Data protection challenges in the IoT

IOT Forum - Aarhus
20\(^{th}\) June 2019

Alain Herrmann
Responsible Units certifications / Data Breach
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 vehicles
- 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)


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;
Typical IoT Components

- 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
Some recommendations

- Privacy impact assessments should be carried out before the launch of any new application;
- The principles of Privacy by Design and Privacy by Default should be applied;
- Raw data should be deleted as soon as data required for processing has been extracted;
Some recommendations

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.
• IoT becomes “intelligent” with decision-making autonomy
Thank you for your attention.