Privacy in the Internet: threats and challenges

Mohamed Hamdi

Elgazala technopark, Tunisia

December 5, 2016

Abundance of security controls

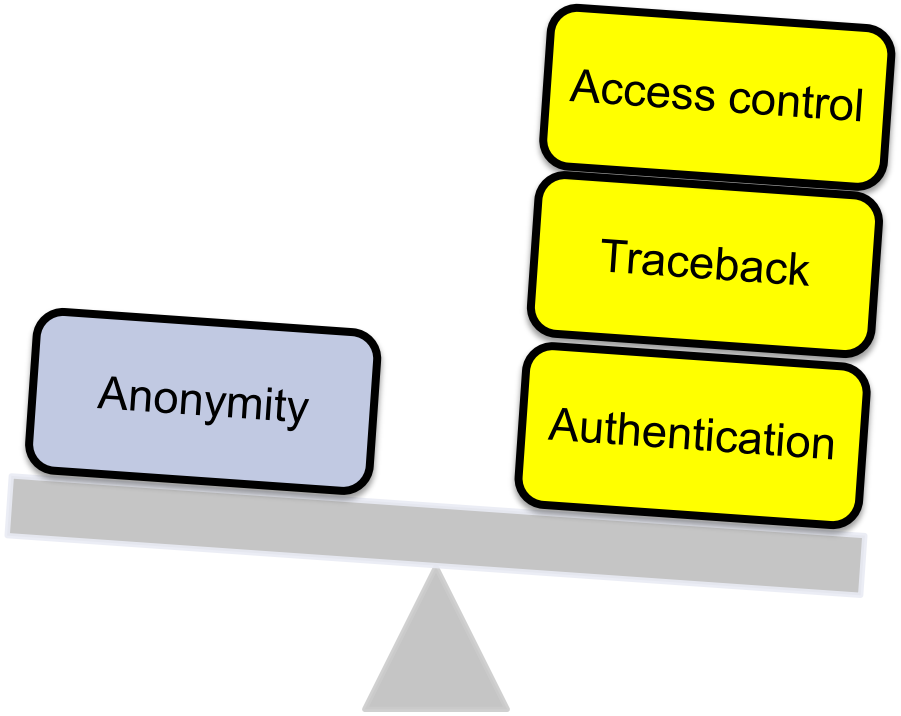
- Many approaches have been developed to address security controls
  - Access control/firewalls
  - Authentication/Authorization
  - Intrusion detection
  - Digital investigation
  - …

Can security be an obstacle to security?

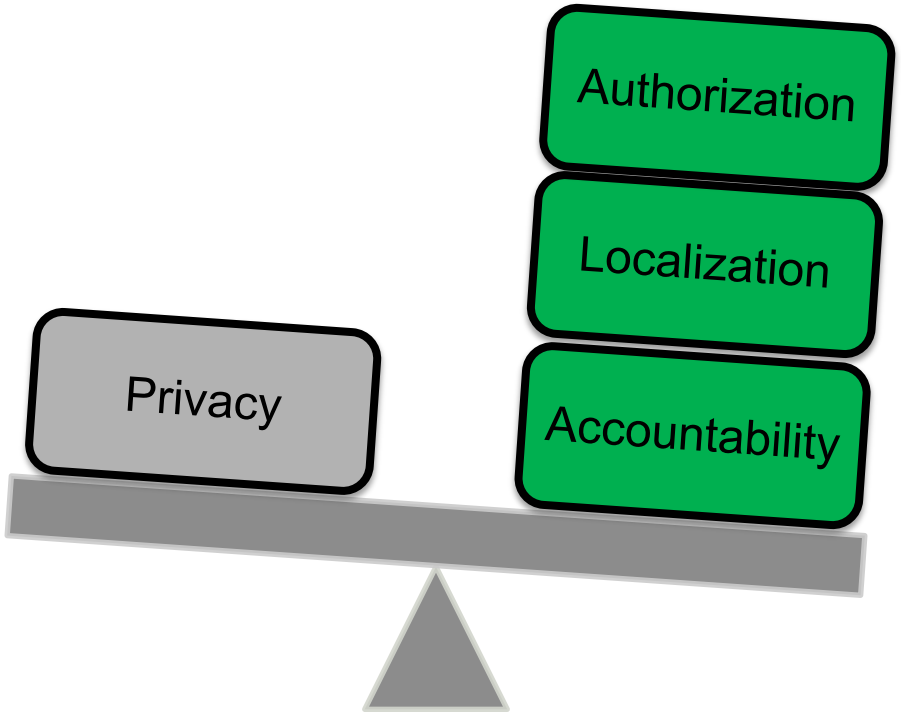
- Security controls: Typically based on the inspection of data
- New protection mechanisms obfuscate information which is crucial for security analysis

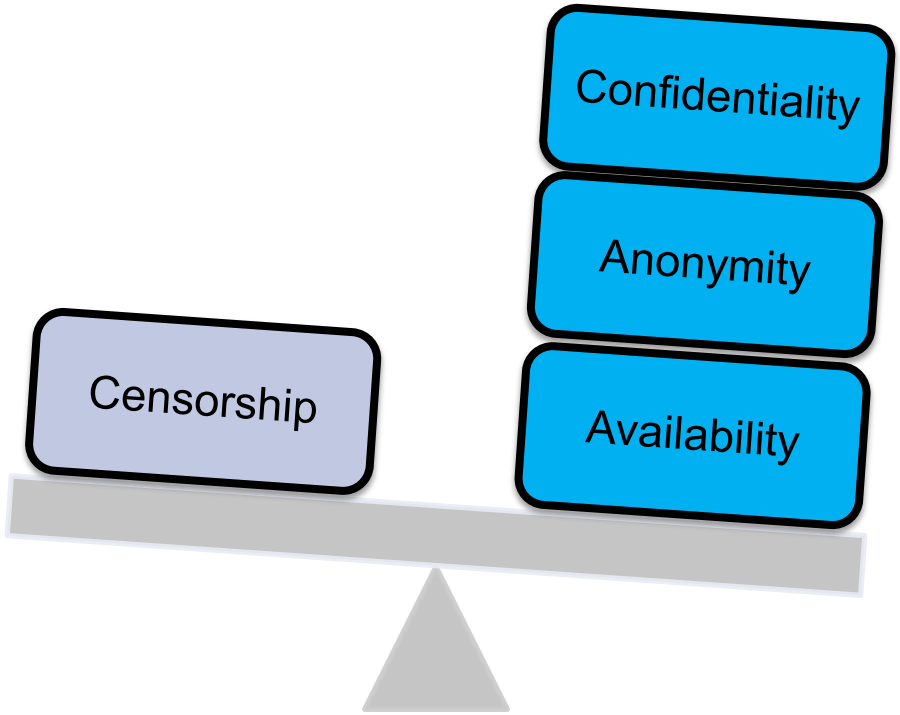
⇨ **Security requirements may be conflicting**

Conflicting security requirements[1]



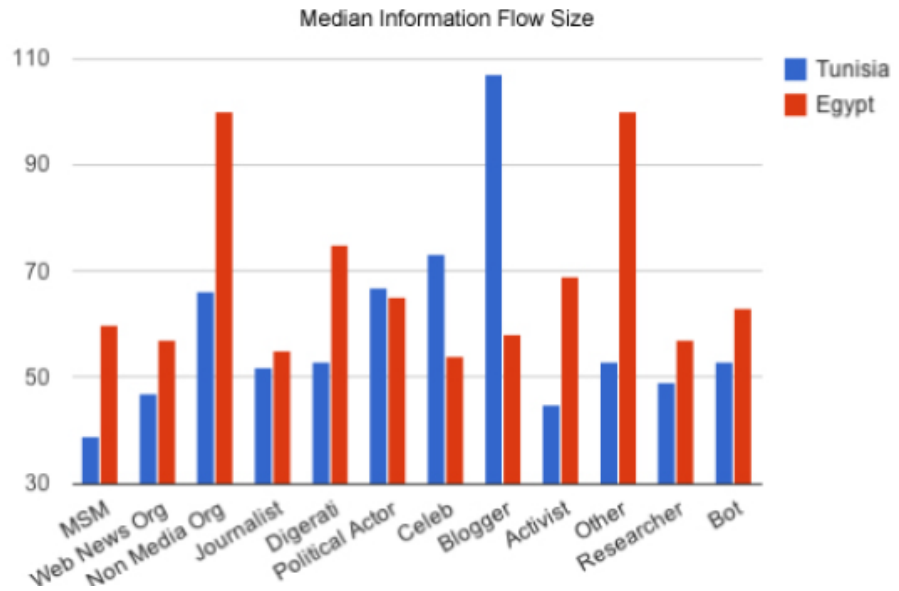
Conflicting security requirements[2]




Confidentiality
Anonymity
Availability
Censorship

Illustrative cases: social networking[1]

- 80% of Internet users are connected to social networks (UNCTAD Annual Report on ICT)

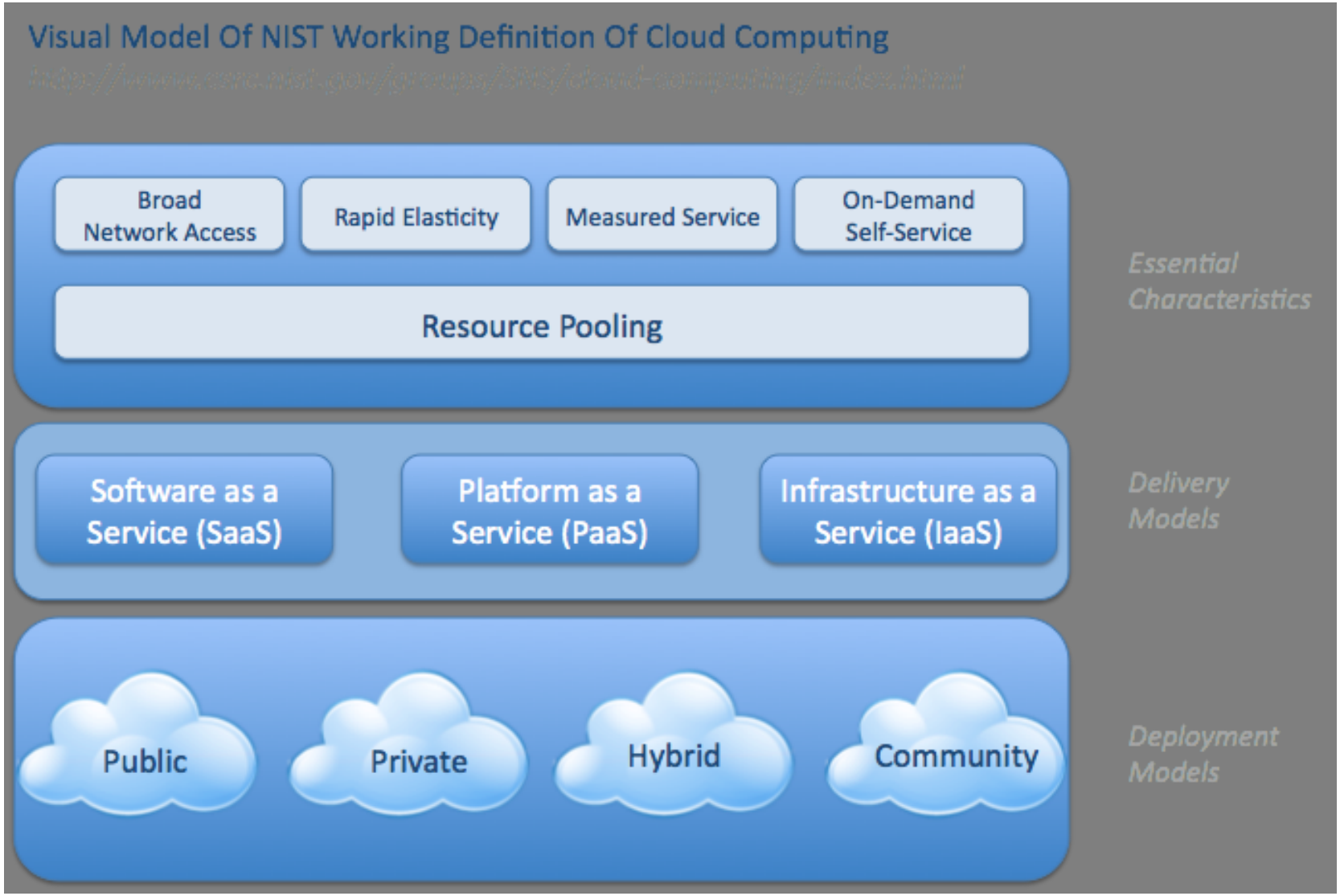


G. Lotan *et al.*, 'The Revolutions Were Tweeted: Information Flows During the 2011 Tunisian and Egyptian Revolutions,' International Journal of Communication, Vol. 5 , pp. 1375–1405, 2011.

Illustrative cases: social networking[2]

- Users use pseudonyms to build their profiles (~anonymity)
- Privacy violation are difficult to detect
  - Cannot be automated
  - Based on abuse reporting and mediator analysis
- Censorship to social networks have been circumvented during the Arab revolutions

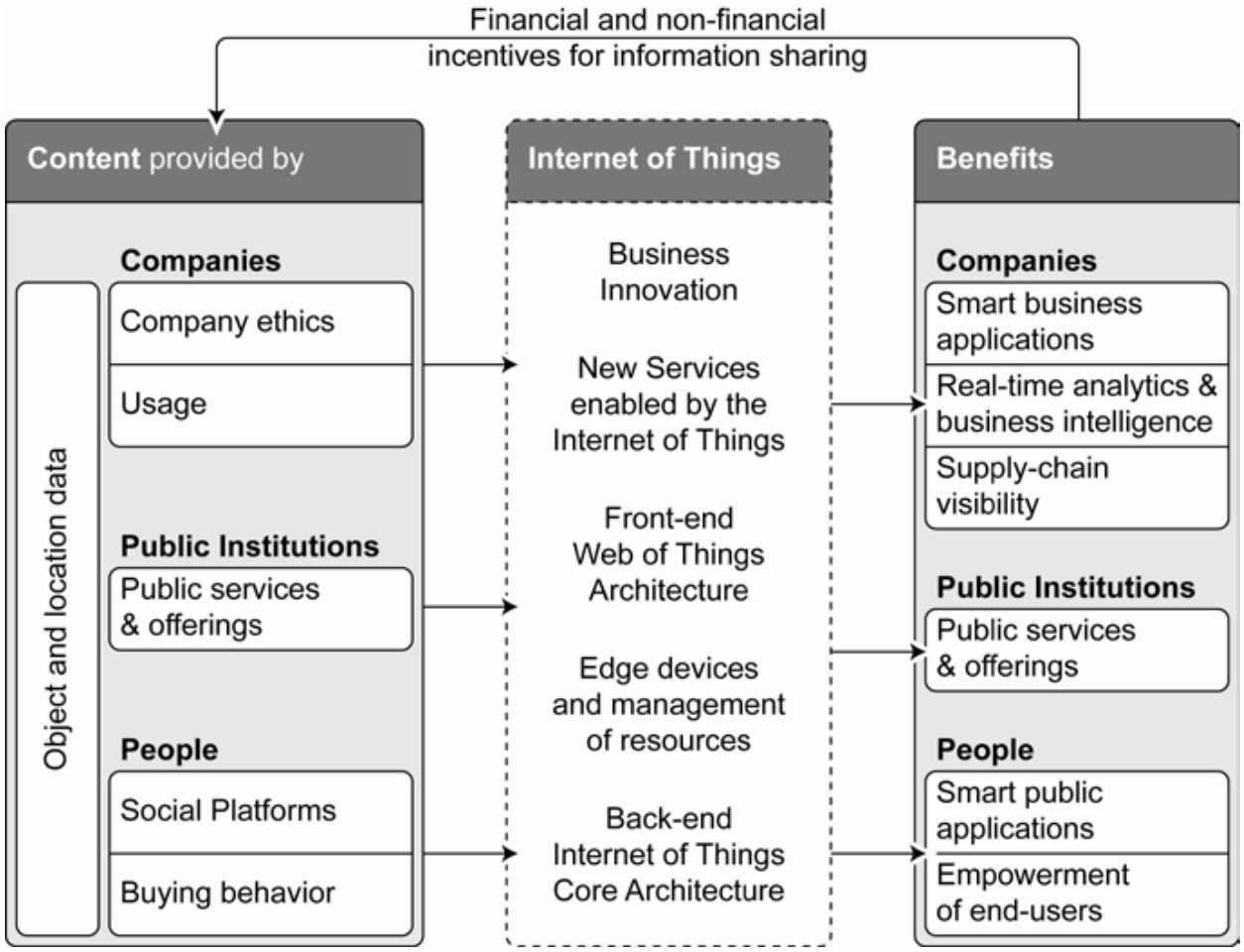
Illustrative cases: cloud computing[1]

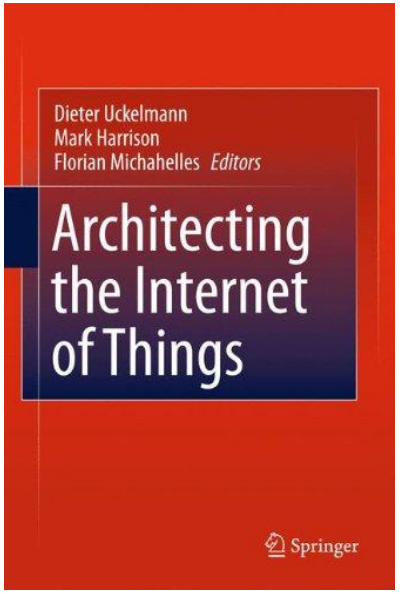


Illustrative cases: cloud computing[2]

- Anonymous access to private information should be guaranteed (e.g., patient files)
- Virtualization and anonymity offers new means of steganography (hiding data into storage infrastructures)
- Federated identities may encompass anonymous and non-anonymous accounts

Holistic IoT Scenario





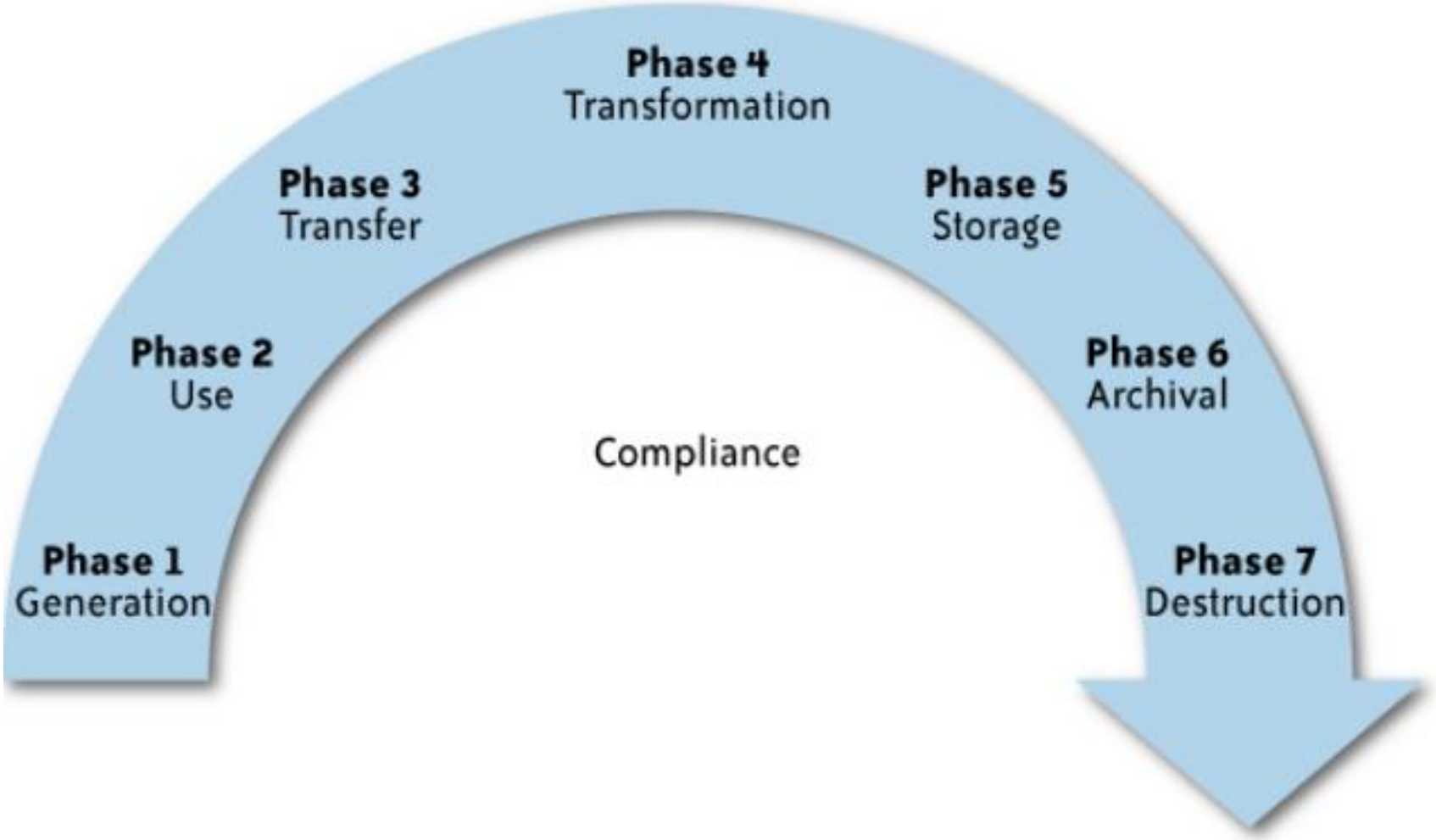
Architecting the Internet of Things
Uckelmann, Dieter; Harrison, Mark; Michahelles, Florian (Eds.)

1st Edition., 2011, SBN: 978-3-642-19156-5,2011.

Basic Components of the IoT

Enabling Building Blocks *These technologies directly contribute to the development of the IoT*	**Synergistic Technologies** *These technologies may add value to the IoT*
▪ Machine-to-machine interfaces and protocols of electronic communication ▪ Microcontrollers ▪ Wireless communication ▪ RFID technology ▪ Energy harvesting technologies ▪ Sensors ▪ Actuators ▪ Location technology ▪ Software	▪ Geo-tagging/geo-caching ▪ Biometrics ▪ Machine vision ▪ Robotics ▪ Augmented reality ▪ Mirror worlds ▪ Telepresence and adjustable autonomy ▪ Life recorders and personal black boxes ▪ Tangible user interfaces ▪ Clean technologies

Data lifecycle



Questions…

- Storage
- Retention
- Destruction
- Auditing, monitoring and risk management
- Privacy Breaches
- Who is responsible for protecting privacy?

Madrid resolution (2009)

- Approved by data protection authorities of 50 countries
- Framework for international standards on privacy and data protection
- Defines a set of principles and rights
  - for protecting privacy with regards to processing of personal data and
  - Facilitate international flow of personal data
- Encourages countries to implement proactive measures to promote better compliance with data protection laws and adapt information systems for processing of personal data

Privacy by design[1]

- EU review of Data Protection Directive in 2011
  - Principle of privacy by design
  - Implement privacy enhancing technologies (PETs)
  - Privacy by default settings
  - EU rules must apply if personal data is handled abroad by companies active in EU market
- Privacy by design binding for
  - Data controllers
  - Developers
  - Business partners
- Need for standardized privacy protection measures

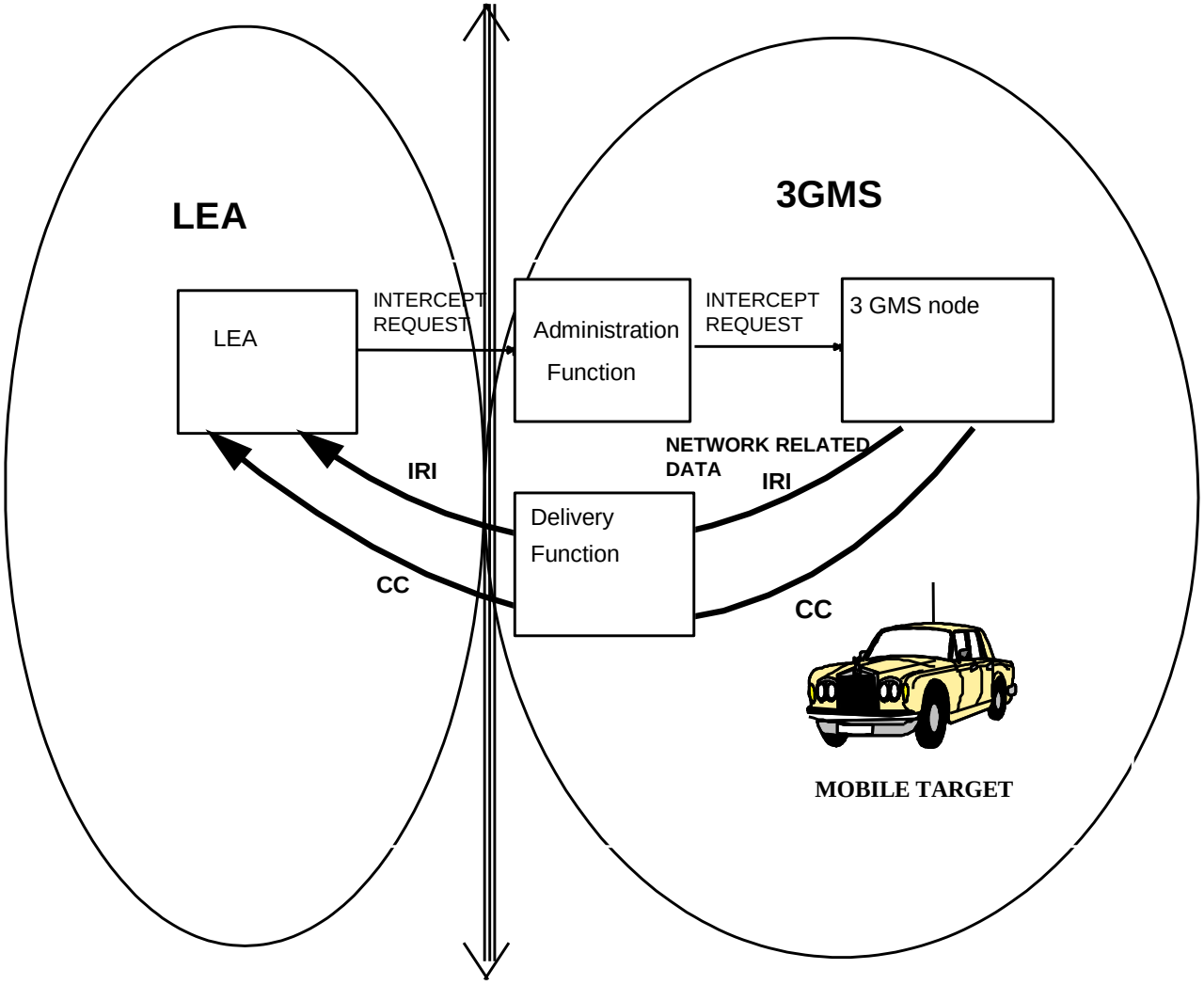
Privacy by design[2]

- 7 principles
  - Data minimization
  - Controllability
  - Transparency
  - User friendly systems
  - Data confidentiality
  - Data quality
  - Use limitation

Open Problems

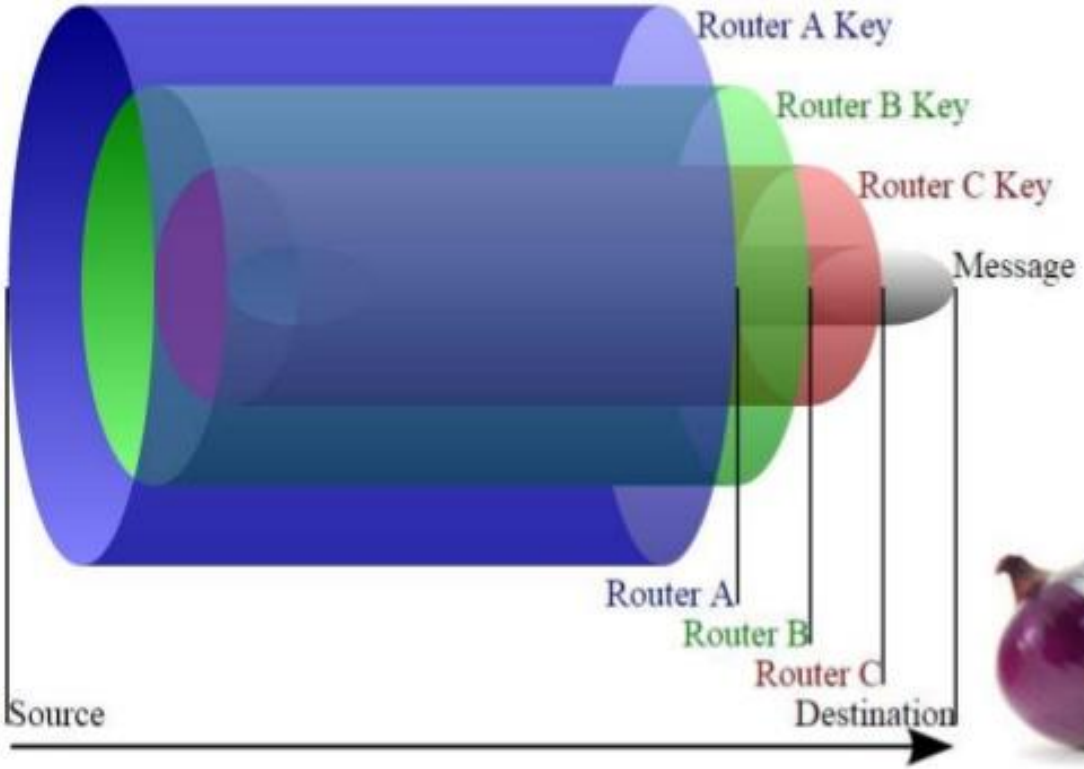
- Privacy/Lawful interception
- Anonymity/Forensics
- Pseudonyms/Privacy
- Federated identities/anonymity/privacy

Privacy/lawful interception

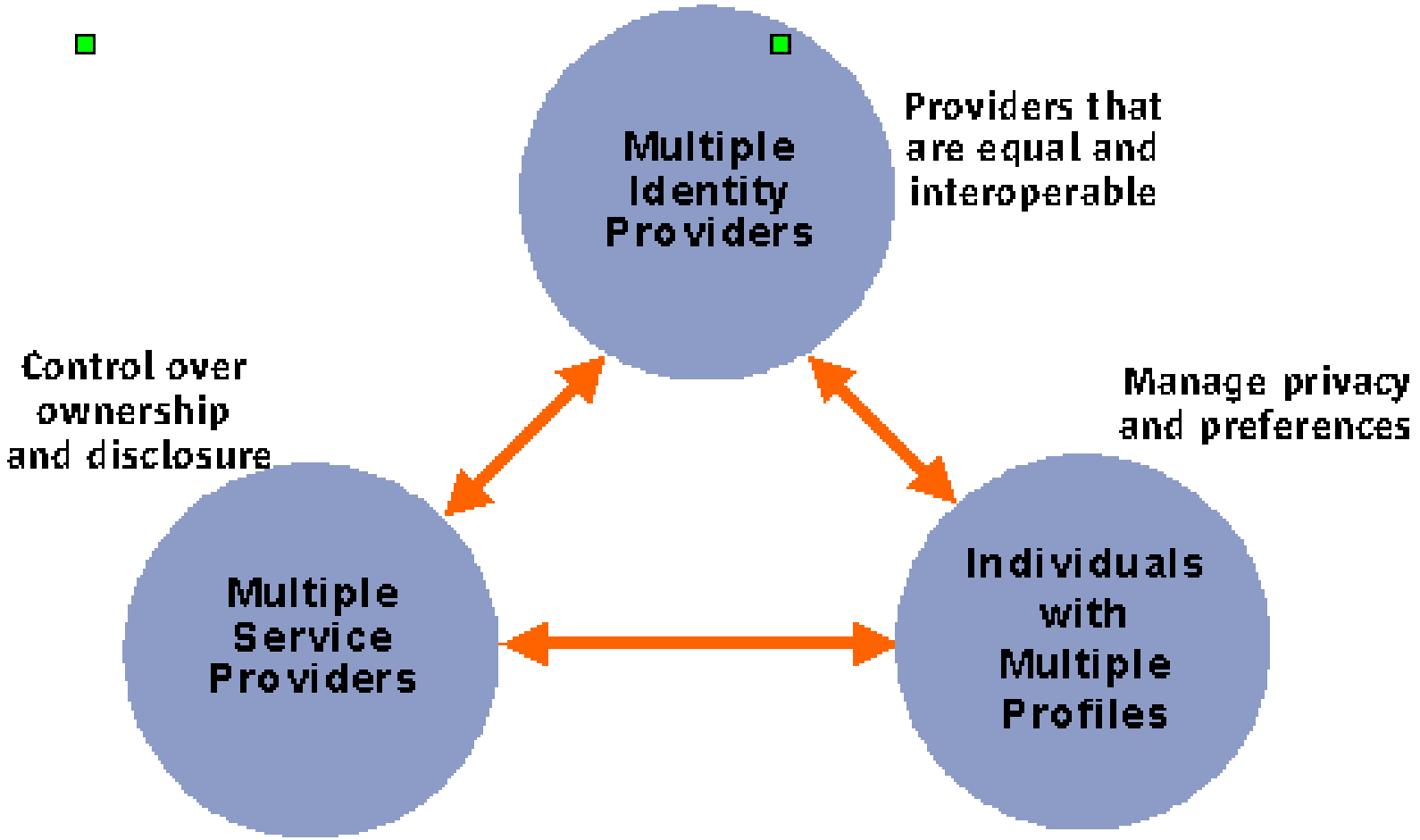


Anonymity/authentication

Onion Router and Analogy



Federated identities/anonymity/privacy



Thank you