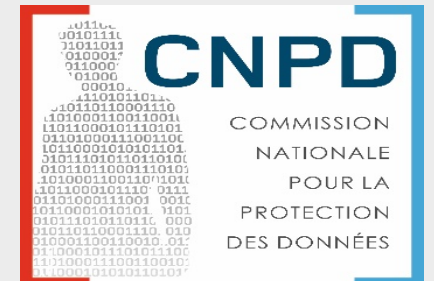# Data protection challenges in the IoT

Université du Luxembourg

4th May 2018

Alain Herrmann

Responsable Services certifications / Violation de données

Internet of Things: Definition

"The concept of the Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices – "things" as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities. "

(Article 29 - Opinion 8/2014 on the on Recent Developments on the Internet of Things)

IoT and personal data
(non-exhaustive list)

Healthcare: wearables and connected medical devices that enable remote health monitoring • Sensitive data • High impact on individuals	**Connected vehicules** • Tracking movement	**Connected toys** • Could reveal sensitive information • Children's data	**Voice assistant** • Profiling • Could reveal sensitive information • Biometric authentication
Smartmetering • Third party apps / services: tracking / profiling at your home	**SmartHome** • Third party apps / services: tracking / profiling at your home	**Smartbuildings**	**Smartcities** • Tracking movement • Freedom of movement

Applicable legislation

General data protection regulation (GDPR – EU 2016/679)

- Projet de loi n° 7184 portant création de la Commission nationale pour la protection des données et la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27avril 2016

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive)

- Loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques

2019 / 2020 ? : ePrivacy regulation

- Proposal for a Regulation on Privacy and Electronic Communications (https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications)

Applicable legislation

ePrivacy:

- protection of fundamental rights and freedom: respect for private life, confidentiality of communications, protection of personal data in the electronic communications sector.

Main points:

➢ Includes Over-The-Top (OTT) providers;

➢ Covers content and associated metadata;

➢ Consent for tracking;

➢ Covers machine-to-machine interaction;

➢ Protection of terminal equipment;

EU Digital Single Market Strategy

Objective:

➤ to increase trust in and the security of digital services

✓ GDPR: one key point

✓ Review of "ePrivacy Directive"

➤ Objective: to provide a high level of privacy protection for users of electronic communications services and a level playing field for all market players

➤ Need for consistency with the GDPR

Typical IoT Components

Figure 1—Typical IoT Components

Source: S. Subramanian and B. Swaminathan
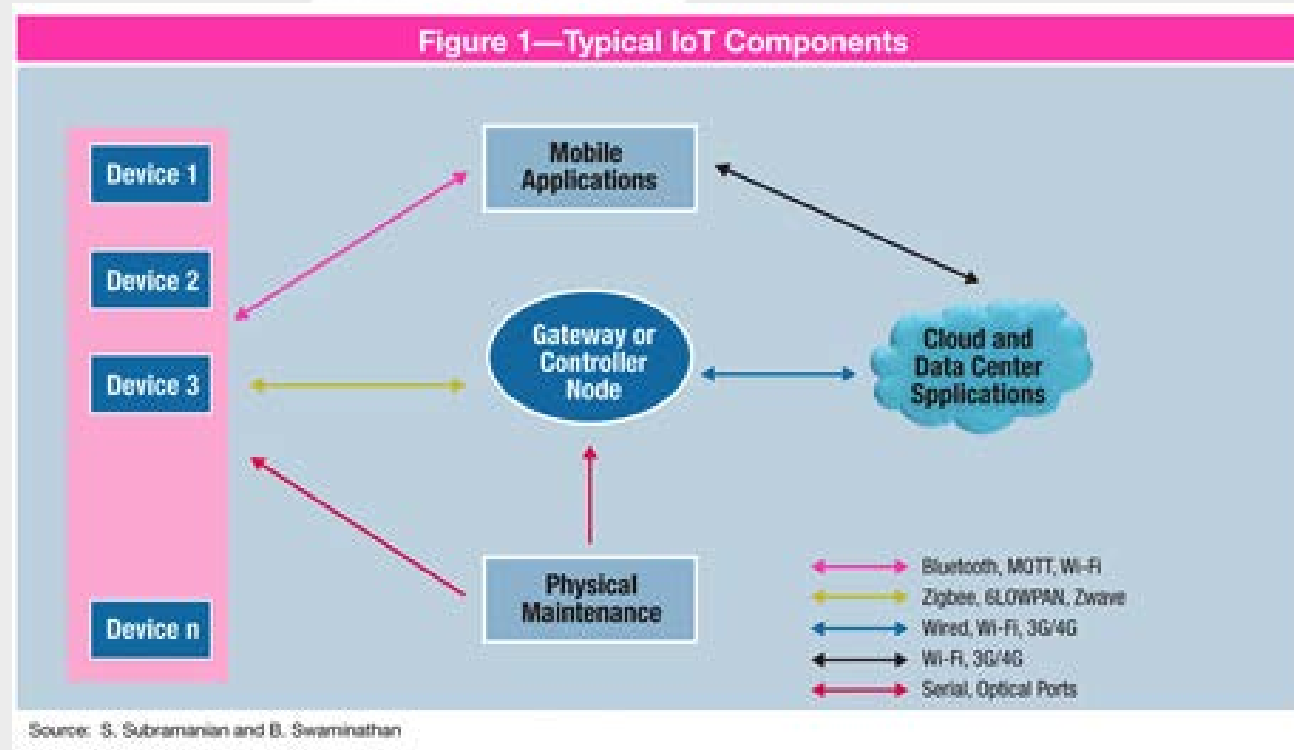
➤ Significant number of stakeholders: manufacturers, data aggregators or brokers, application developers, social platforms, device lenders or renders,…

➤ Multiple communication protocols: poor security for some of them

Privacy and data protection challenges

Complex mesh of stakeholders involved

(necessity of a precise allocation of legal responsibilities)

- Device manufacturers:
  - Develop OS / installed software (determining functionality, data and frequency of collection, when and to whom data are transmitted for which purposes)
- Social platforms:
  - Determine purposes for data "pushed" by DS
- Third party application developers:
  - Many sensors expose APIs
  - App developers can have access to the data through the API from an installed software
  - Consent to be obtained from users: clear, specific and informed (not often the case)
- IoT Data Platforms:
  - Storage of the collected data
  - Data platform owner: usage of data for other purposes?
- Processing of data from non-users:
  - Wearable devices like smart glasses are likely to collect data about other data subjects

Privacy and data protection challenges

Lack of control and information asymmetry

- Users under third-party monitoring
- Dissemination of the user's data
- Excessive self-exposure
- Connection between objects can be triggered automatically (without the individual being aware of it)

Quality of the user's consent

- Users may not be aware of the data processing carried out by specific objects
- Classical mechanisms used to obtain individual's consent may be difficult to apply in IoT
  - "low-quality": lack of information + impossible to provide a fine-tuned consent

Inferences derived from data and repurposing of original processing

Privacy and data protection challenges

Application of the article 5(3) of the e-Privacy directive:

- Access / storage of data on the user's "terminal equipment
- User's consent needs to be obtained before accessing device information + clear and comprehensive information => it can be technically challenging

IoT as sensors are mostly designed to be non-obtrusive (as invisible as possible)

- Risk to the fairness principle

IoT and Security

Challenges:

➢Security vs efficiency: lack of computing power to implement efficient security measures

➢Security of communication protocols poorly designed

➢Incapacity of updating vulnerabilities in a device

Some recommandations

Privacy impact assessments should be carried out before the launch of any new application;

Raw data should be deleted as soon as data required for processing has been extracted;

The principles of Privacy by Design and Privacy by Default should be applied;

Some recommandations

Data users and subjects should be "in control" – they should be able to determine how their data is used;

Information about the processing should be given in a user-friendly manner; and
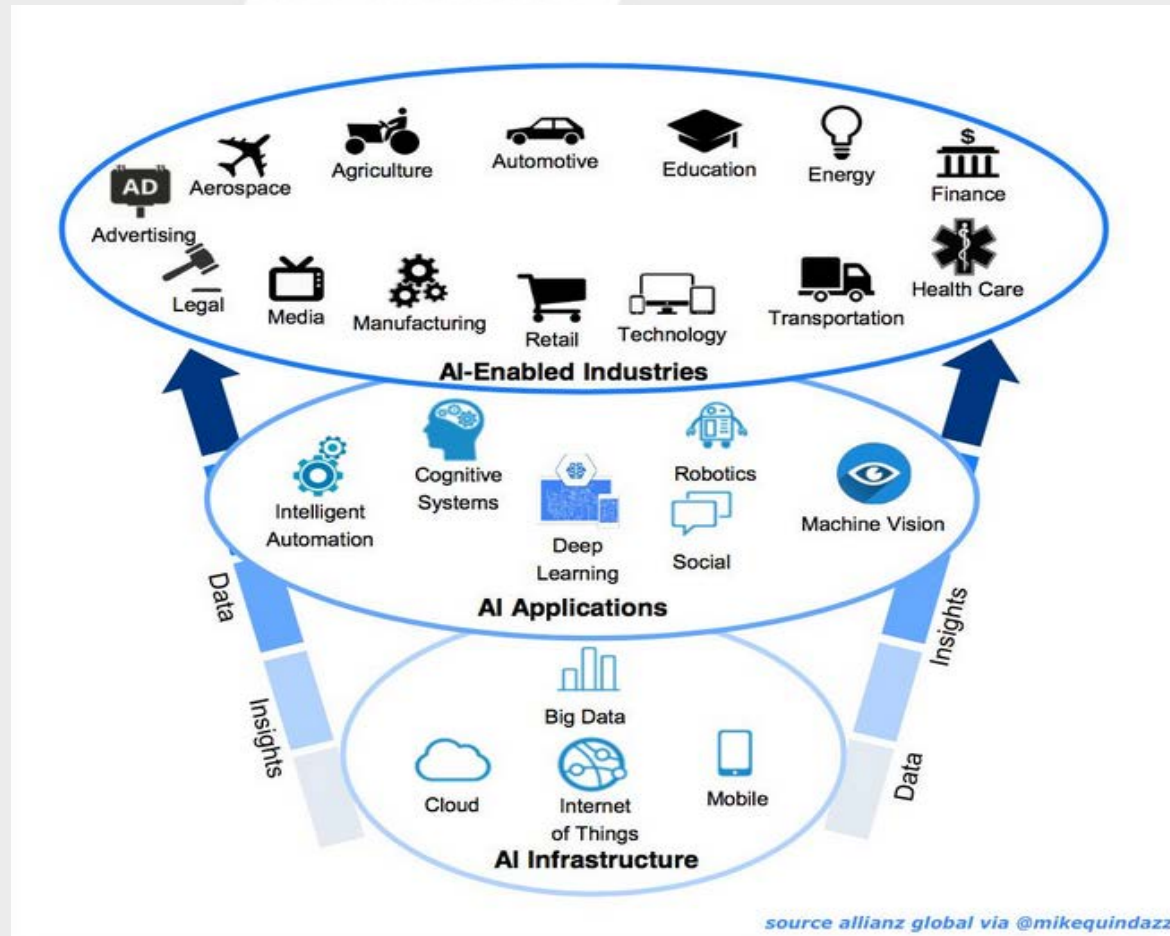
Consent must be explicit, informed and freely given and users should have the opportunity to withdraw it.

Some recommandations

Privacy Proxies

Sticky Policies

Work towards standards

IoT and AI
and cloud, big data, mobile…

source allianz global via @mikequindazzi

- IoT becomes "intelligent" with decision-making autonomy

Thank you for your attention.

Questions?