ITU Workshop on "Future Trust and Knowledge Infrastructure", Phase 2
Geneva, Switzerland
1 July 2016

The Quest for Privacy

Dr. Corinna Schmitt

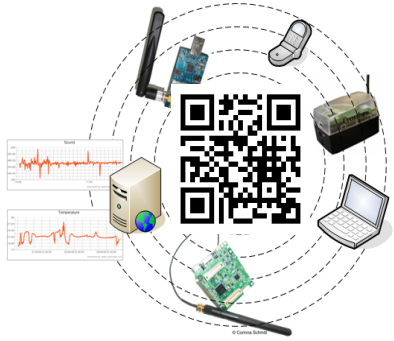
Head of Mobile and Trusted Communications

Communication Systems Group, Department of Informatics, University of Zurich

schmitt@ifi.uzh.ch

Content

- Motivation, challenges, and consequences
- The quest for privacy
- Characteristics for an IoT privacy framework
- Conclusions and future steps



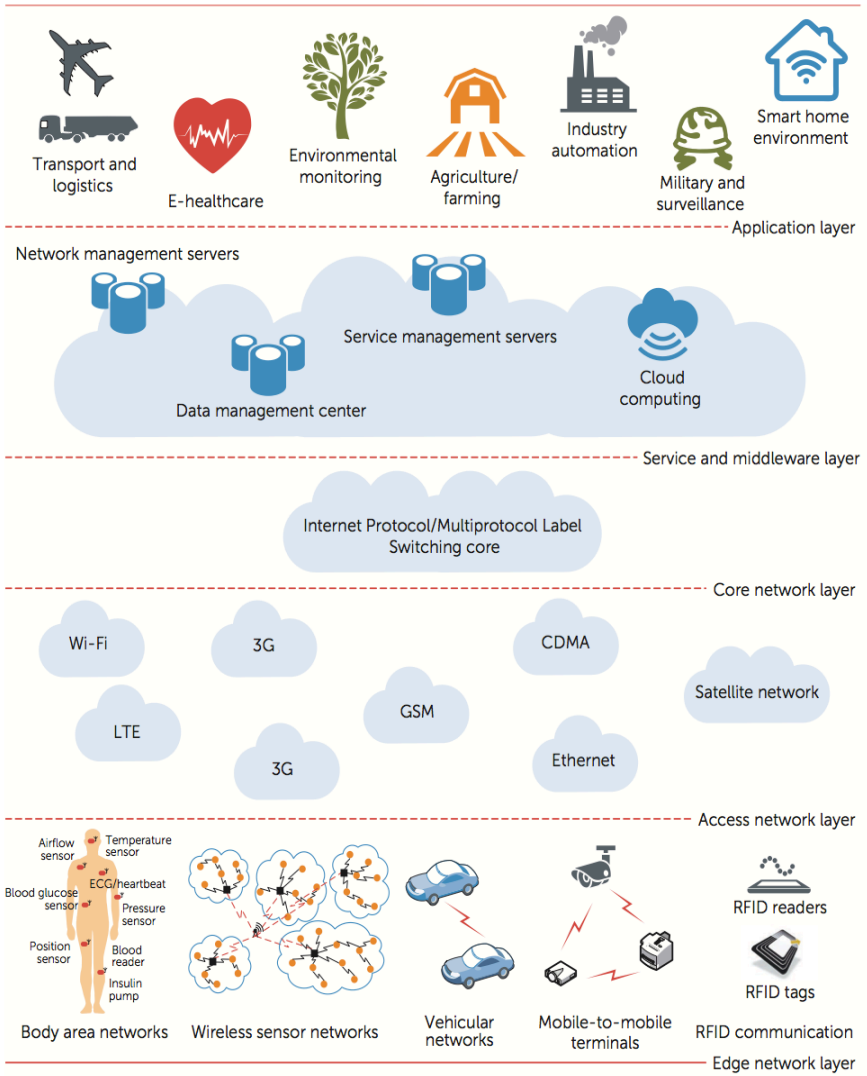
SEVENTH FRAMEWORK PROGRAMME

http://www.fp7-flamingo.eu

Motivation

- 25 billion connected devices vs. 7.2 billion world population
- Heterogeneous characteristic
- Sensitive data
- Technology diversity
- Application diversity

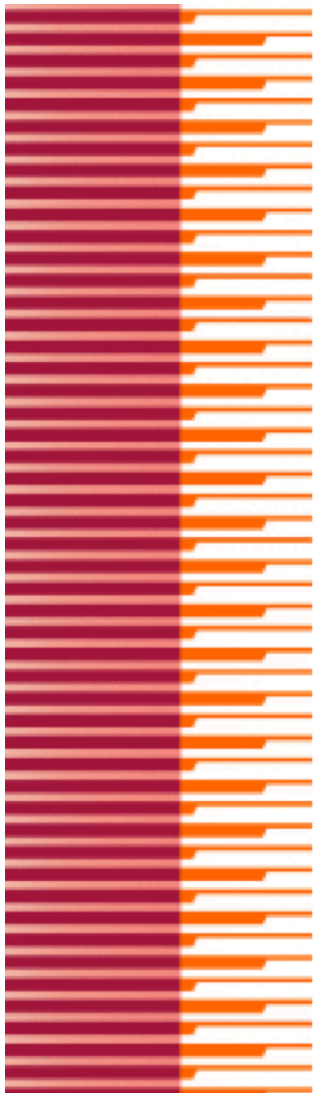
→ **Internet of Things (IoT)**



Internet of Things

http://www.affectiva.com/wp-content/uploads/2015/07/IOT-without-text-image-680x415.png

ITU – Definition of IoT (1)



http://www.itu.int/itu-t/recommendations/rec.aspx?rec=Y.2060

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2060

(06/2012)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

Overview of the Internet of things

ITU – Definition of IoT (2)

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 device: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.2.2 Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.2.3 thing: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

http://www.itu.int/itu-t/recommendations/rec.aspx?rec=Y.2060

ITU – Definition of IoT (3)

Location-based communications and services may be constrained by laws and regulations, and should comply with security requirements.

- Security: In the IoT, every 'thing' is connected which results in significant security threats, such as threats towards confidentiality, authenticity and integrity of both data and services. A critical example of security requirements is the need to integrate different security policies and techniques related to the variety of devices and user networks in the IoT.
- Privacy protection: Privacy protection needs to be supported in the IoT. Many things have their owners and users. Sensed data of things may contain private information concerning their owners or users. The IoT needs to support privacy protection during data transmission, aggregation, storage, mining and processing. Privacy protection should not set a barrier to data source authentication.
- High quality and highly secure human body related services: High quality and highly secure human body related services needs to be supported in the IoT. Different countries have different laws and regulations on these services

http://www.itu.int/itu-t/recommendations/rec.aspx?rec=Y.2060

ITU – Definition of IoT (4)

8.6 Security capabilities

There are two kinds of security capabilities: generic security capabilities and specific security capabilities. Generic security capabilities are independent of applications. They include:

– at the application layer: authorization, authentication, application data confidentiality and integrity protection, privacy protection, security audit and anti-virus;

– at the network layer: authorization, authentication, use data and signalling data confidentiality, and signalling integrity protection;

– at the device layer: authentication, authorization, device integrity validation, access control, data confidentiality and integrity protection.

Specific security capabilities are closely coupled with application-specific requirements, e.g., mobile payment, security requirements.

http://www.itu.int/itu-t/recommendations/rec.aspx?rec=Y.2060

EU – Definition of IoT (1)

http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

Briefing

May 2015

European Parliament

The Internet of Things
Opportunities and challenges

SUMMARY

The Internet of Things (IoT) refers to a distributed network connecting physical objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines or computers. The data these devices report can be collected and analysed in order to reveal insights and suggest actions that will produce cost savings, increase efficiency or improve products and services. The IoT is growing rapidly, with an estimated 25 billion connected objects throughout the world by 2020, and added value from the IoT of US$1.9 trillion by the same year. The IoT can thus be a key contributor to achieving the EU's Europe 2020 strategy for smart, sustainable and inclusive growth.

EU – Definition of IoT (2)

http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

Briefing

May 2015

European Parliament

The Internet of Things
Opportunities and challenges

…

However the IoT also poses important challenges to society. Open standards and interoperability may need to be encouraged, in order to widen choices for consumers and ensure competition and innovation. Sufficient radio spectrum must be allocated for future needs. With so many interconnected devices, security is a major concern. A balance needs to be achieved between the rights of citizens to keep personal data private and protected, and to consent to its use in other contexts, and the significant benefits that can accrue to enterprises and society from the analysis of such rich data sources.

…

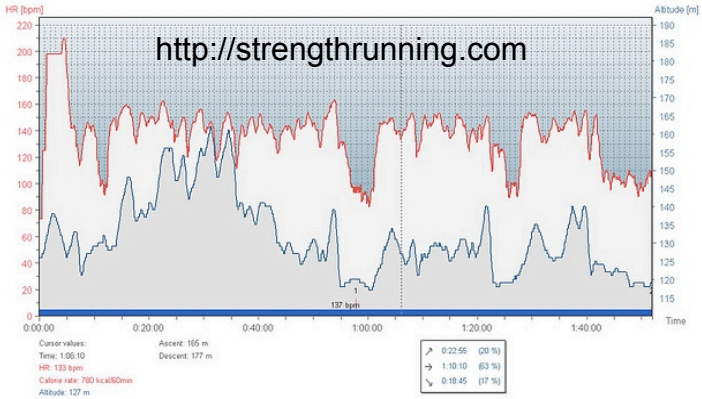
Profiling (1)

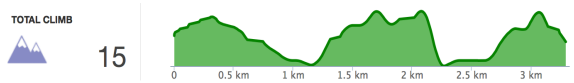
Data collection

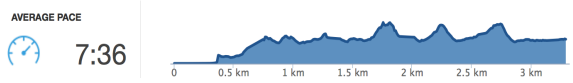
http://running.competitor.com

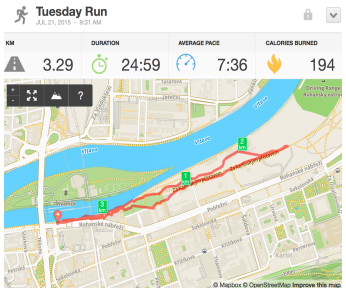
Upload to IoT Service

Profiling









Splits

NAME	PACE	CLIMB
1 km	4:21	-2
2 km	8:50	4
3 km	9:29	0
4 km	8:00	-2

Profiling (2)

Upload to IoT Service

Profiling

Consequences

Danger / Awareness

Person is in good physical condition

Runs every day around 9:30 a.m. for 30 minutes
→ No one at home

Running area has high attack rate

ifi

Advantages vs. Danger

- Collected data allows for profiling!
- Information about health status and training conditions
  - Heart beat and burned calories
  - Speed
  - Running track and duration
- But also brings dangerous aspects with
  - Prediction of preferred track
  - Absence from home
  - Prediction of breaks

→ Am I really aware of what data tells about me?

Consequences

- Sensitive Information can be concealed or controlled without data owners knowledge
- Small leakage of information could severely damage user privacy

→ Not everyone has the same awareness for security and privacy threats!

→ IoT acceptance requires secure, trustworthy, and privacy preserving infrastructure!

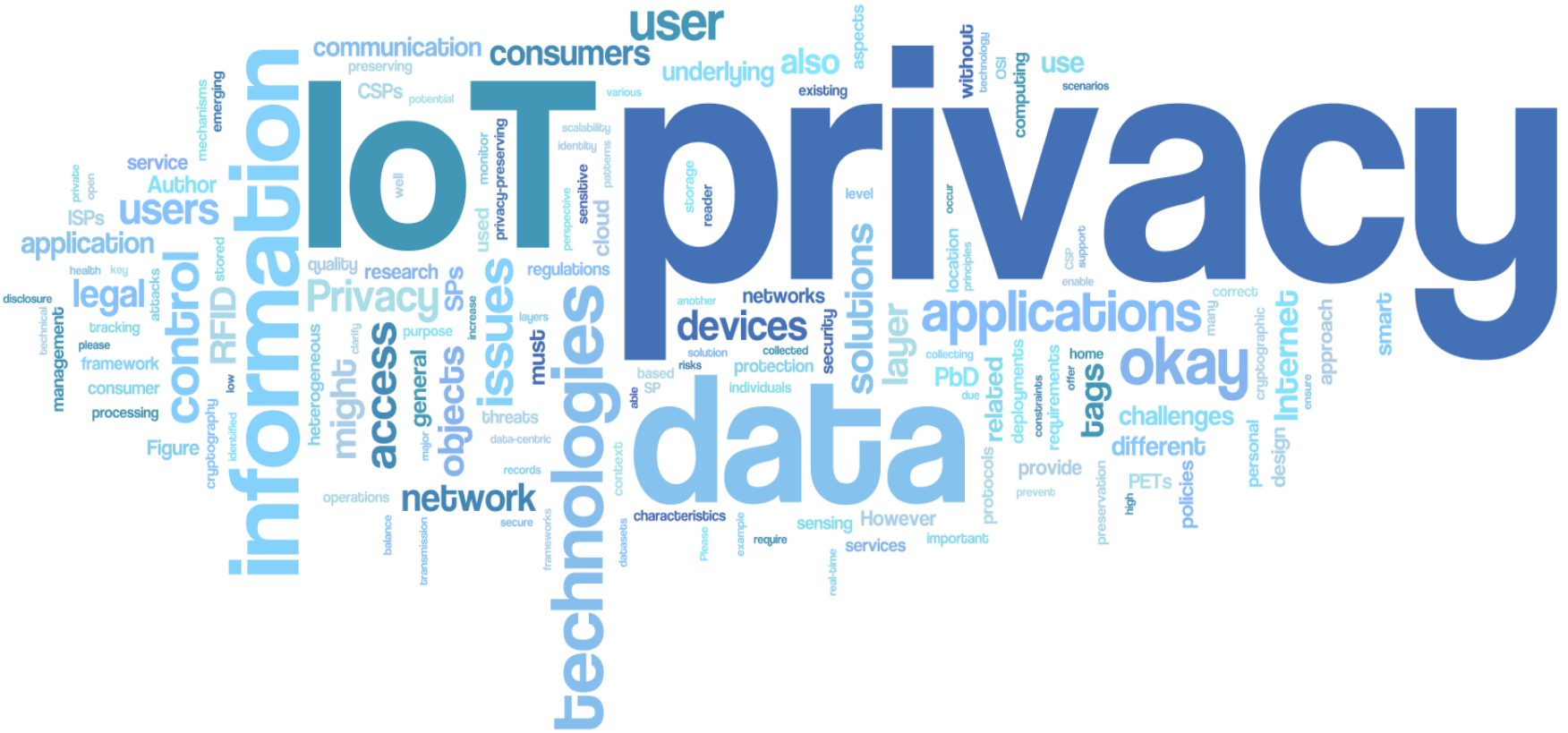
Definitions

- Security incorporates all mechanisms used to transmit and store data in a secure manner
  - Encryption technologies, DTLS, certificates

- Privacy is a request that the data owner stays owner of the data and can manage data access to authorized entities
  - Access control, credentials

→ Security + Privacy = Indication for trustworthiness of a service

The Quest for Privacy



ifi

IoT Applications and Privacy Concerns (1)

Privacy is the right of individuals or cooperative users to maintain confidentiality and control over their information when it is disclosed to another party.

- In IoT applications privacy challenges can be identified primarily from the perspective of consumers and their stored data sets.

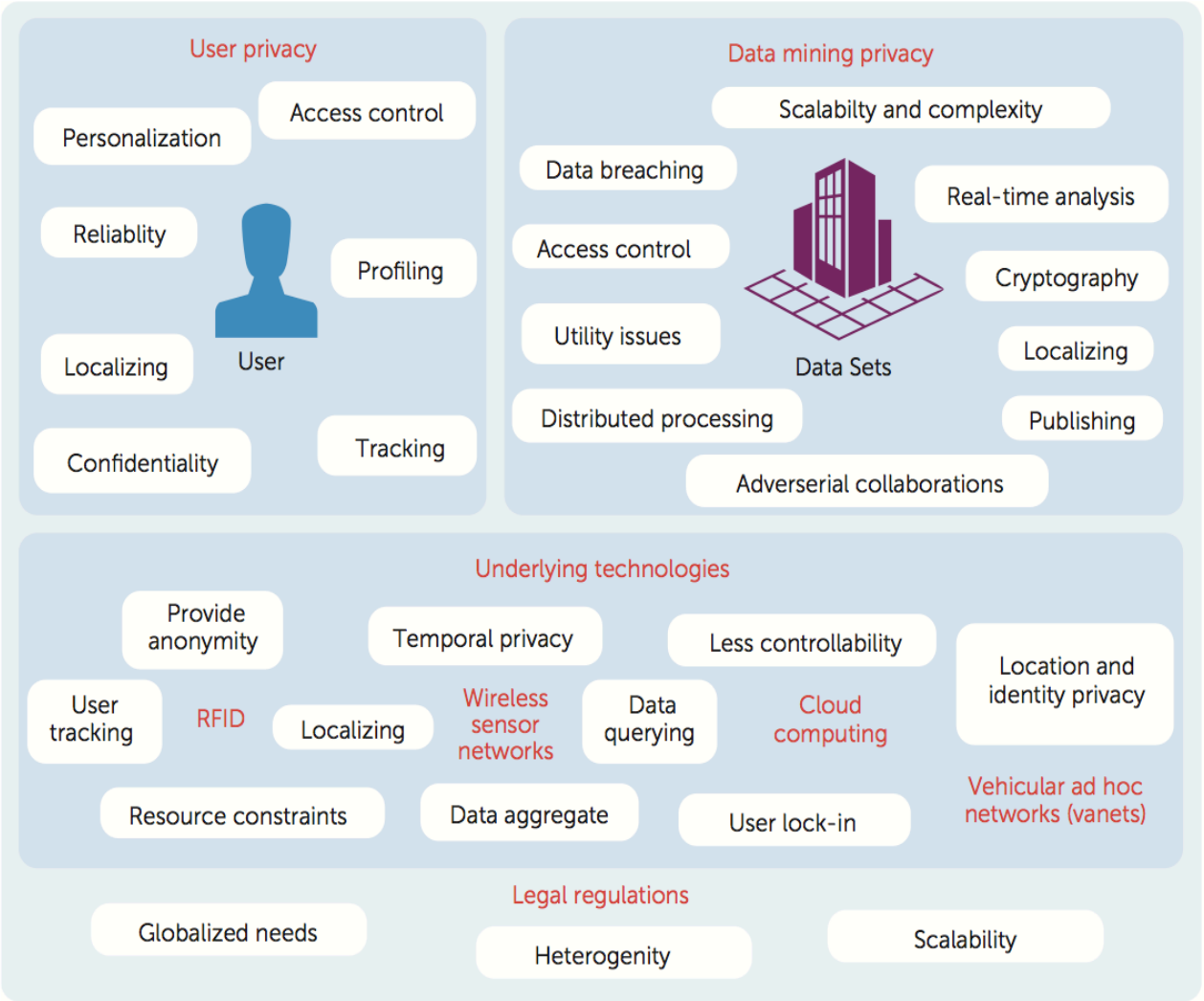
IoT Applications and Privacy Concerns (2)

- Cloud Service Provider (CSP) and Internet Service Provider (ISPs) process user‘s personal information
  → Unexpectedly initiate privacy threats and attacks

- IoT networks can compromise tens of millions of devices with heterogeneous characteristics
  – Resources constraints, mobility, scalability, degree of autonomy, interoperability

→ Privacy issues in IoT vary widely with respect to the application involved!

Key Aspects for IoT Privacy



User Privacy

- Identification of personal information during transmission over the Internet.

- Example:
  - Buy RFID-tagged object with credit card.
    → Personal information may be linked to the object and to CSP

- Privacy threats:
  - Tracking, localizing, and profiling
  - Access control and confidentiality
  - Data protection, content confidentiality and reliability

Data Mining

- Critical issues:
  - Scalability, distributed processing, real-time analytics
  - Data publishing, application context, cryptography

- Privacy threats:
  - Data sharing and transmitting with disclosure of location and temporally sensitive data traffic.
  - Large data sets require balance in privacy preservation in data cleaning and the intentional reduction of data quality

→ Different privacy constraints

→ Treat data sets differently for anonymization purposes

→ Access control and maintenance

Underlying IoT Technologies

- Challenges
  - Heterogeneous structure of devices and resources.

- Examples:
  - RFID objects can allow context-aware digital objects to represent physical objects
  - Wireless Sensor Networks have high self-organizing ability
  - Cloud services might lead to loss of processing control for users and are requested to support transparency

→ Data oriented or context oriented privacy

→ Privacy support depends on resources

Legal Regulations

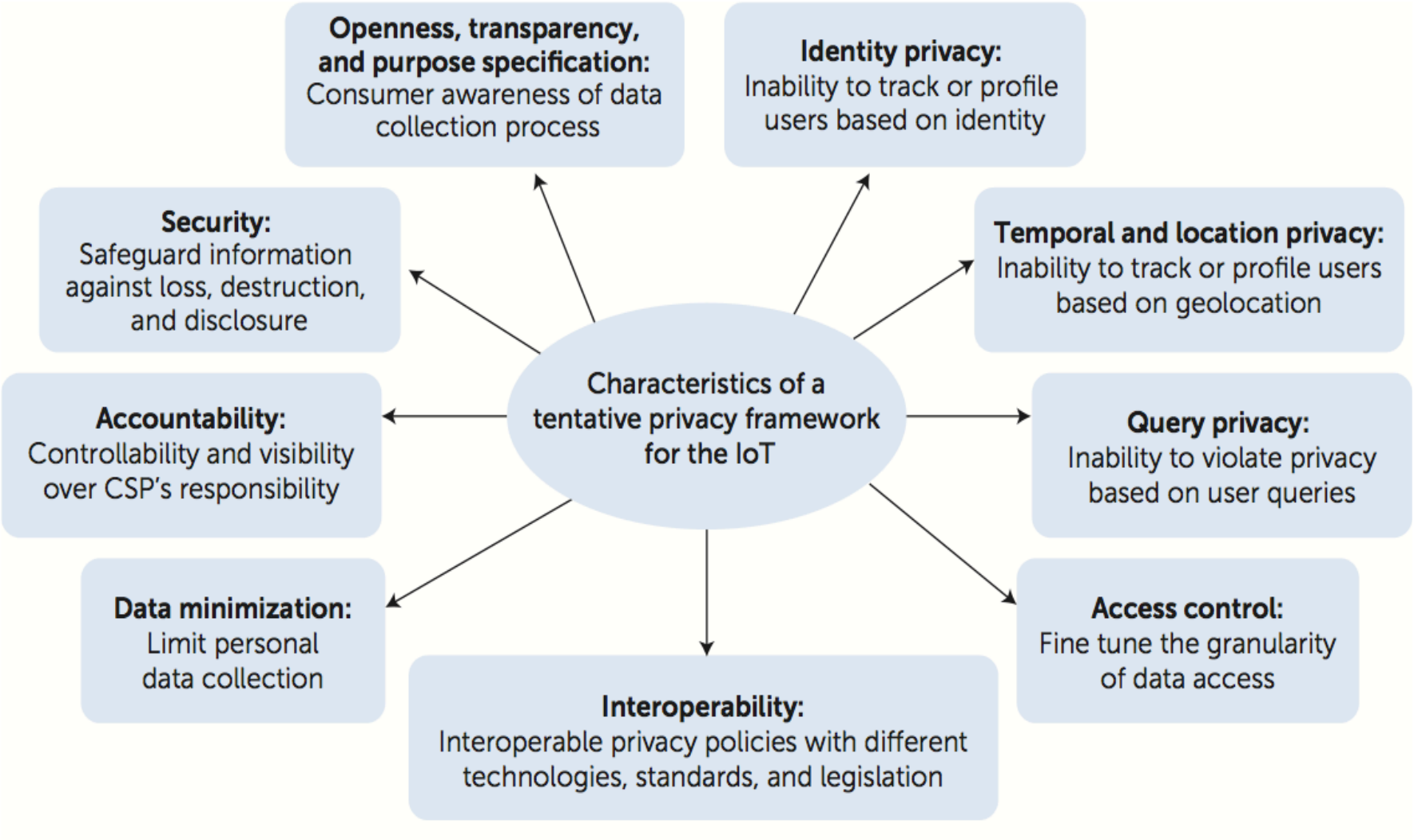
- Privacy is a compliance issue sitting at the intersection of social norms, human rights, and legal mandates

- Legislation is required to support basic privacy principles
  - Lawfulness and fairness
  - Proportionality, purpose specification, data quality, openness, and accountability

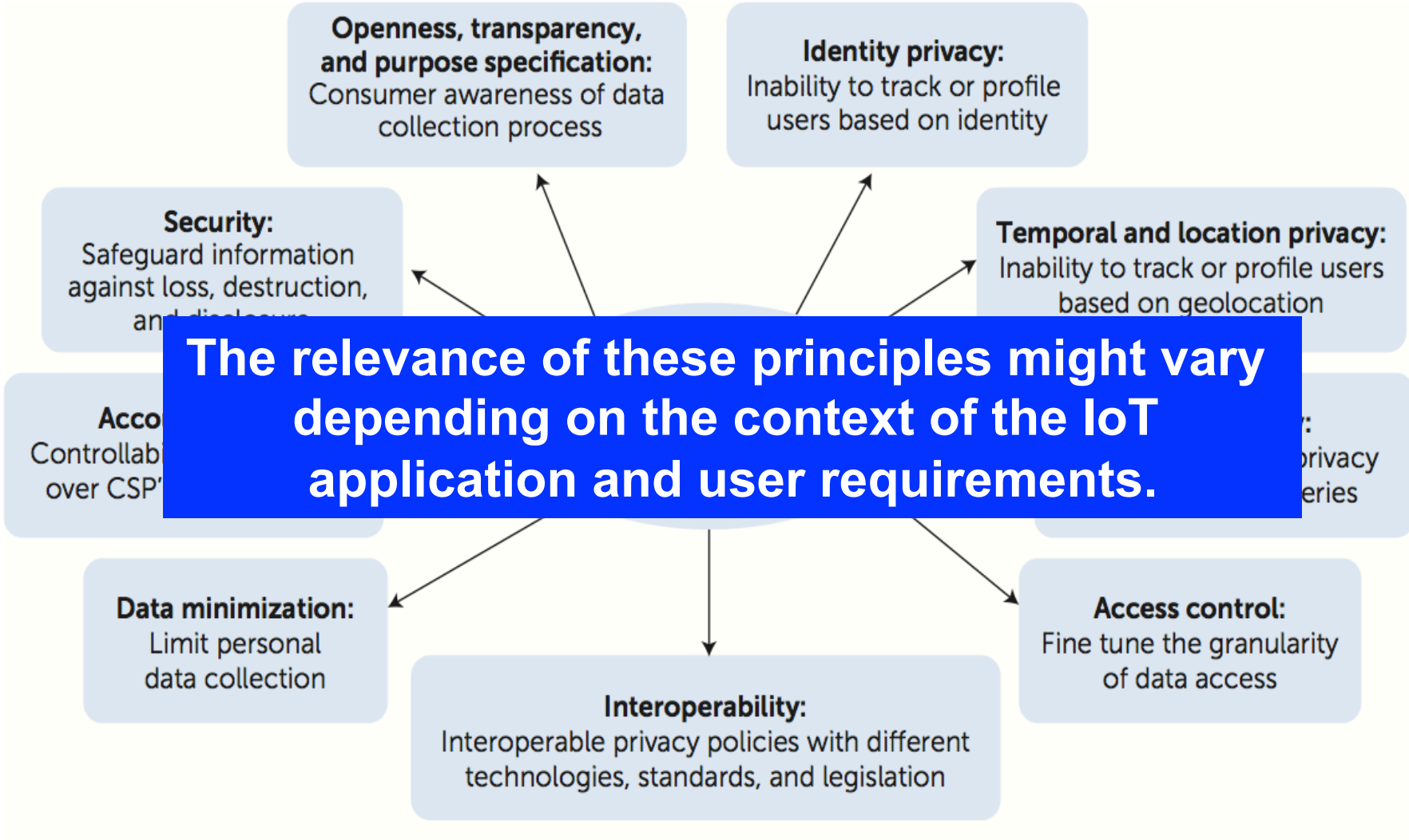
→ Collaboration of governmental & private organizations

→ Strong legal framework

IoT Privacy Framework Characteristics

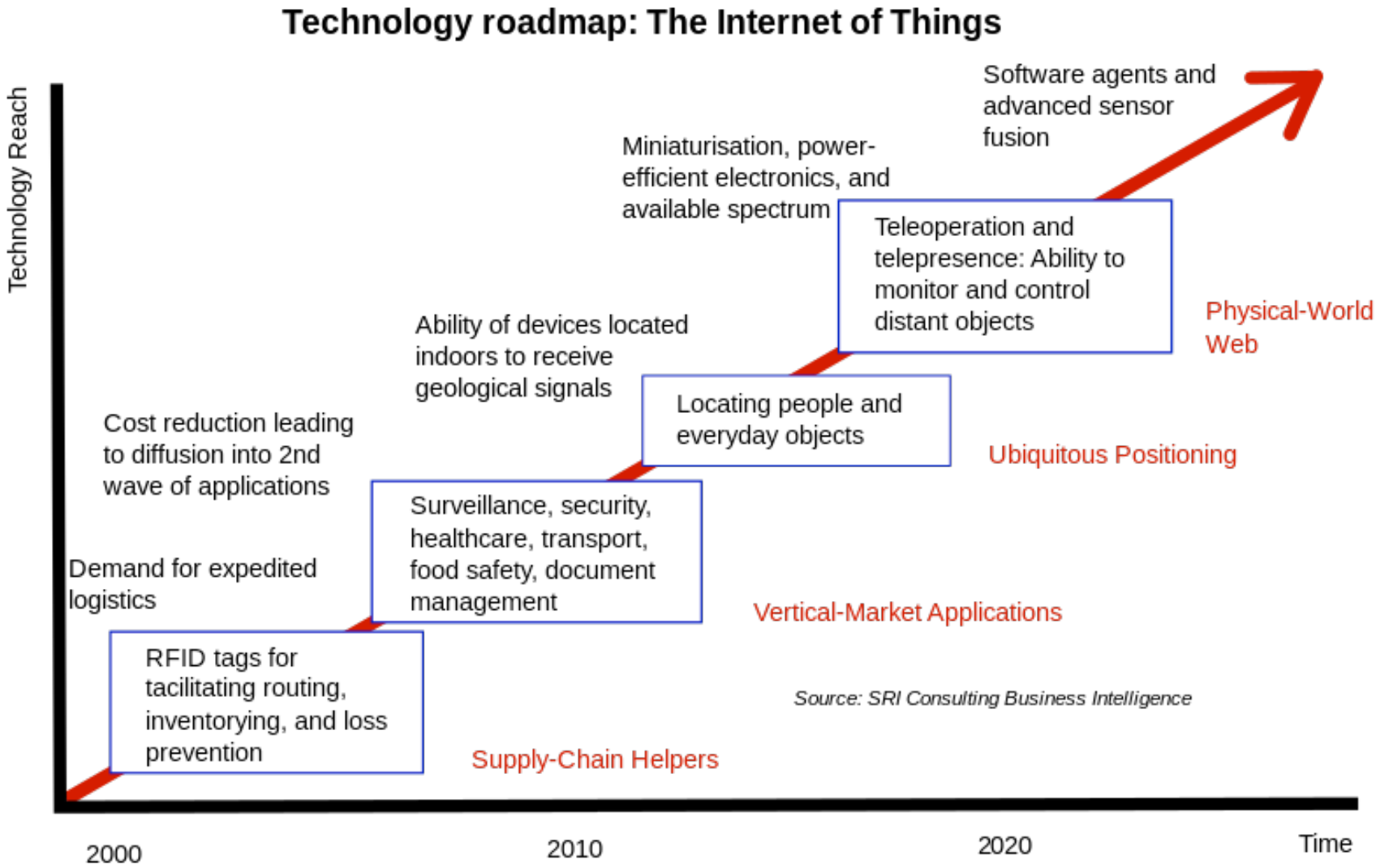


IoT Privacy Framework Characteristics



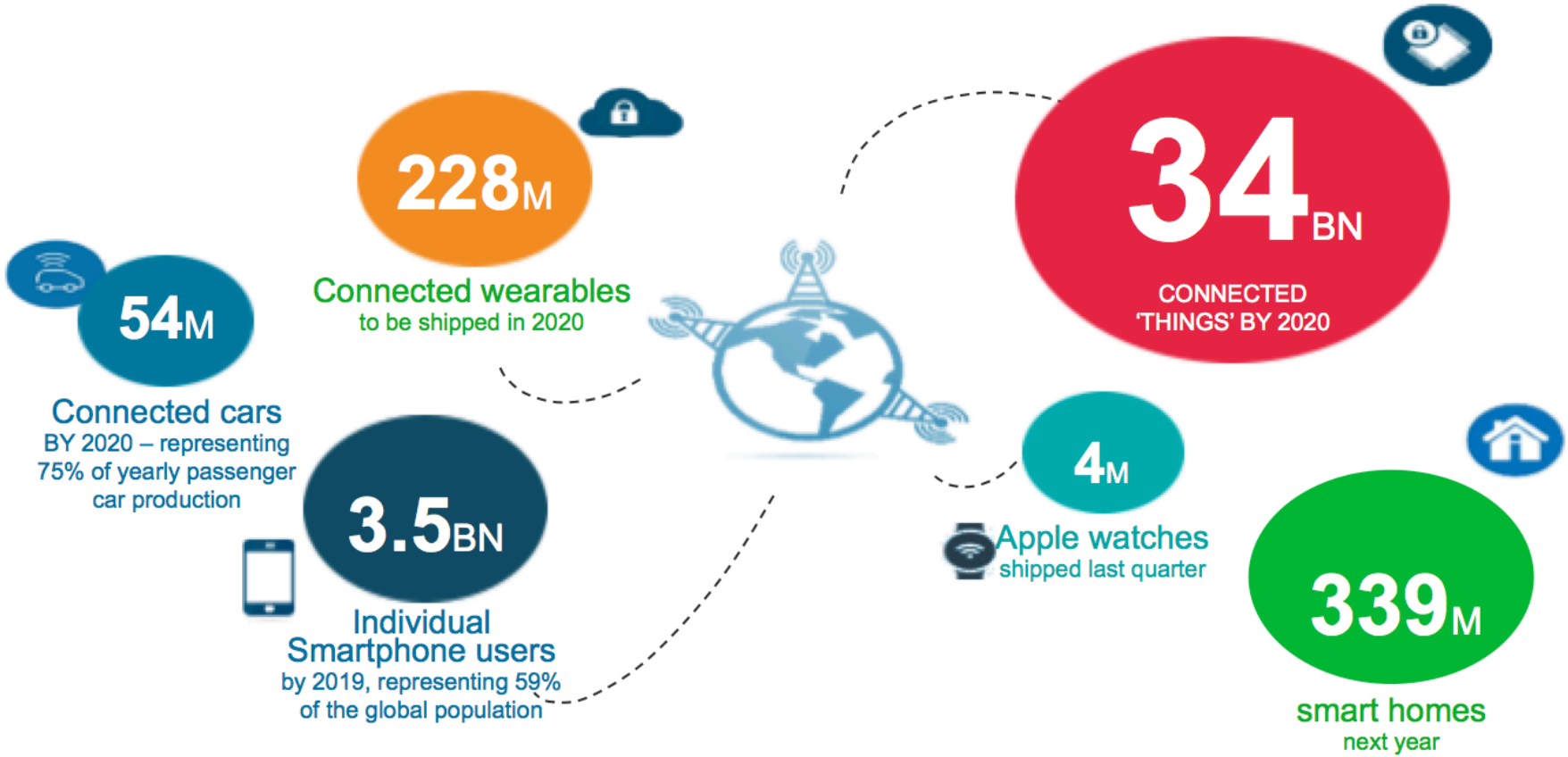
The relevance of these principles might vary depending on the context of the IoT application and user requirements.

IoT Development Prediction (1)



ifi

IoT Development Prediction (2)



Sources:
IDC, SCOTIABANK, BI INTELLIGENCE, GARTNER, FORRESTER, IHS TECHNOLOGY

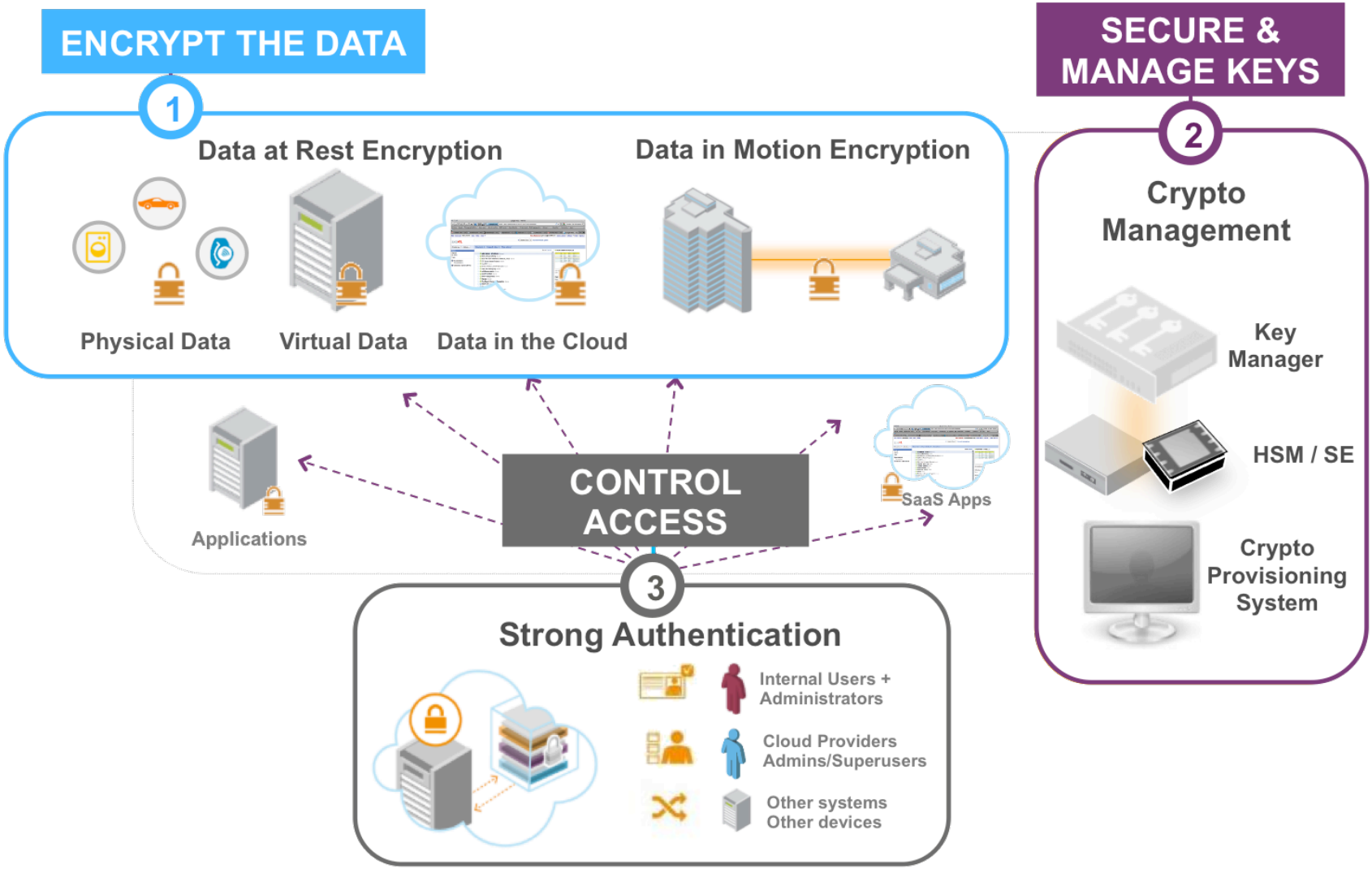
Conclusions

- Privacy becomes more and more relevant
- Key areas to work on
  - Security, transparency, access control, etc.

- Addressing privacy already during design of solution
  → Law change for 2017 predicted in EU
- Include privacy support
  - As a MUST in upcoming ITU-T recommendations
  - In all questions handled by SG 20, especially in Q2-Q4

→ Trustworthy IoT services and applications will be accepted better by the consumer!

Future Steps



Thanks ...

References

- P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, A. V. Vasilakos: *The Quest for Privacy in the Internet of Things*; IEEE Computer Society, IEEE Cloud Computing, Vol. 2016, No. 3, pp. 34-43, April 2016
- Gartner Report: *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*; November 10, 2015, http://www.gartner.com/newsroom/id/3165317
- R. Roman, J. Zhou, J. Lopez: *On the Features and Challenges of Security and Privacy in Distributed Internet of Things*; *Computer Networks*, vol. 57, no. 10, 2013, pp. 2266–2279
- *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FTC Report, 2012; http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer
- D. Evans: *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything*, Cisco, April 2011, http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
- European Parliament: *The Internet of Things – Opportunities and Challenges*, May 2015, http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf
- *ITU-T Recommendation Y.2060: Overview of the Internet of Things*, June 2012, http://www.itu.int/itu-t/recommendations/rec.aspx?rec=Y.2060