Fifth SG13 Regional Workshop for Africa on "ITU-T Standardization Work on Future Networks: Towards a Better Future for Africa"

Cairo, Egypt

April 2, 2017

IoT Connectivity vs Privacy Requests

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

universität wien

Cooperative Systems Group

symbIoTe

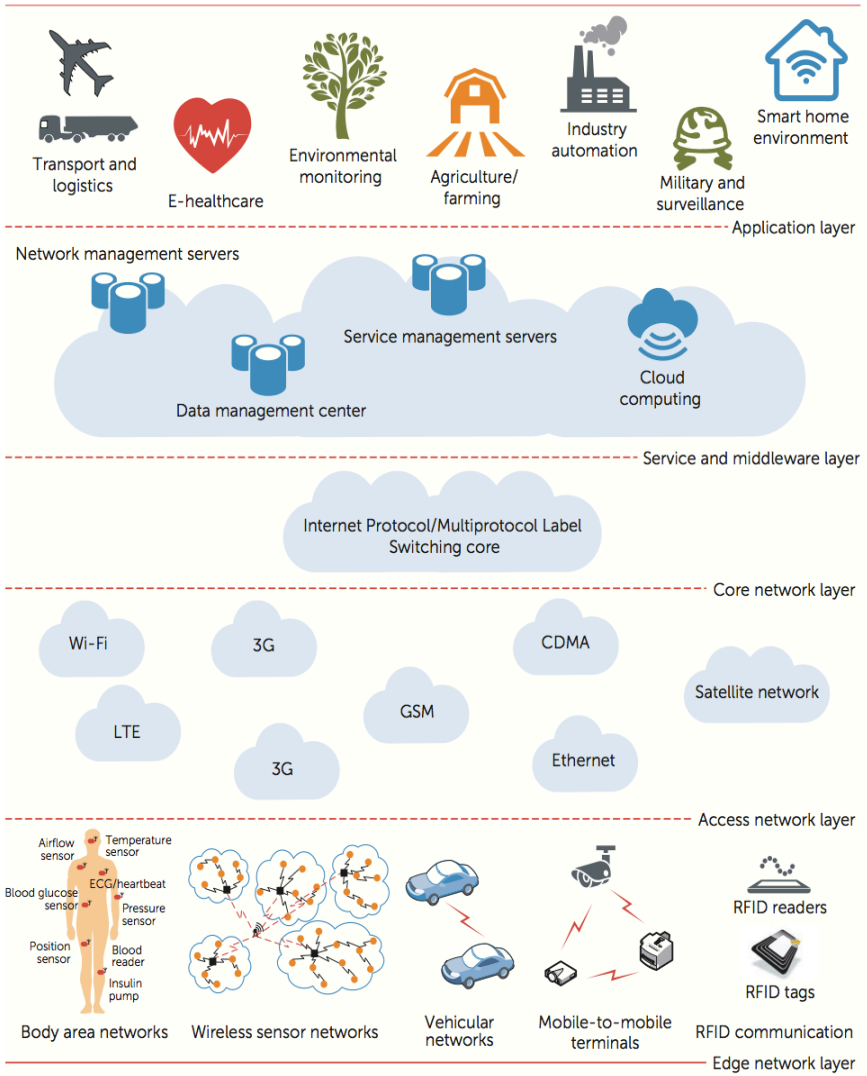
CSG Communication Systems Group

Universität Zürich[UZH]

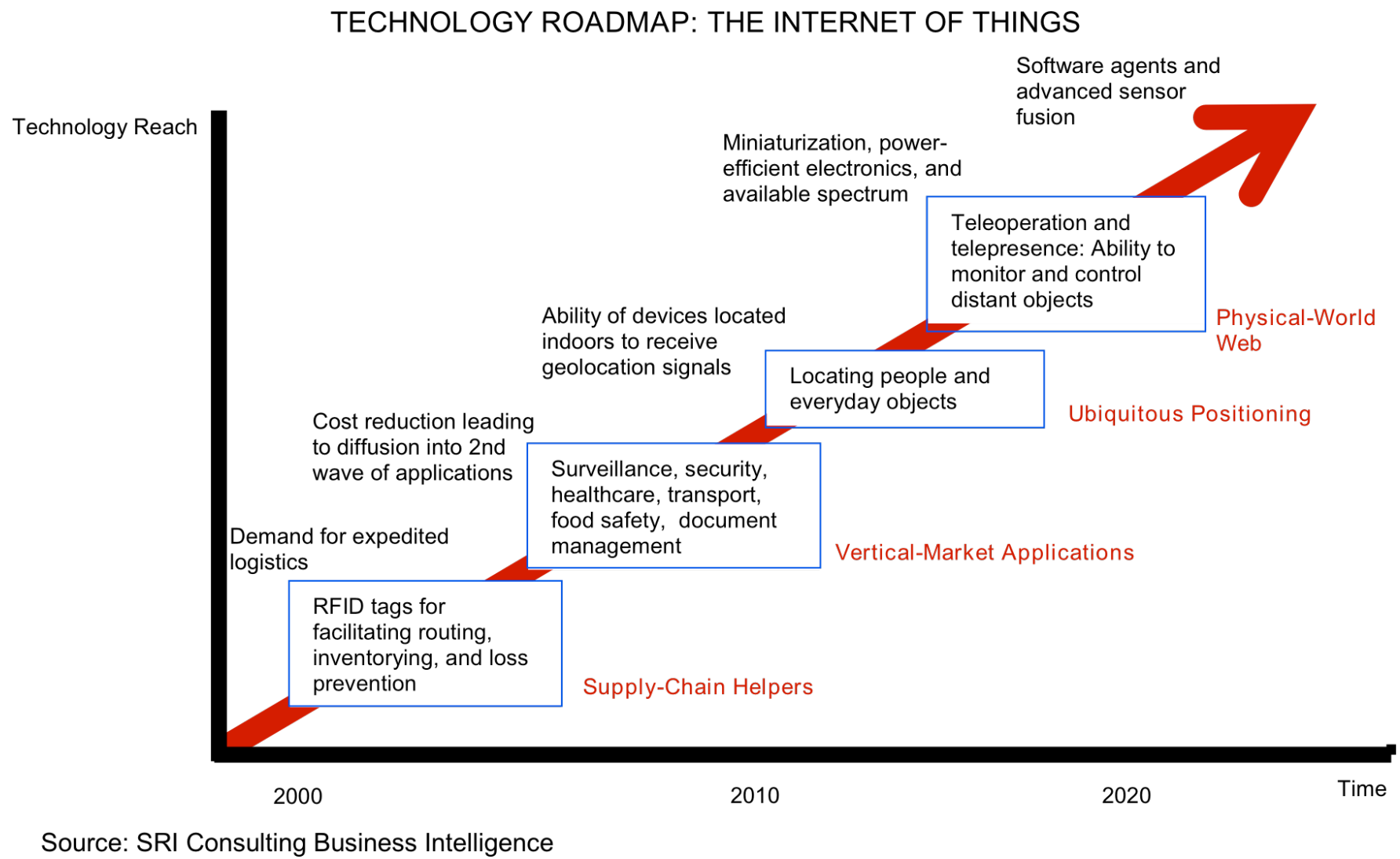
Motivation

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

→ **Internet of Things (IoT)**



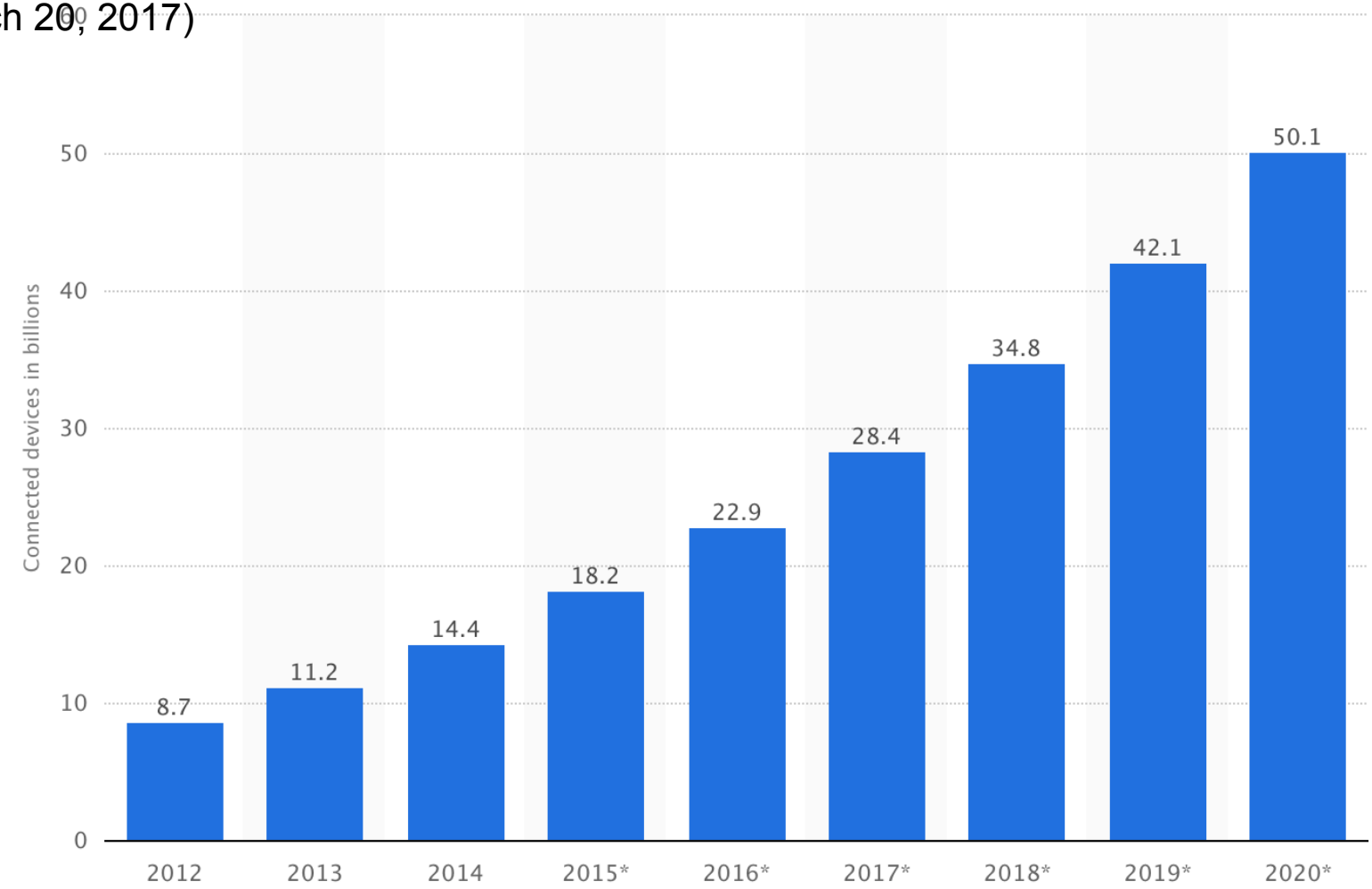
IoT Development



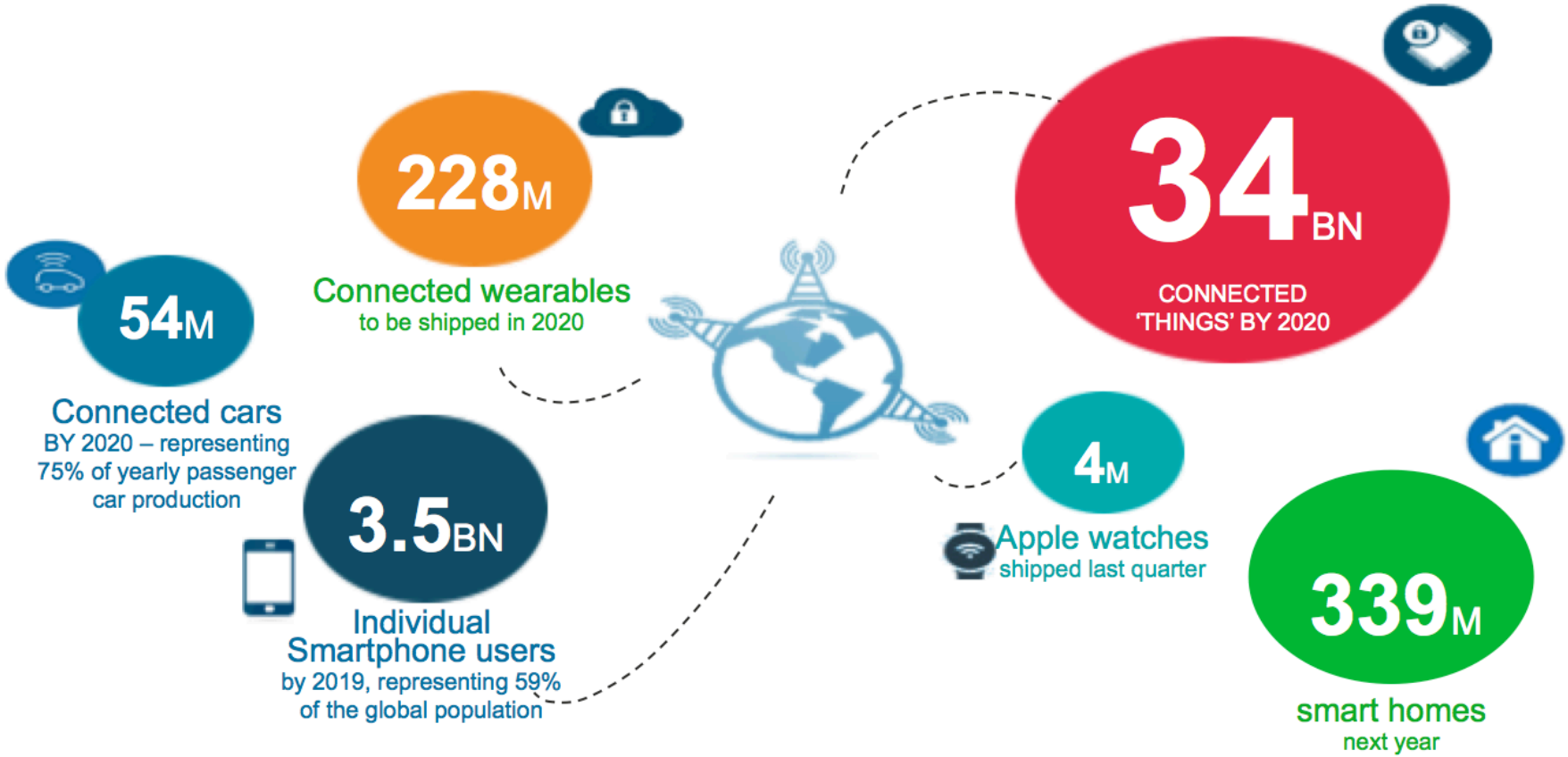
Source: SRI Consulting Business Intelligence

Expected IoT Device Connectivity

https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
(March 20, 2017)



IoT Landscape



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

Challenges in IoT

- Heterogeneous stakeholders
  - Private end-users
  - Public end-users
- Different devices and data formats
  - Autonomic and intelligent devices (robots, actors, alarm & control system)
  - Dump devices (RFID-Tag, light sensors)
  - Smart devices (wearables, smartphones)
  - Embedded devices (in fridge, machines, cars)
- Different communication patterns
  - Human-to-Machine
  - Machine-to-Analytic, Machine-to-Machine
  - Machine-to-Data-Lake
  - Machine-to-Process

Research Problem Statement

- Different definitions/understanding of the term IoT, including security and privacy support, but in common:

  IoT devices communicate via Internet

- Existing solutions for security, privacy, and trust are
  - Either high supported by the architecture and network structure
    → User-unfriendly, technical drawbacks
  - Or supported to a limited extent or not realized at all
    → Contradict the user‘s request for controlling information disclosure in
    a secure and/or trustworthy manner
- Collected data includes information allowing profiling

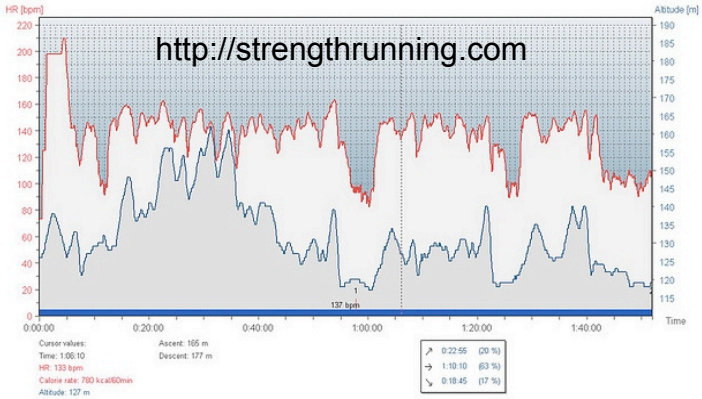
IoT Profiling Sports

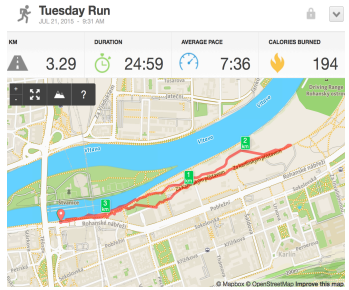
Data collection

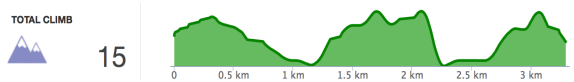
http://running.competitor.com

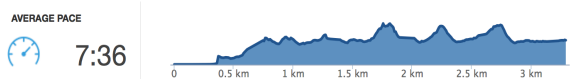
Upload to IoT Service

Profiling





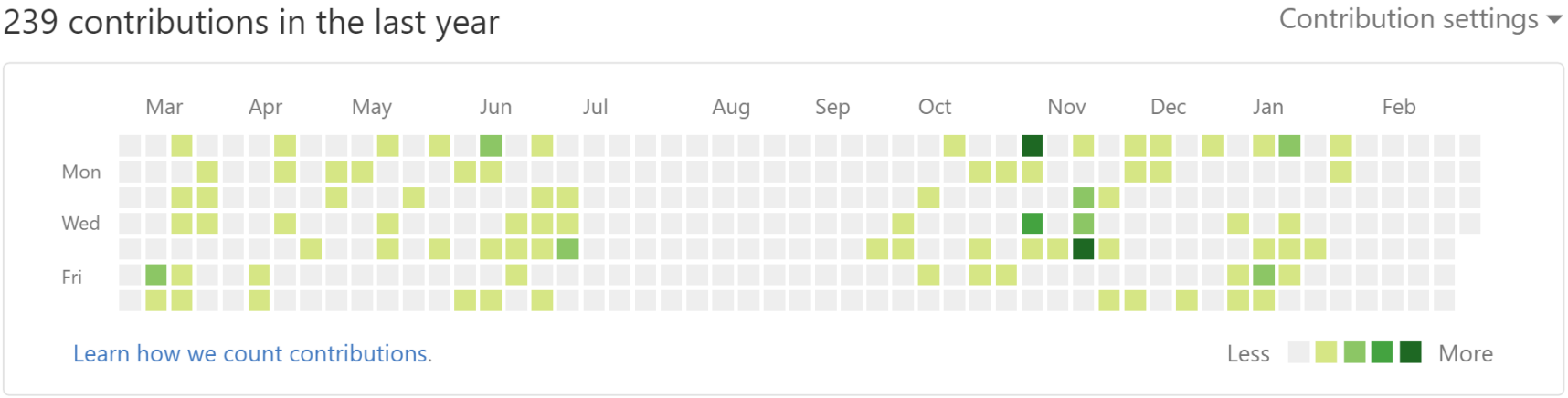


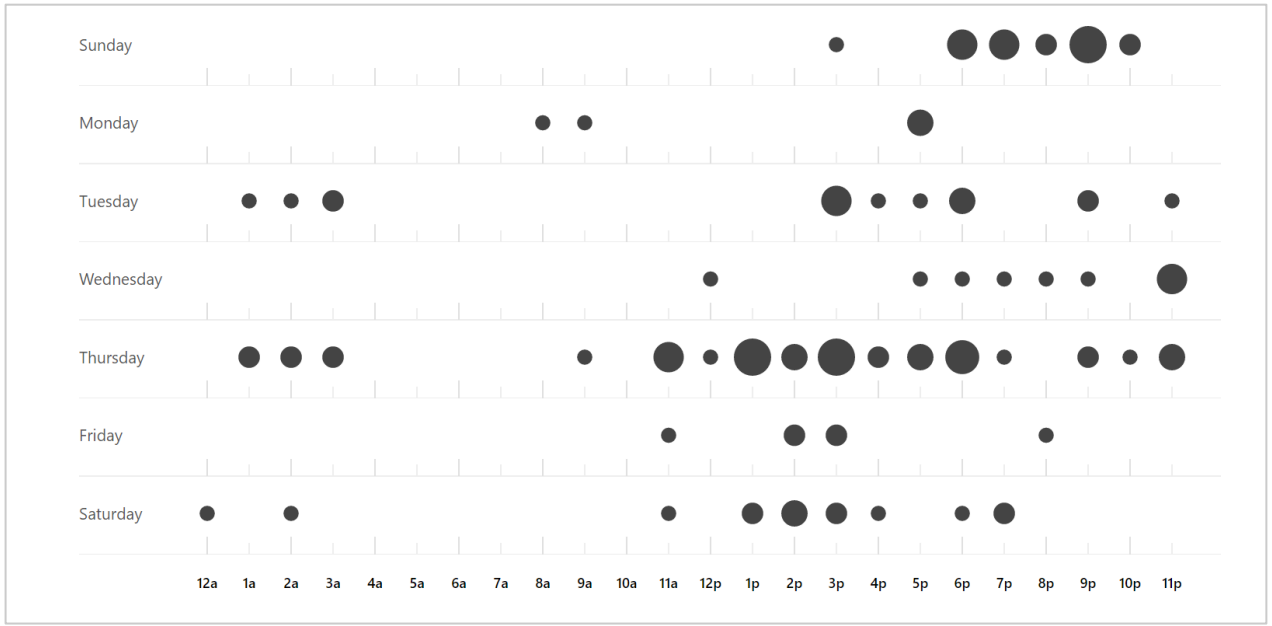


Splits

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

IoT Profiling – Business





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
- Information of working activity
  - Data transfer, data amount
- But also brings dangerous aspects with
  - Prediction of preferred track or working times
  - Prediction of breaks
  - Prediction of data flows using Internet

→ 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!

Gaining Trust

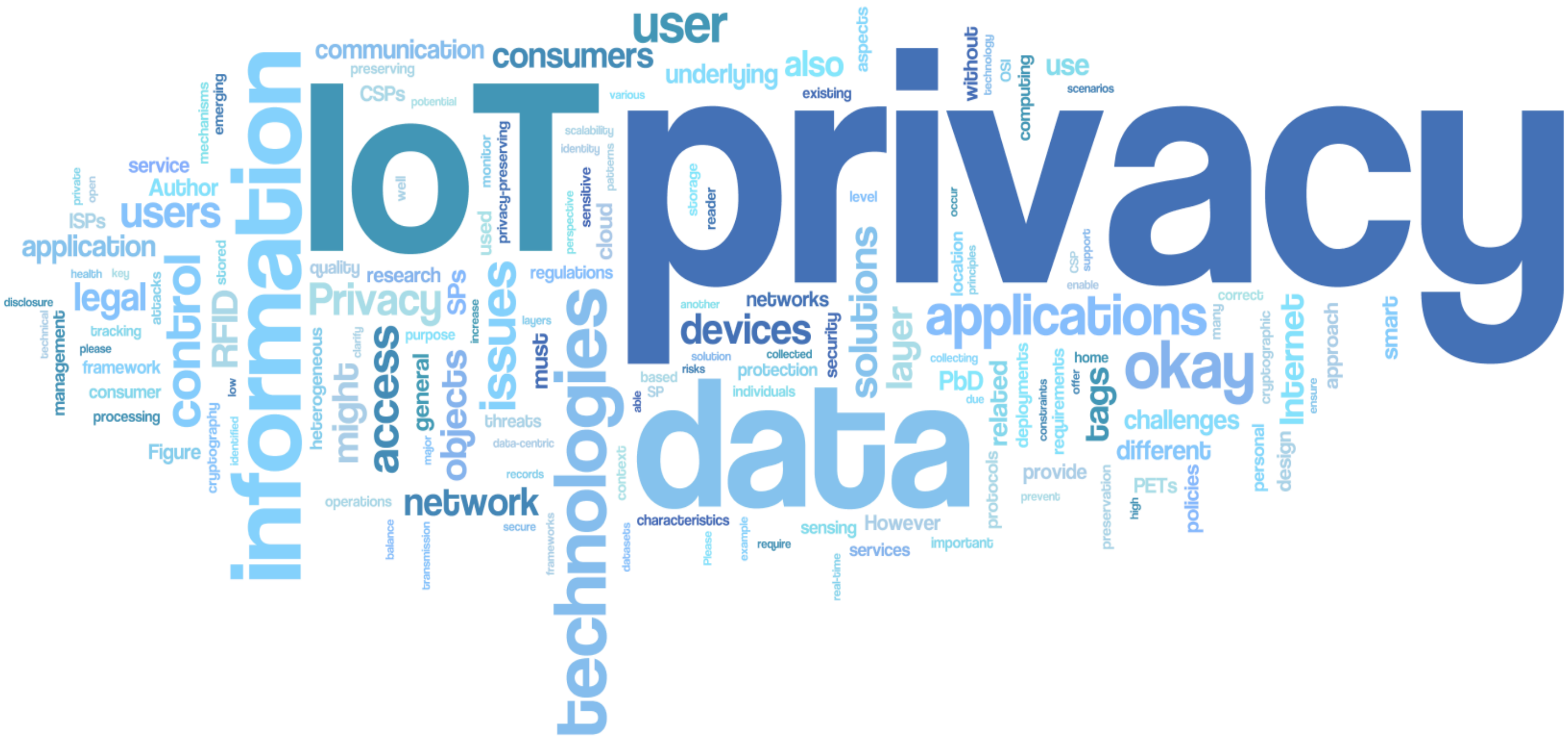
- Security + Privacy = Indication for trustworthiness of a service

- **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

→ Better: Security + **Privacy** + Transparency

The Quest for Privacy



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.

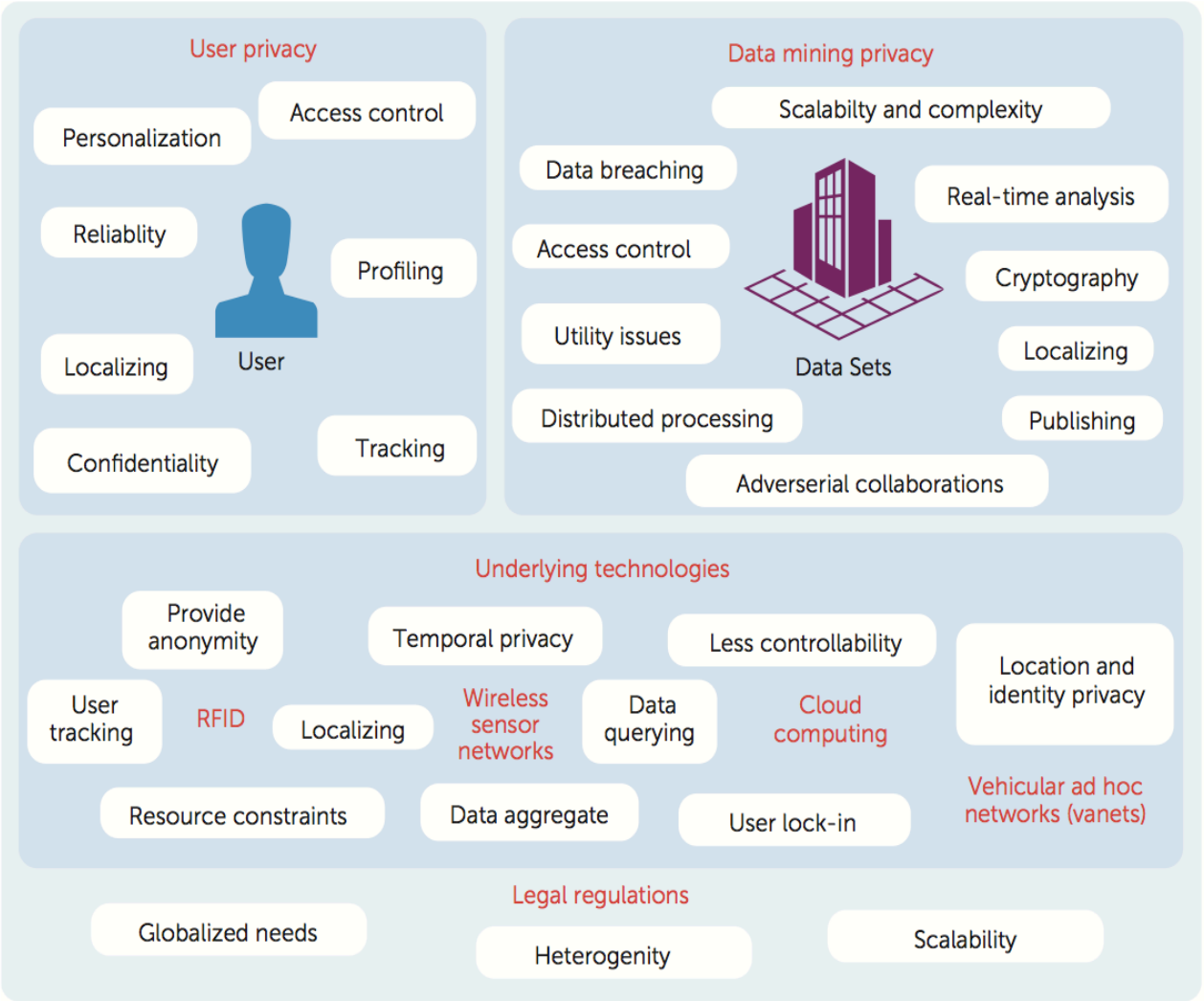
IoT Applications and Privacy Concerns (2)

- 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

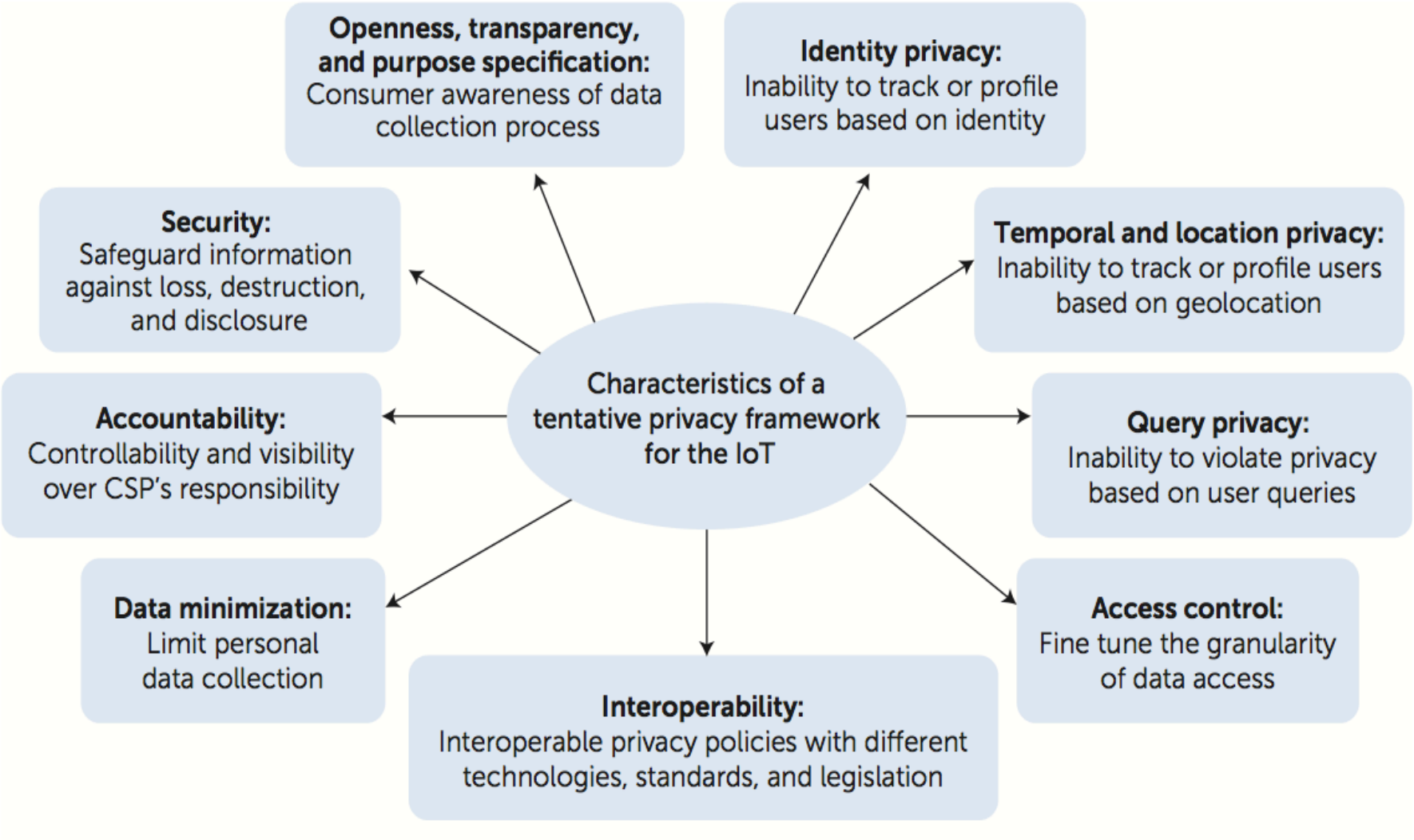
- Privacy is a compliance issue sitting at the intersection of social norms, human rights, and legal mandates

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

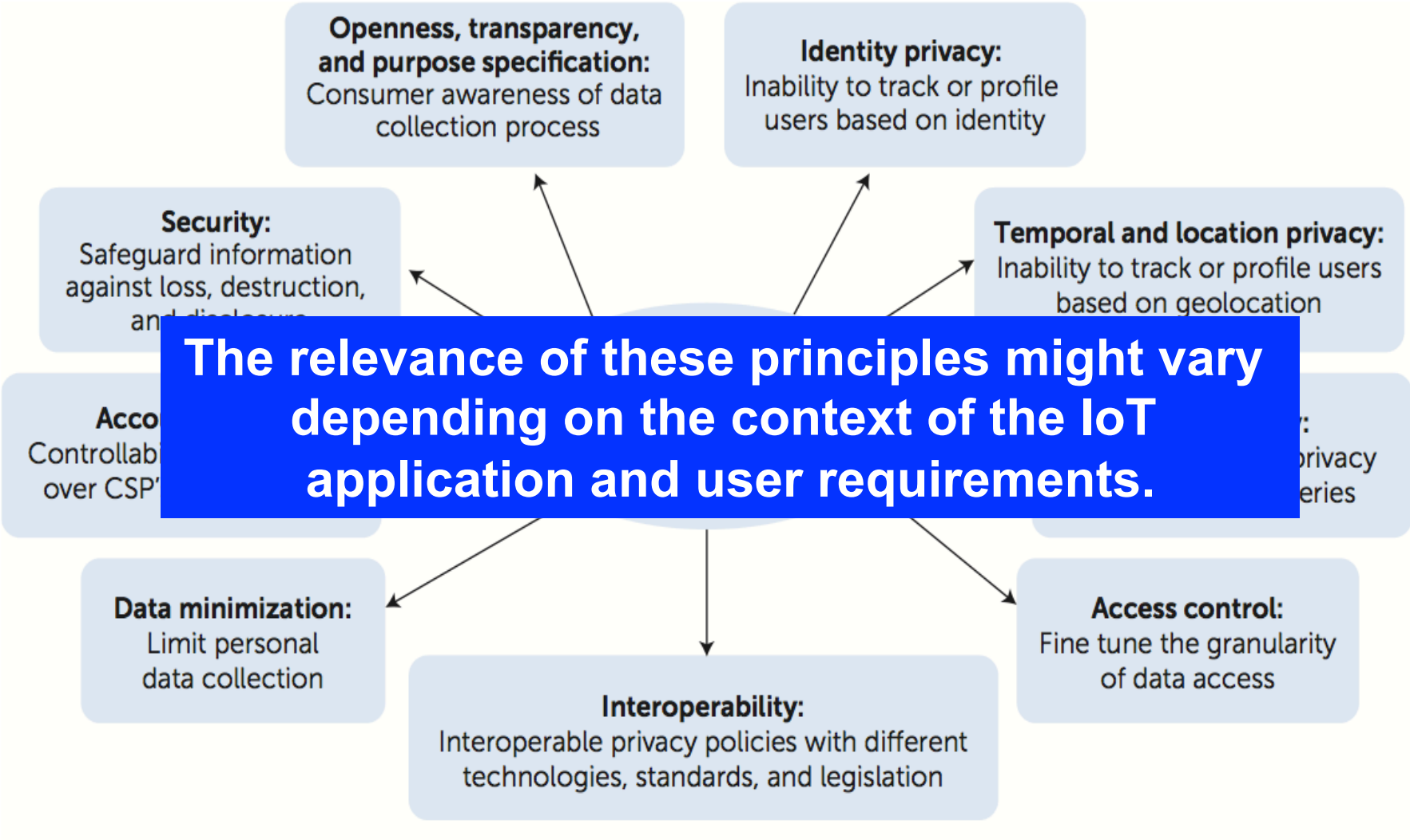
→ Collaboration of governmental & private organizations

→ Strong legal framework

IoT Privacy Framework Characteristics



IoT Privacy Framework Characteristics



Conclusions

- Privacy becomes more and more relevant
- User awareness grows

- Key areas to work on
  - Security, transparency, access control, key management, 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

→ Privacy support is a MUST

→ Acceptance of IoT connectivity and eServices grows

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