Are tracking and surveillance unavoidable in the Internet of Things?

Achim Klabunde
Head of Sector IT Policy
EDPS
ISACA Valencia 28 October 2016
1. Who we are
2. The Problem
3. The Law
4. The Challenge
The EDPS

The EU’s independent data protection authority
The work of the EDPS: Who we are, what we do and how we do it...
What is “personal data”? 

• any information relating to an identified or identifiable natural person (data subject); 
• an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

Art. 2(a) Reg. 45/2001
The European Data Protection Supervisor: an independent institution responsible for ensuring the protection of personal data by the EU institutions and bodies.
The EDPS

1. **Supervise** data processing done by EU institutions and bodies;
2. **Advise** the EU legislator and appear before the EU courts;
3. **Monitor** new technologies with an impact on privacy;
4. **Cooperate** with other supervisory data protection authorities.
Appendix 2 of the Guidelines contains a sample on-the-spot data protection notice:

[Insert your video-surveillance pictogram: you may consider, for example, the ISO pictogram or the pictogram customarily used where you are located.]

For your safety and security, this building and its immediate vicinity is under video-surveillance. No images are recorded. [Alternative: The recordings are retained for 48 hours.]

For further information, please consult www.domainnameofyourinstitution/cctv or contact the Agency’s security unit at [telephone number and email address].

[Include multiple language versions when applicable.]
Technology & law in the EU

- Hessen (Germany): 1st data protection law in Europe
- France: 1st EU Member State to have data protection law + DPA
- Council of Europe: Convention 108
- UK Computer Misuse Act
- Directive 95/46

Timeline:
- 1970: Hessen (Germany)
- 1978: France: 1st EU Member State to have data protection law + DPA
- 1981: Council of Europe: Convention 108
- 1990
- 1995
The Problem
"Surveillance is the business model of the Internet. We build systems that spy on people in exchange for services. Corporations call it marketing."

Photograph by Rama, Wikimedia Commons, Cc-by-sa-2.0-fr
Challenges to Privacy

A HELPFUL VENN DIAGRAM
The next DDOS attack

... The ‘S’ in ‘IoT’ is for Security
Growth expectations

212BB Connected Devices by 2020

- **MOBILE DEVICES**
- **IoT DEVICES** *IDC
- **IoT DEVICES** *Cisco
Sensitive data collection
The Law
Article 25

Data protection by Design and by Default (…) the controller shall (…) implement appropriate technical and organisational measures (…), which are designed to implement data-protection principles (…) in order to meet the requirements of this Regulation and protect the rights of data subjects.
GDPR Recital 78:

... the controller should adopt **internal policies and implement measures** which meet ... the principles of data protection by design and ... by default. (examples) ... producers of the products, services and applications should be encouraged to take into account the right to data protection .... The principles ... should also be taken into consideration in the context of public tenders.
The Challenge
Data Protection Authorities

- Article 29 WP Opinion 02/2013 on apps on smart devices - WP 202
- Article 29 WP Opinion 8/2014 on the Recent Developments on the Internet of Things - WP223
- EDPS Opinion of 21 May 2015 on Mobile Health - Reconciling technological innovation with data protection
Data Protection Authorities

Tracking in Public Spaces

The use of tracking technologies in public spaces is on the rise. This has adverse consequences for the right to privacy and may in some cases be unlawful.

https://www.datatilsynet.no/English/Publications/tracking-in-public-spaces/
Data Protection Authorities

Privacy information falls short in mobile health devices
(Published: 19.10.2016)

The Norwegian Data Protection Authority has checked how six different devices that helps you measure your health vitals communicate privacy related matters to their customers.
https://www.datatilsynet.no/English/Publications/privacy-in-mobile-health-devices/
The Challenge

In real-life development, existing building blocks are used and reused as they are available, often designed without privacy in mind. Developers do not have time and resources to re-develop existing tools, and poor privacy propagates into new applications. Even new mistakes may be added due to lack of detailed knowledge of the tools.
Privacy and security must become design goals for IoT (and other) devices at all levels:

- Protocols
- Operating systems
- HW
- User interfaces
- Applications
IPEN Action Points

- Developers’ cookbook
- Funding for privacy
- Bridge between lawyers and techies
- Resource list
- Local IPEN groups
Thank you!

For more information
www.edps.europa.eu
@EU_EDPS
edps@edps.europa.eu
@achimkla