The Future of IoT: Toward More Secure and Human-Centered Devices

Marit Hansen
Data Protection Commissioner
Schleswig-Holstein, Germany

IGF
Berlin, 27 November 2019

Setting of ULD

- Data Protection Authority (DPA) for both the public and private sector
- Also responsible for freedom of information

Source: en.wikipedia.org/wiki/Schleswig-Holstein
Source: www.maps-for-free.com
Overview

1. Privacy and data protection
2. Risk according to the GDPR
3. Protection goals
4. Reality check: current IoT implementation?
5. Demands for future IoT

The Future of IoT: Privacy and Data Protection

Imbalance in power ⇦
data protection necessary

Important: Perspective of the individual

The Future of IoT: Privacy and Data Protection
**Data protection: rights of individuals**

*Article 1*

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

**General Data Protection Regulation (EU) 2016/679**

---

**Rights and freedoms of natural persons**

EU Charter of Fundamental Rights

- Art. 7 Respect for private and family life (privacy)
- Art. 8 Protection of personal data (data protection)

Processing of data is interference:
- Must be justified
- Interference must be as minimal as possible

- Article 11: Freedom of speech
- Article 12: Freedom of assembly
- Article 21: Non-discrimination
- And others
Overview

1. Privacy and data protection

2. Risk according to the GDPR
   General Data Protection Regulation (EU) 2016/679

3. Protection goals

4. Reality check: current IoT implementation?

5. Demands for future IoT

The Future of IoT: Privacy and Data Protection

Not just any risk

Recital 75 of the GDPR

75. The risk to the rights and freedoms of natural persons of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated; in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles, where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.
• Risk sources
  - processor/ controller
  - third parties (IT security)
  - adverse events (safety)

• Risk = severity of potential damage x likelihood
• But cannot be quantified
• Can be approximated objectively

• Risk for rights must be mitigated with technical and organisational measures, etc. to protect rights
  → Arts 24, 25, 32, 35 GDPR
**Overview**

1. Privacy and data protection
2. Risk according to the GDPR
3. Protection goals
4. Reality check: current IoT implementation?
5. Demands for future IoT

**Protection goals: more than IT security**

- Confidentiality
- Unlinkability
- Intervenability
- Transparency
- Availability

*Classical IT security protection goals*

*) From the data subject’s perspective
How to implement?

Unlinkability
Separation of domains, separation of power, purpose binding

Transparency
Objective: awareness, understanding and control; different media, support by technology

Intervenability
E.g. opt-out, complaints, judicial relief, reversing decisions ... deactivating sensors and data processing, defined help desk ...

Objective: risk mitigation - i.e. of the risk for the rights and freedoms of natural persons

Overview

1. Privacy and data protection
2. Risk according to the GDPR
3. Protection goals
4. Reality check: current IoT implementation?
5. Demands for future IoT
**IoT + Big Data (+ AI)**

- Everything can communicate with everything
- Everything produces data trails
- Naïve implementation: everything is linkable

- Range of key questions:
  - Personal data or non-personal data?
  - Accumulation of non-personal data still non-personal data?
  - Risks? (more than indiv. privacy)
  - Who is in control?

**Art. 25 GDPR:**
Data Protection by Design and by Default

Anonymisation, pseudonymisation (e.g. attribute-based credentials), early erasure, encryption, access control...

**Smart Cities - personal data?**

Connection Cars Can Build A Better Map

Use your connected vehicles to maintain, improve and augment the navigation map and content layers

Smart Cities - personal data?

http://cloudmade.com/solutions/car-driver-analytics

Connected cars as WiFi Access Points, can be tracked

**Smart Home: Who is in control?**

Best starting point: Unlinkability

[Image: geralt via Pixabay]

---

**The Future of IoT: Privacy and Data Protection**

---

**Smart Cities: Who is in control?**

Best starting point: Unlinkability

[Image: geralt via Pixabay]
**IoT: ubiquitous sensors**

“Asking the user” wouldn’t work; consequences when deactivating sensors?

---

**Not to forget:**

*Tech Abuse in Smart Environments*

---

The Future of IoT: Privacy and Data Protection
Not to forget:
Tech Abuse in Smart Environments

Overview

1. Privacy and data protection
2. Risk according to the GDPR
3. Protection goals
4. Reality check: current IoT implementation?
5. Demands for future IoT

Photo: Ashtyn Renee
Unter CC BY 2.0-Lizenz
https://creativecommons.org/licenses/by/2.0/
Demands for future IoT

- Data protection by design and by default
  - Demanded by the GDPR
  - Thereby to be demanded by controllers

- Liability of manufacturers?

- Current IoT
  - Not only teething trouble!
  - Obviously insufficient incentives to do it right
  - Innovation with data protection should conquer ignorant or even privacy-invasive services