

1st Annual Symposium, Cambridge 2014

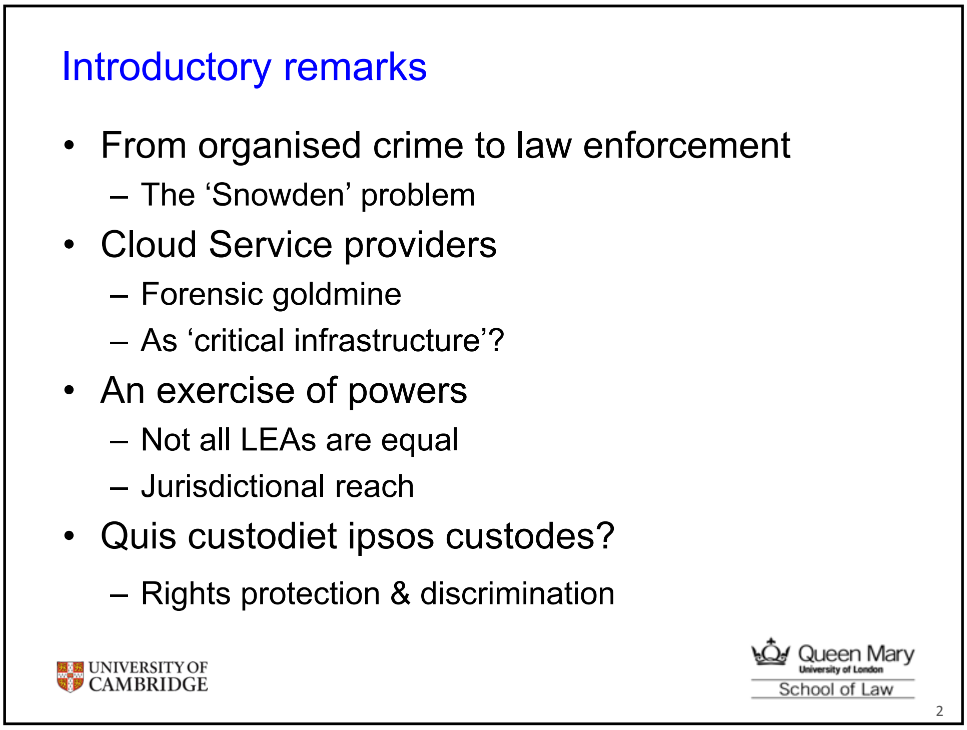
Cloud Panopticon: Legal frameworks

Ian Walden
i.n.walden@qmul.ac.uk

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London School of Law

1



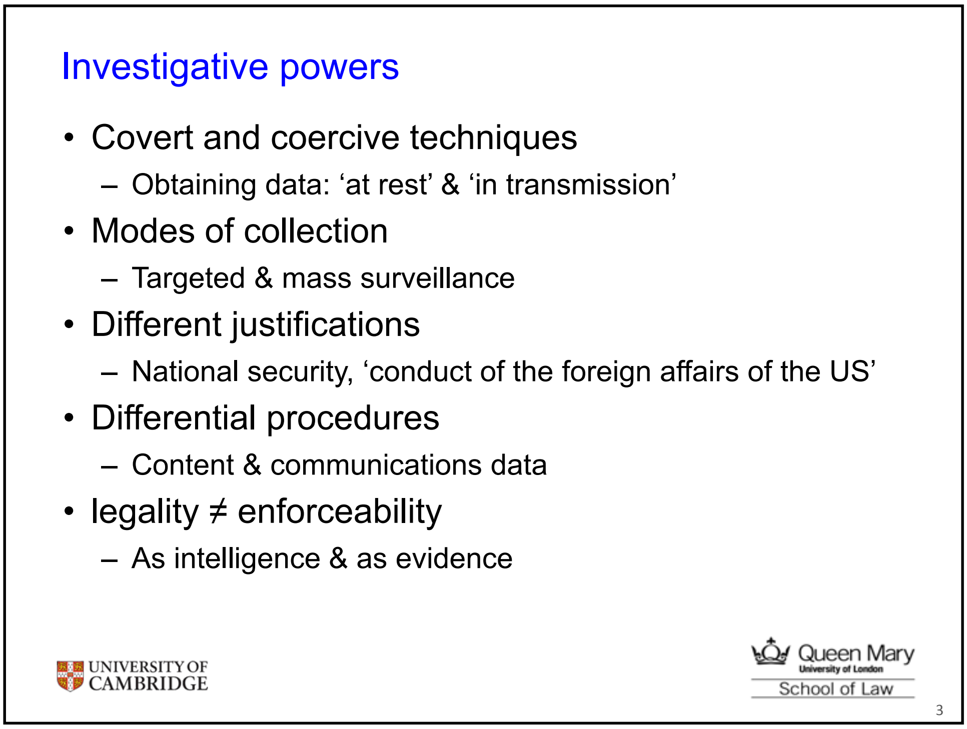
Introductory remarks

- From organised crime to law enforcement
  - The ‘Snowden’ problem
- Cloud Service providers
  - Forensic goldmine
  - As ‘critical infrastructure’?
- An exercise of powers
  - Not all LEAs are equal
  - Jurisdictional reach
- Quis custodiet ipsos custodes?
  - Rights protection & discrimination

UNIVERSITY OF CAMBRIDGE

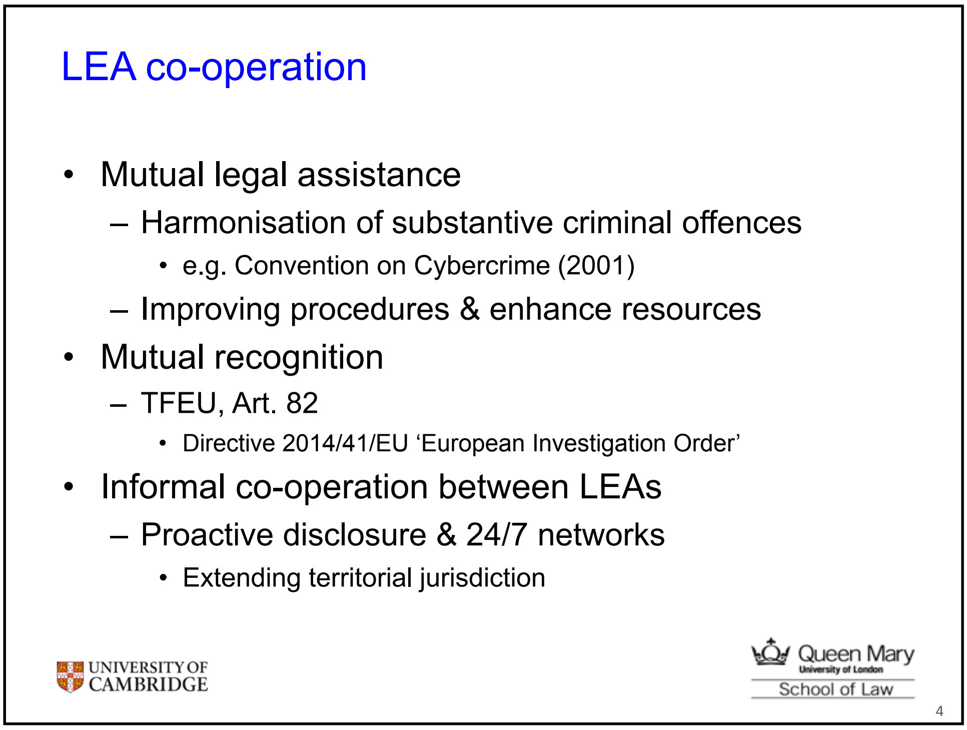
Queen Mary University of London School of Law

2



Investigative powers

- Covert and coercive techniques
  - Obtaining data: ‘at rest’ & ‘in transmission’
- Modes of collection
  - Targeted & mass surveillance
- Different justifications
  - National security, ‘conduct of the foreign affairs of the US’
- Differential procedures
  - Content & communications data
- legality ≠ enforceability
  - As intelligence & as evidence



LEA co-operation

- Mutual legal assistance
  - Harmonisation of substantive criminal offences
    - e.g. Convention on Cybercrime (2001)
  - Improving procedures & enhance resources
- Mutual recognition
  - TFEU, Art. 82
    - Directive 2014/41/EU ‘European Investigation Order’
- Informal co-operation between LEAs
  - Proactive disclosure & 24/7 networks
    - Extending territorial jurisdiction

Dealing with law enforcement

- Obligations to assist
  - Capture data: ‘LI capability’
  - Retain data
  - Decrypt protected data
  - Disclose data
- Voluntary assistance
  - National
    - Immunity from liability
  - International
    - “obtains the lawful and voluntary consent of the person who has lawful authority to disclose the data..” (Cybercrime Convention, Art. 32b)

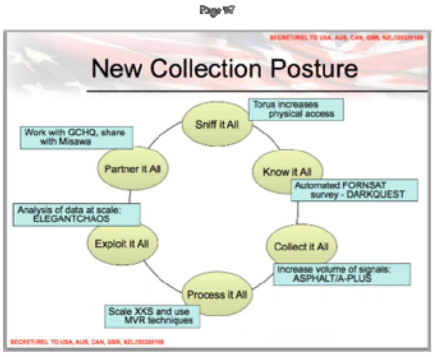
UNIVERSITY OF CAMBRIDGE

Queen Mary University of London School of Law

5

Not dealing with law enforcement

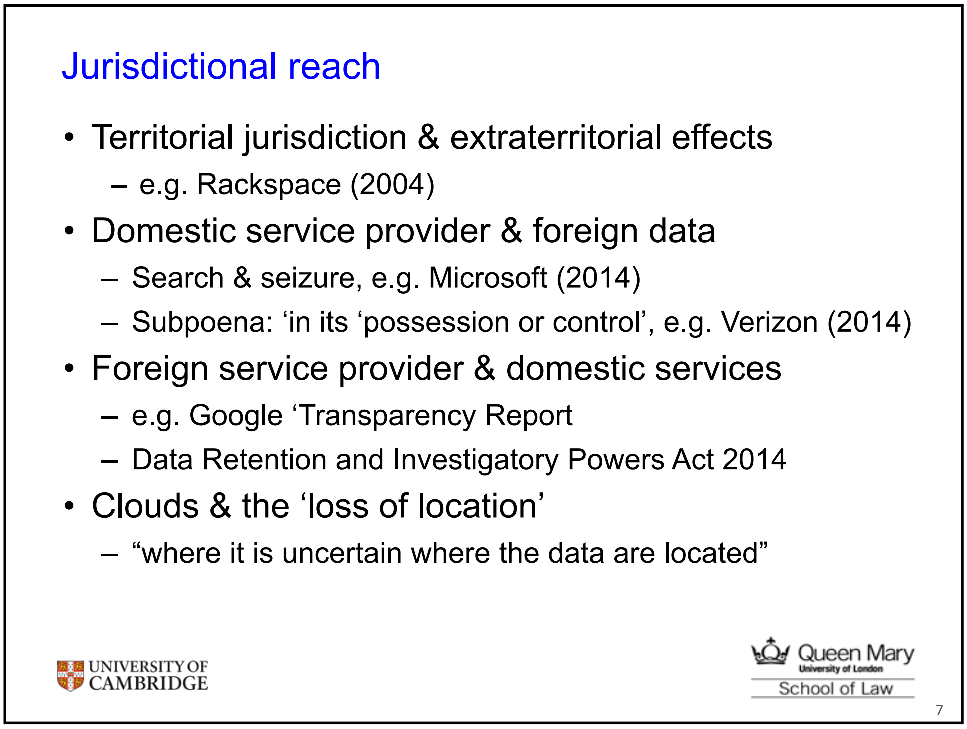
- Engage directly with the material sought
  - ‘Publicly available’
  - NSA’s ‘Tailored Access Operations’
- Unmediated access
  - Black boxes
- LEA Co-operation
  - ‘Five Eyes’


Page 97
SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108
New Collection Posture
Sniff it All
Torus increases physical access
Know it All
Automated FORNSAT survey - DARKQUEST
Collect it All
Increase volume of signals: ASPHALT/A-PLUS
Process it All
Scale XKS and use MVR techniques
Exploit it All
Analysis of data at scale: ELEGANTCHAOS
Partner it All
Work with GCHQ, share with Misawa
SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

UNIVERSITY OF CAMBRIDGE

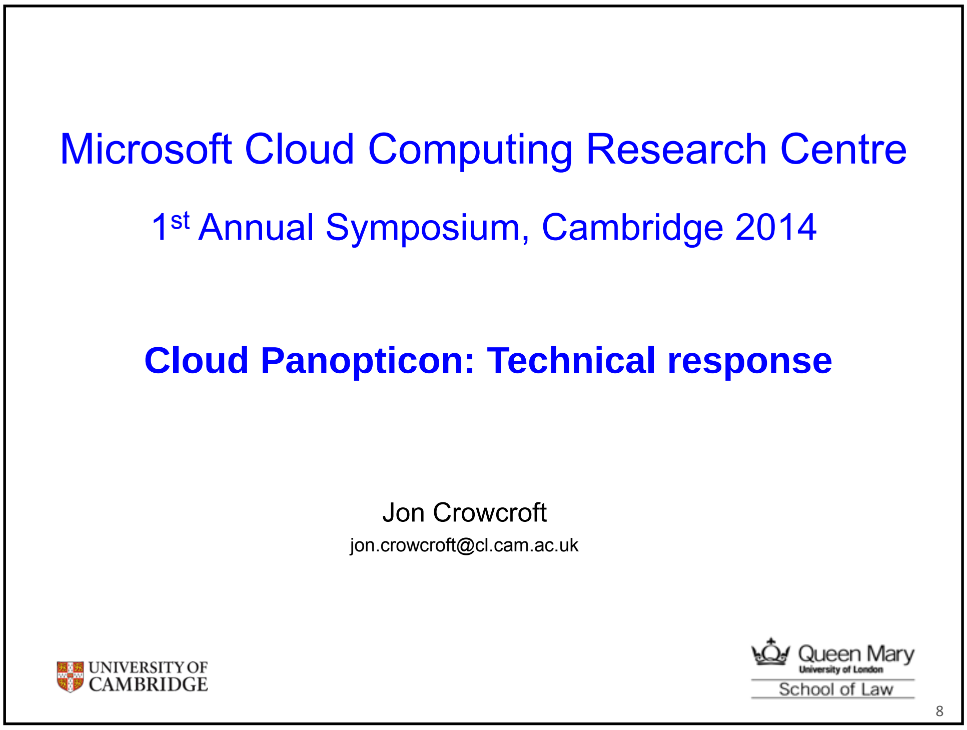
Queen Mary University of London School of Law

6



Jurisdictional reach

- Territorial jurisdiction & extraterritorial effects
  - e.g. Rackspace (2004)
- Domestic service provider & foreign data
  - Search & seizure, e.g. Microsoft (2014)
  - Subpoena: ‘in its ‘possession or control’, e.g. Verizon (2014)
- Foreign service provider & domestic services
  - e.g. Google ‘Transparency Report
  - Data Retention and Investigatory Powers Act 2014
- Clouds & the ‘loss of location’
  - “where it is uncertain where the data are located”

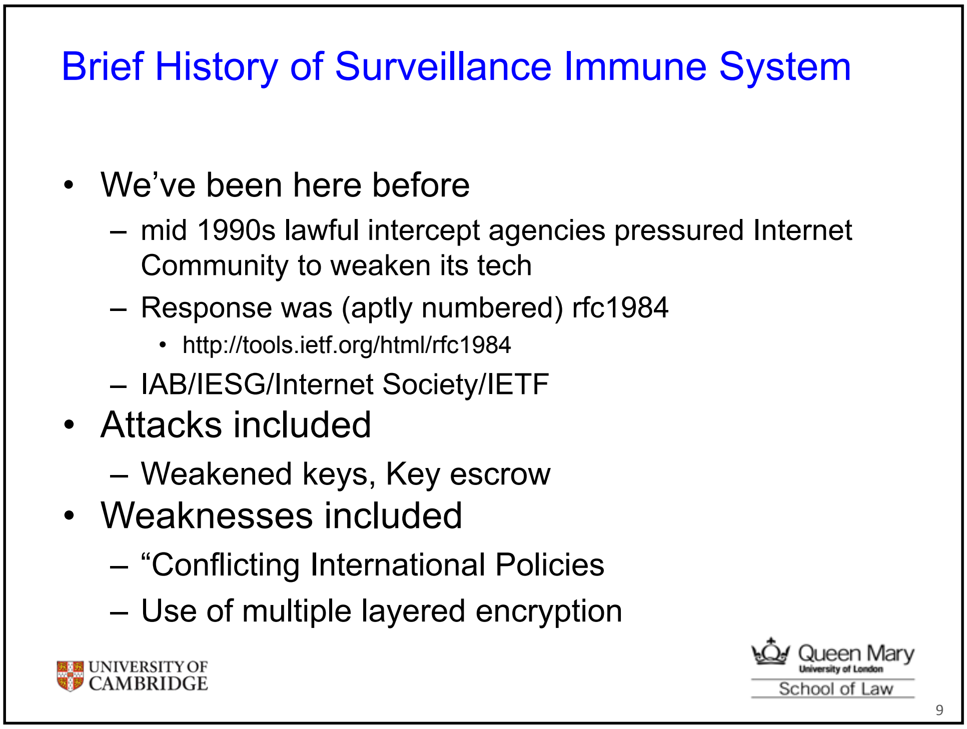


Microsoft Cloud Computing Research Centre

1st Annual Symposium, Cambridge 2014

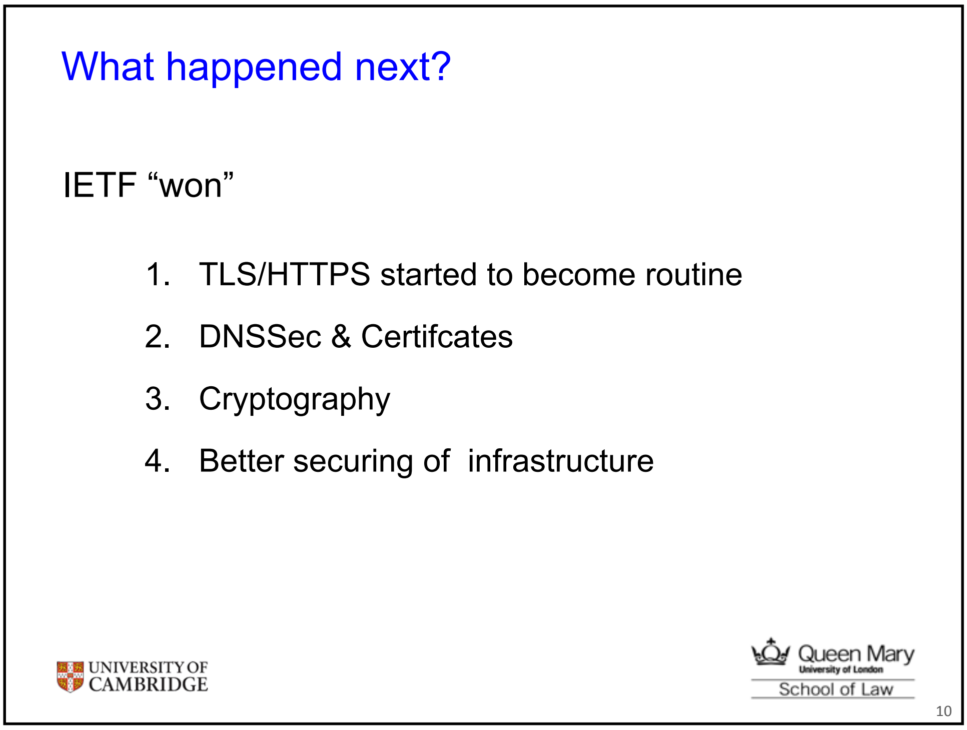
Cloud Panopticon: Technical response

Jon Crowcroft
jon.crowcroft@cl.cam.ac.uk



Brief History of Surveillance Immune System

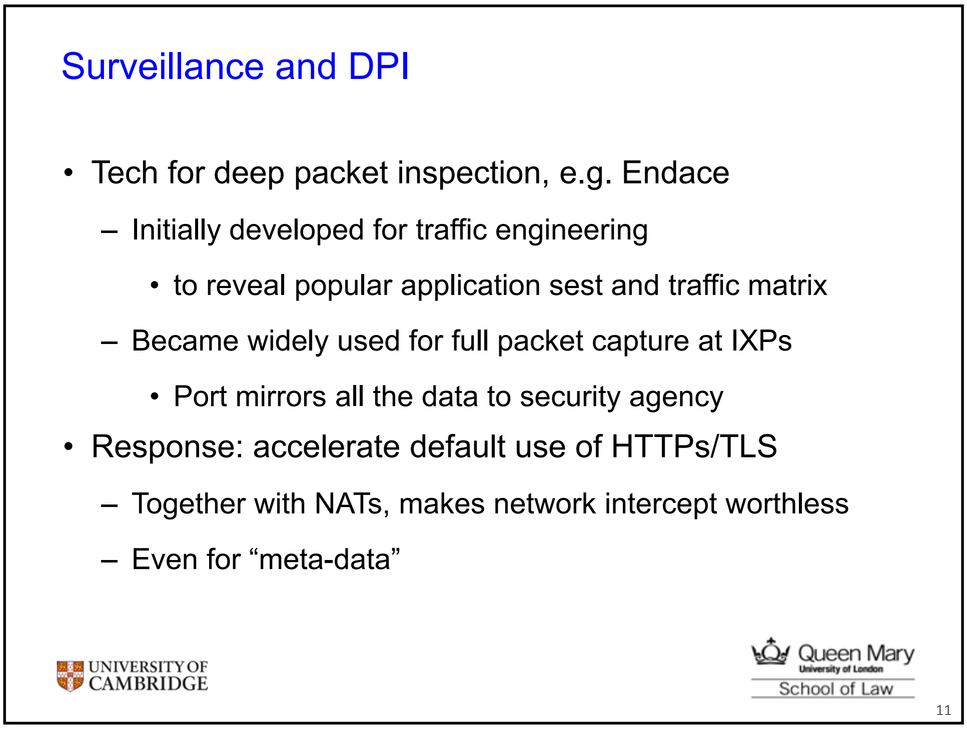
- We’ve been here before
  - mid 1990s lawful intercept agencies pressured Internet Community to weaken its tech
  - Response was (aptly numbered) rfc1984
    - http://tools.ietf.org/html/rfc1984
  - IAB/IESG/Internet Society/IETF
- Attacks included
  - Weakened keys, Key escrow
- Weaknesses included
  - “Conflicting International Policies
  - Use of multiple layered encryption



What happened next?

IETF “won”

1. TLS/HTTPS started to become routine
2. DNSSec & Certifcates
3. Cryptography
4. Better securing of infrastructure



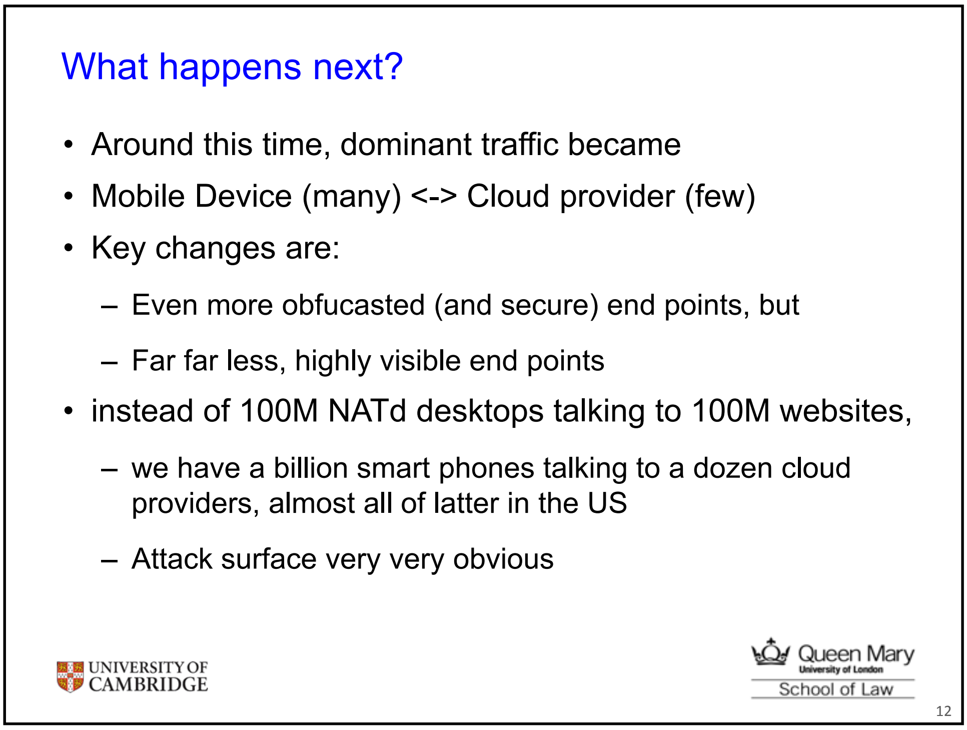
Surveillance and DPI

- Tech for deep packet inspection, e.g. Endace
  - Initially developed for traffic engineering
    - to reveal popular application sest and traffic matrix
  - Became widely used for full packet capture at IXPs
    - Port mirrors all the data to security agency
- Response: accelerate default use of HTTPs/TLS
  - Together with NATs, makes network intercept worthless
  - Even for “meta-data”

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London School of Law

11



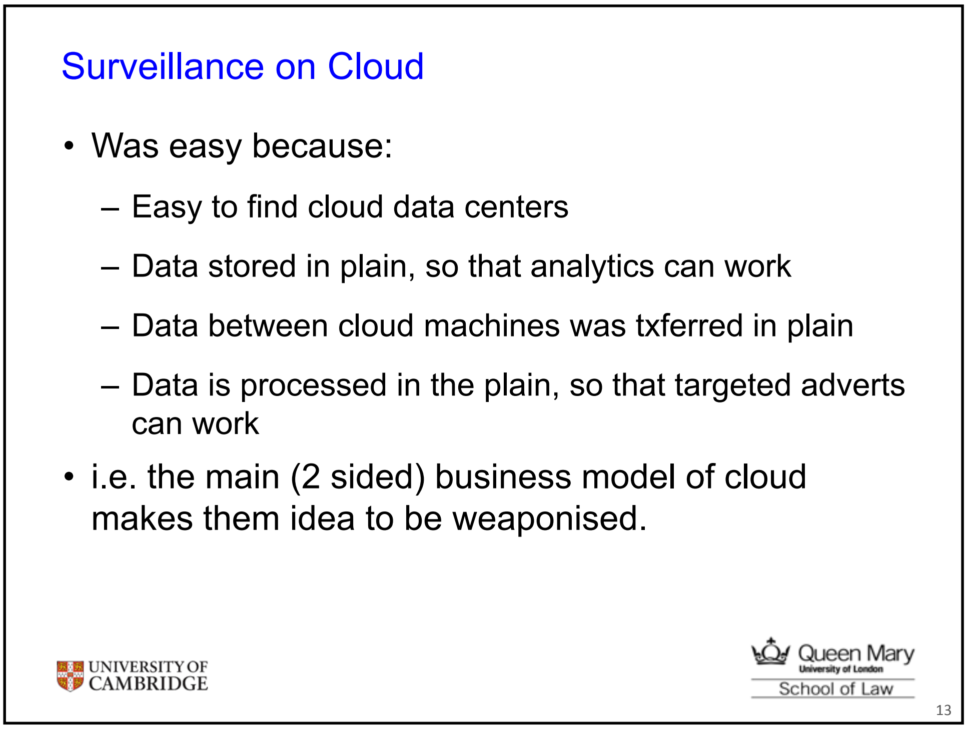
What happens next?

- Around this time, dominant traffic became
- Mobile Device (many) <-> Cloud provider (few)
- Key changes are:
  - Even more obfucasted (and secure) end points, but
  - Far far less, highly visible end points
- instead of 100M NATd desktops talking to 100M websites,
  - we have a billion smart phones talking to a dozen cloud providers, almost all of latter in the US
  - Attack surface very very obvious

UNIVERSITY OF CAMBRIDGE

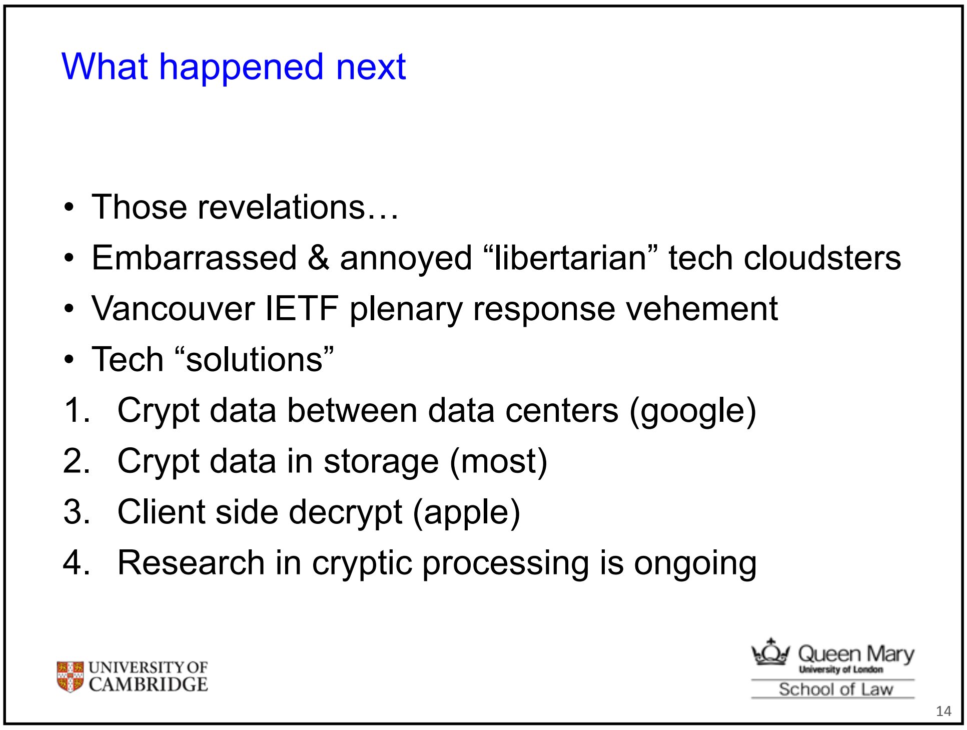
Queen Mary University of London School of Law

12



Surveillance on Cloud

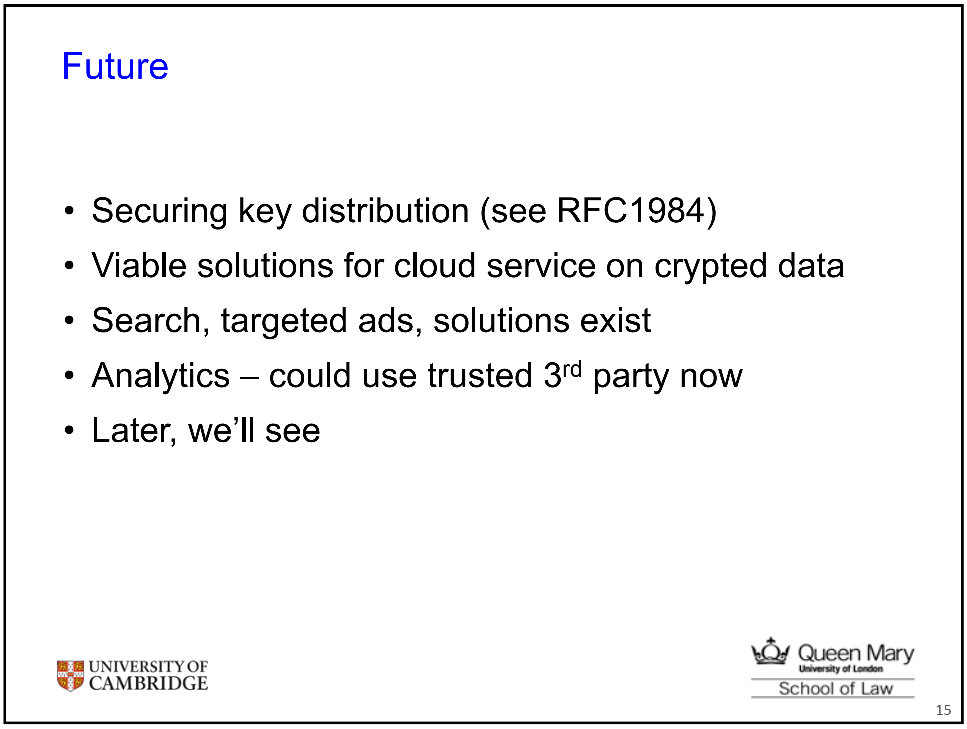
- Was easy because:
  - – Easy to find cloud data centers
  - – Data stored in plain, so that analytics can work
  - – Data between cloud machines was txferred in plain
  - – Data is processed in the plain, so that targeted adverts can work
- i.e. the main (2 sided) business model of cloud makes them idea to be weaponised.



What happened next

- Those revelations…
- Embarrassed & annoyed “libertarian” tech cloudsters
- Vancouver IETF plenary response vehement
- Tech “solutions”

1. Crypt data between data centers (google)
2. Crypt data in storage (most)
3. Client side decrypt (apple)
4. Research in cryptic processing is ongoing



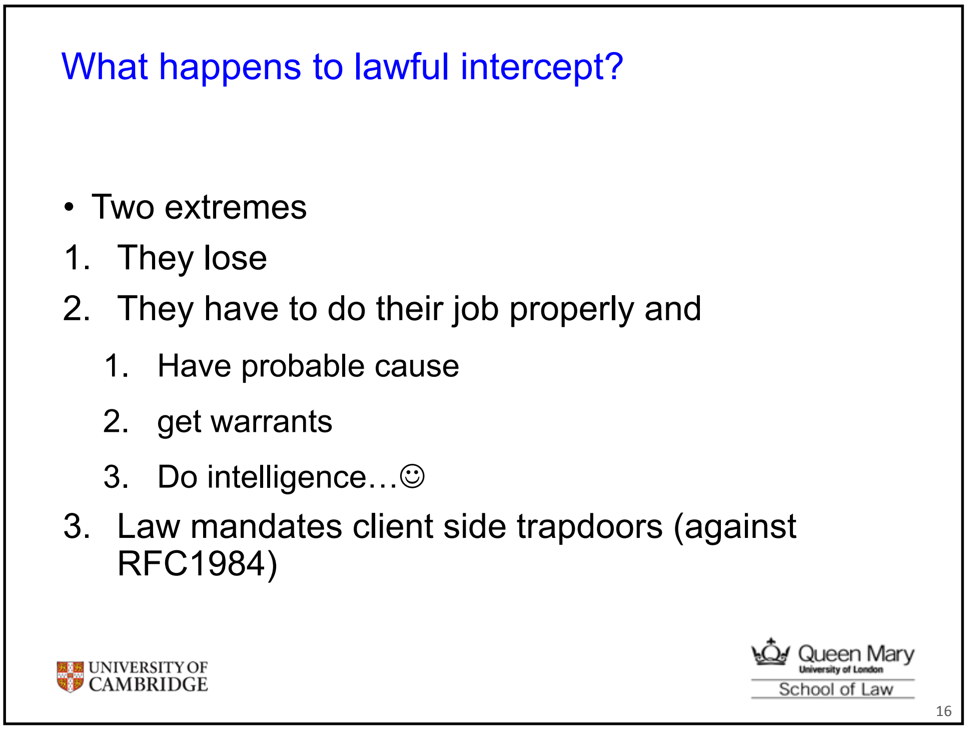
Future

- Securing key distribution (see RFC1984)
- Viable solutions for cloud service on crypted data
- Search, targeted ads, solutions exist
- Analytics – could use trusted 3rd party now
- Later, we'll see

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London School of Law

15



What happens to lawful intercept?

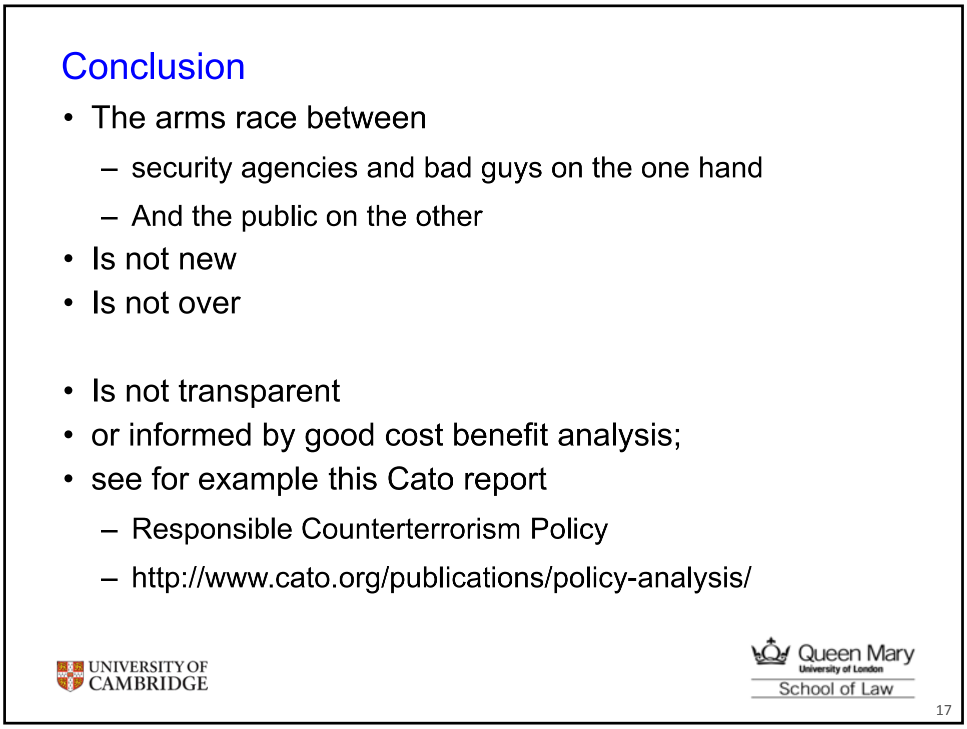
- Two extremes

1. They lose
2. They have to do their job properly and
   1. Have probable cause
   2. get warrants
   3. Do intelligence…☺
3. Law mandates client side trapdoors (against RFC1984)

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London School of Law

16



Conclusion

- The arms race between
  - security agencies and bad guys on the one hand
  - And the public on the other
- Is not new
- Is not over

- Is not transparent
- or informed by good cost benefit analysis;
- see for example this Cato report
  - Responsible Counterterrorism Policy
  - http://www.cato.org/publications/policy-analysis/

UNIVERSITY OF CAMBRIDGE
Queen Mary
University of London
School of Law
17