eHealth and Smart Home Data Protection

Peter Wintlev-Jensen
DG CONNECT- E4 Internet of Things Unit
European Commission
The potential is enormous

Data-driven innovation

Prevention and early risk detection  New therapies and diagnostics  Personalised Medicine  New health and care models

High-performance computing  Artificial Intelligence  Cloud computing  4G/5G  Internet of Things (IoT)

Advanced Data-Analytics  Wearables  Telehealth

Smart Appliances  Smart Media  Air Control

Lights & Curtain  Video Intercom  Background Music

Central AC  Safeguard  Central Heating
But major security/privacy risks
Main EU Security/Privacy Policy Framework

**General Data Protection Regulation (GDPR)**
EU regulation setting out the rules for protection of personal data across the EU.

**Network & Information Security Directive NIS + Cyber Security Act**

**EU Blockchain Observatory and Forum**
Highlight key developments of the blockchain technology, promote European actors and reinforce European engagement.

**EiDAS Regulation**
Electronic identification and trust services for electronic transactions Mutual recognition of electronic signatures.

**ePrivacy proposal**
EU proposal setting out the rules for privacy in electronic communications.
Main GDPR Principles

- Lawfulness, fairness and transparency
- Storage limitation
- Purpose limitation
- Integrity and confidentiality
- Data minimisation
- Account ability
- Accuracy

Privacy by design & by default
Automated decision making & profiling

WP29 Opinion 8/2014 on Internet of Things

WP29 Guidelines on Automated individual decision-making and Profiling (wp251rev.01) 13/02/2018

"Whenever I walk in a room, everyone ignores me."
WP29 Opinion

General Guidelines
- Privacy Impact Assessments
- Early data aggregation
- Privacy by Design/Default Principle
- User Empowerment

OS/Device Manufacturers
- Inform about data collected
- Granular choices
- Minimise tracking and inform about security risks
- User access to data in standard data formats

Application Developers
- Facilitate users exercise of rights to data access, delete, transfer
- Apply data minimisation principle

Social Platforms based on IoT
- Ask users to review, edit and decide on information generated by their device before publication on social platforms
- Information published by IoT devices on social platforms should, by default, not become public or be indexed by search engines

IoT Device Owners/Additional recipients
- Consent to the use of a connected device and to the resulting data processing must be informed and freely given
- Users should not be economically penalised or have degraded access if they decide not to use the device or a specific service
- The data subject whose data is being processed in the context of a contractual relationship with the user of a connected device (i.e. hotel, health insurance or a car renter) should be in a position to administrate the device.

Standards Bodies/Platforms
- Promote portable and interoperable as well as clear and self-explanatory data formats
- Not only focus on the format for raw data but also on the emergence of formats for aggregated data
- Promote data formats that contain as few strong identifiers as possible in order to facilitate the proper anonymisation of IoT data
- Work on certified standards that would set the baseline for security and privacy safeguards for data subjects
- Develop lightweight encryption and communication protocols adapted to the specificities of IoT
Relevant EU IoT Activities

- **Large Scale Pilots under Horizon 2020**
  - Workshop on experience on GDPR compliance planned
  - Contributing to privacy by design and standards experience
  - Further pilots launching in 2019

- **New cluster of IoT security/privacy projects launched**
  - Blockchain/DLTs

- **AIOTI WG3 on standardisation**

- **ENISA planning to look at IoT trust**

- **FP9/Next Generation Internet**
Further Information

- **EU Activities on IoT**

- **General Data Protection Regulation**

- **Network and Information Security Directive**

- **ePrivacy proposal**

- **EU Blockchain Observatory**