Data privacy and security in smart meters

How to face this challenge?

Monika Štajnarová

beuc

Workshop on

Regulatory aspects of data transmission, data security and data protection in relation to smart metering

Florence

26th November 2010

BEUC ? BERRK ? BEUIK ?

European Consumers' Organisation:

- **1962**: Established by
  6 consumer organisations

- **2010**: 44 independent national consumer organisations
  from 31 European countries
  (EU, EEA and applicant countries)

www.beuc.eu

Smart metering

- From business of mechanical devices and manual labour towards smart technologies and new functionalities;
- Worldwide deployment of SM (in electricity) will reach 302 mil. by 2015 *(Berg Insight);*
- EU strategy – 3rd Energy package (80% by 2020);
- SM roll-out across the EU: between 133 million to 145 million new smart electricity meters by 2020 => a market worth $25 billion *(Greenbang Research).*

What does it mean for consumers?

Consumers' benefits

- End of estimated and inaccurate bills;
- Access to real-time information about energy use and historical consumption data;
- Lower energy bills;
- Raising consumer awareness;
- Increased consumer choice by products and services available through SM.

Consumers' concerns

- Costs
- Sustainability
- ***Privacy and security***
- Remote disconnection

Privacy and security concerns

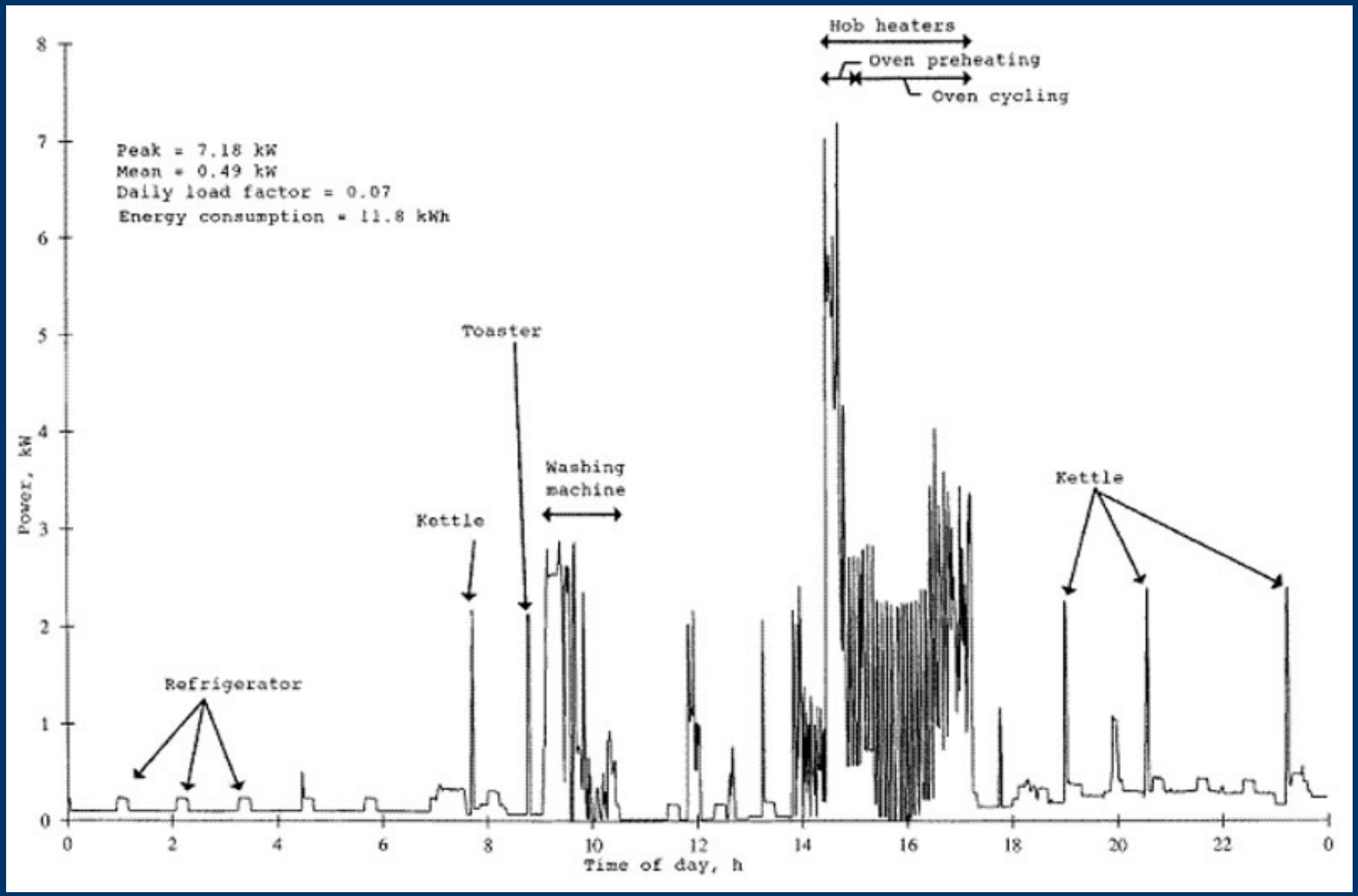
Increasing collection of personal data – real privacy & security concerns:

- ❑ Information proliferation
- ❑ Lax control
- ❑ Insufficient oversight

Library of personal information

(potential risks: targeted marketing, fraud, misuse of information,…)

Consumer profiling



Source: National Institute of Standards and Technology (NIST)

Privacy and security

- Key questions (privacy):
  - How do we ensure that people are not subjected to **unwanted targeting, profiling and marketing activity**?

- Key question (security):
  - How do we protect smart meters and grids against **hackers**? Will relevant **technical standards** be developed in time for their roll-out?

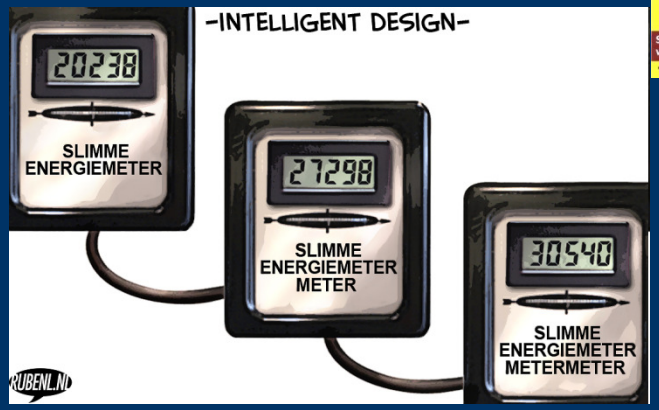
Dutch Case (2008)

The original law proposal (2008)

- ❑ A mandatory roll out in six years, starting 01/01/2009;
- ❑ A consumer duty to accept the smart meter, display in private market;
- ❑ Collection 15 minutes values (E) and hour values (G) for both DSO and supplier;
- ❑ Consumer consent required for sending data to (other) 'third parties'.

According to the Tilburg Institute for Law and Technology (TILT) privacy assessment, the 2008 Dutch smart meter law proposal constituted a violation of Art. 8 ECHR:

1. Generating and passing on of 15 min./ hour values to the DSO
2. Daily values to DSO and supplier
3. Mandatory use



Dutch Case (2010)

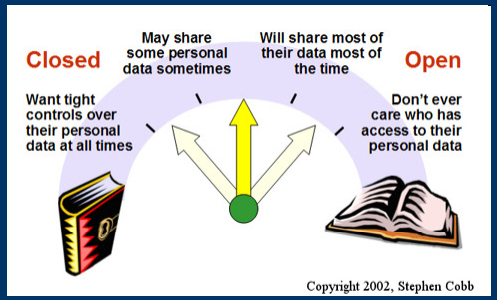
The new Dutch smart metering proposal (2010)

- Voluntary role out
- Consumer choice:
  1. Right to refuse instead of duty to accept;
  2. A smart meter, but no communication;
  3. Standard information (default), 6 times a year.

….and how will be the role of the consumer in smart metering promoted in other countries?

Consumers' perception

- Consumer **trust** is the core issue for successful deployment of smart meters (confidence, satisfaction & engagement);



- Smart meters must be **reliable, secure and under individuals' control**;

- **System security and data protection** are crucial issues for success (smart meters = smart solutions?)

What has to be kept in mind

- **Privacy**
  (what data should be collected and for what purpose, who owns and deals with the data, frequency of the meter readings, what data to be exported out of the smart meter)
- **End-to-end security**
  (technical and legal measures to ensure security, responsibility of the data security, sanctions)
- **“Future proof”**
  (complete system to cope with changes and future challenges)

There are known knowns. There are known unknowns.
But there are also unknown unknowns.
(Donald Rumsfeld)

Privacy by design

Making privacy the default

To significantly minimise the risks and to secure users' willingness to rely on smart meters, it is crucial to integrate, at practical level, **data protection and privacy from the very inception** of the Smart Metering Project and at all stages of its development.

- The importance of privacy by design during the implementation of **data minimisation** principle which ensures the safe disposal of data and the limitation of data retention.

- Using **privacy-enhancing technologies** (cryptography)

Privacy by design

7 Foundational Principles:

I. Proactive not Reactive; Preventative not Remedial;
II. Privacy as the Default;
III. Privacy Embedded into Design;
IV. Full Functionality (Positive-Sum, not Zero-Sum);
V. End-to-End Security: Lifecycle Protection;
VI. Visibility and Transparency;
VII. Respect for User Privacy.

Source: www.ipc.on.ca

Data protection

- Data Protection Directive
- European Convention on Human Rights
  (Article 8 – Right to respect for private and family life)
- Existing legislation at national level
- Guidelines for EU Member States ensuring privacy and data protection
- Recommendation of Task Force Smart Grids & Smart Meters - Expert Group 2

Way forward

- Privacy impact analysis on all aspects of smart meters;
- Privacy by design to protect consumers by making privacy the default in the SM design;
- Communication with consumers (consumer consent)

Thank you for your attention

More information on www.beuc.eu

📖 EC transparency register: identification number 9505781573-45 📖