Privacy by design in smart energy

kjetil.rommetveit@uib.no

Kjetil Rommetveit
Centre for the study of the sciences and humanities
University of Bergen, Norway

IFIP summer school, Milano 3 – 8 september 2017
• ‘smart technologies’, including energy and health

• Integration of social science, humanistic and legal perspectives into smart technologies and environments

• trying to provide concrete experience and advice;
• analysing developments theoretically

Together with: Alessia Tanas, Niels van Dijk, Charles Raab, Katja de Vries
• Mapping central documents, regulatory and academic

• Consulting with practitioners: lawyers, citizens, engineers, impact assessors...

• What happens as engineers and software designers interact with legal practitioners: are the boundaries between these practices erased or re-inforced? How do they change?

• Basic conceptual move: ‘design’ is also social, institutional and political
Structure of talk

• PbD in smart metering: infrastructural development across institutional and disciplinary boundaries

• The Dutch introduction of smart metering

• Networks: a) Privacy engineering; b) Regulatory; c) Legal; d) civic society

• Summing up:

Infrastructure and collaboration across institutional domains and boundaries. Questions and problems
Large scale sociotechnical systems and infrastructures: smart grid

• “A Smart Grid is an electricity network that can cost **efficiently** integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both” (EC: Smart Grid Task Force Mandate, 2011)
smart metering policies

- opens up new markets for industry, whose vision and interests underpin the agenda from the outset

- markets (or industry) cannot act alone. They solicit help from other actors, significantly technology, law and regulation

- enabled through technical possibility: renewables, two-way communication, improved efficiency and controls with load distributions, etc.

- grounded in an already-established legal framework (the 2009 Energy Directive), and triggers legislation and regulations at EU and national levels

- privacy and data protection are not add-ons, but main essential components of emerging infrastructure(s)
In 30 seconden minder energiekosten?
Schrijf je in voor de Energiestaster?

Slimme energiemeter in strijd met EVRM

Geschrven op 12 november 2008

De invoering van de slimme energiemeter is in strijd met het Europees Verdrag van de Rechten van de Mens. Tot deze conclusie komt de Universiteit van Tilburg die in opdracht van de Consumentenbond een privacytoets uitvoerde. De bond roept de Eerste Kamer op het wetsvoorstel 'slimme meters' af te wijzen, zodat de minister Van der Hoeven van Economische Zaken een beter voorstel moet doen. Op www.consumentenbond.nl kan de hele privacytoets van de Universiteit van Tilburg worden gedownload.
The importance of security, rights and freedoms for regulation

- "The electric grid is different from RFID's: it's a huge challenge, for both state and industry (interactions); **one better get it right**" (EDPR representative, Epinet project workshop)

- Fixing the problem afterwards may be very expensive and time consuming (if at all possible)

- In line with developments over the last 20 years towards ‘upstream’ anticipatory and precautionary governance

- Stabilising expectations of highly different actors
The Dutch case

• Smart meters discussed in a regulatory context in the Netherlands since around 2004, gained traction around 2006

• primarily driven forward by the Ministry of Economic Affairs, with support from the Dutch Standardisation Institute

• Dutch first chamber: the bill was contested, mainly on privacy grounds

• the bill was rejected and a new legislative proposal requested. The new proposal was accepted into law in 2012, this time with considerable concessions to the public and the consumers
• One can **use the data to monitor individual customers** in order to detect abnormal usage / behavior and **to stop energy from remote** .... Legislative proposals which are now before the Senate, propose the introduction of the 'espionage' meters mandatory for all domestic consumers. **This obviously constitutes an unacceptable violation of people's personal lives whose dangers are obvious.** In addition, the system provides, at a distance of data to be registered, but also the risk that they can be **tapped into by unauthorized persons.** ...

• On November 10, 2008 The Consumers reject the Senate on the bill 'smart meters'. This is because the judgment of Tilburg University, who carried out **a privacy assessment commissioned by the Consumer Association**, stated that: **"The introduction of smart energy meter is contrary to the European Convention on Human Rights (ECHR)"**
Privacy assessment: The triple test of Art. 8 ECHR (Cuijpers and Koops 2012)

- Smart metering data provides insights into people’s general living patterns and goes well beyond informational privacy.

- **Energy privacy**: “…if energy supply can be reduced or completely cut off through the meter, there can even be a restriction in a primary necessity of life, which can constitute an invasion of privacy as well.”

- 1. Does the smart meter interfere with privacy?
- 2. Is the infringement in accordance with the law?
- 3. Does the infringement serve any of the interests mentioned in art. 8(2)?
- 4. **Is the infringement necessary in a democratic society?**
“not (proven to be) necessary in a democratic society”:

- The generation and passing on of quarter-hourly/hourly readings to grid managers
- The daily readings to grid managers and suppliers
- The compulsory roll-out of smart meters to all households
- Questioned necessity of building in a switching function that would enable capacity to be switched on and off remotely, and a signalling function for combating fraud
- Generally: a lack of evidence to underpin the Dutch government’s policies
Outcomes in terms of consumer choice

• 1. No smart meter, hold on to the traditional (‘stupid’) meter

• 2. A smart meter that can be administratively shut down (‘admin off’)

• 3. A smart meter with a standard measurement regime

• 4. A smart meter for which explicit consent is given to read out more data than is allowed under the standard measurement regime
Key lessons (Cuijpers and Koops 2012)

• From the outset, privacy and data protection law must be taken into account as an important requirement for the design of smart metering systems.

• For smart metering, two new obligations can be considered most relevant. Article 23 of the proposed Regulation introduces the principle of **privacy by design and default**.

• In article 33 the popular notion of **Data protection impact assessment** (also known as PIA, Privacy Impact Assessment) is introduced. If data processing operations present specific risks, controllers must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

• The problems could have been avoided through earlier and better interventions.
( ... break ... )
Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
Cavoukian et al. (2010): SmartPrivacy for the Smart Grid

- A win-win system: interests of both large organisations (utilities, grid operators) and citizens/consumers are served

- ‘Without diminishing the benefits of the Smart Grid, it is possible to design privacy directly into the Smart Grid by making it the default ...in all physical, administrative and technological aspects of the system’ (276)

- 7 Privacy by Design Principles
<table>
<thead>
<tr>
<th>Smart Grid</th>
<th>Smart Grid with SmartPrivacy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intelligent</strong>—capable of sensing system overloads and rerouting power to prevent or minimize a potential outage; of working autonomously when conditions require resolution faster than humans can respond and cooperatively in aligning the goals of utilities, consumers and regulators.</td>
<td><strong>Intelligent</strong>—capable of collecting the minimum amount of personal information necessary from consumers, without diminishing the quality and range of services offered. Works transparently with consumers to communicate information regarding the collection, use and disclosure of their personal information. Plans in advance how to protect privacy and security, and builds it into the system in advance of its use.</td>
</tr>
<tr>
<td><strong>Efficient</strong>—capable of meeting increased consumer demand without adding infrastructure.</td>
<td><strong>Efficient</strong>—capable of meeting increased consumer demand without compromising the privacy and security of personal information. Securely disposes of personal information when it is no longer needed for the purpose for which it was originally collected.</td>
</tr>
<tr>
<td><strong>Accommodating</strong>—accepting energy from virtually any fuel source including solar and wind as easily and transparently as coal and natural gas; capable of integrating any and all better ideas and technologies—energy storage technologies, for example—as they are market-proven and ready to come online.</td>
<td><strong>Accommodating</strong>—accepting of a variety of consumer preferences with regards to the use, retention, and disclosure of personal information—makes these options easily accessible to the individual.</td>
</tr>
<tr>
<td><strong>Motivating</strong>—enabling real-time communication between the consumer and utility so consumers can tailor their energy consumption based on individual preferences, like price and/or environmental concerns.</td>
<td><strong>Motivating</strong>—enabling communication and notice between the consumer and utility so that consumers can tailor their personal information options, based on individual preferences. Proactively obtains consent before disclosing any personal information to a third party.</td>
</tr>
<tr>
<td><strong>Opportunistic</strong>—creating new opportunities and markets by means of its ability to capitalize on plug-and-play innovation wherever and whenever appropriate.</td>
<td><strong>Opportunistic</strong>—creating new opportunities and markets by means of its ability to capitalize on privacy-enhancing technologies, wherever and whenever appropriate.</td>
</tr>
<tr>
<td><strong>Quality-focused</strong>—capable of delivering the power quality necessary—free of sags, spikes, disturbances and interruptions—to power our increasingly digital economy and the data center.</td>
<td><strong>Quality-focused</strong>—capable of delivering information that is free of inaccuracies, and allowing individuals to access to their personal information and make any corrections necessary.</td>
</tr>
</tbody>
</table>
(but the authors did not really specify how to do it)
The rubicon of PbD?
from law to engineering

- GDPR ‘could really make a change ... the theory (PbD) is already there, but too few people care ...’ (DPA)

- ‘... for PbD to become common practice a cultural change in engineering practices is necessary’ (By Design practitioner)

- Unfortunately ... there is so far little experience in applying privacy by design in engineering (Hoepman 2014)

- There is still not a unified view on privacy requirements engineering (Beckers 2012, quoted in Notario et al. 2015)

- (are the problems technical or organisational, or perhaps also cultural and political?)
Data Protection and Privacy by Design (GDPR Art. 25)

State of art, cost of implementation, nature, scope and purpose of processing, risks to the rights and freedoms of natural persons

Data protection principles

Technical and organisational measures

Meet the requirements of GDPR and protect the rights of data subjects
• **PIA: objectives and context.** identifying the main threats to data subjects rights and freedoms (incl. stakeholder consultation)

• $likelihood \times magnitude\ of\ threat = quantifiable\ privacy\ risk$ (cf. CNIL, SG Template)

• **Design privacy goals** into architecture: context and objective, privacy and data protection principles, techniques (PETs)...

• Key criteria: trust assumptions, user involvement (not needed for smart metering?), technical constraints. A set of design strategies have been agreed: minimise, hide, separate, aggregate

• Result: *a reduction of design space*

• **Evaluations:** compliance checks, privacy seals, accountability

*express a fundamental structural organisation or schema for software systems* (17 – 18)

Solutions: Technical or organisational? (political? cultural?)
Translating data protection and privacy principles into technical (and organisational) requirements: the strength is the weakness?

- **IT people are good at thinking about risks, but it is usually the risks to the organisation** (DPA, CANDID interview data)

- Risk assessments are mainly limited to an organisational view (Van Dijk et al. 2016, cf. Power 2007)

- Informants express that major obstacles to PbD reside in the organisations/businesses (do not understand their own data flows, have to buy technologies off-the-shelf, usually ill-fitted, too late, do not care, etc.)

- Are the problems mainly technical or organisational? (or something else?)
Good governance

Written by lawyers

They observe that smart metering have strong impacts on privacy as a basic human right

The Dutch (and UK) cases have already demonstrated this in practice
<table>
<thead>
<tr>
<th>Question</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>When are you usually away from home?</td>
<td>Is your household protected with an electronic alarm system? If so, how often do you arm it?</td>
</tr>
<tr>
<td>How often do you arrive home around the time the bars close?</td>
<td>How often do you get a full night’s sleep v. drive sleep deprived?</td>
</tr>
<tr>
<td>How often are you late to work, or rushing to get there on time?</td>
<td>Does the time it takes you to get from your home to your workplace require that you break the speed limit to get there?</td>
</tr>
<tr>
<td>On what days and during what times do you watch TV?</td>
<td>How much home time do you spend in front of your computer?</td>
</tr>
<tr>
<td>How often do you eat in?</td>
<td>Do you tend to eat hot or cold breakfasts?</td>
</tr>
<tr>
<td>What’s the relative frequency of microwave dinners to three-pot feasts?</td>
<td>How often do you entertain?</td>
</tr>
<tr>
<td>Are any of your appliances failing or operating below optimal efficiency?</td>
<td>Do you own lots of gadgets?</td>
</tr>
<tr>
<td>Are you a Laundromat person, or do you have your own washer and drier?</td>
<td>Are you a restless sleeper, getting up frequently throughout the night?</td>
</tr>
<tr>
<td>In a custody battle: Have you ever left your child home alone? How often, and for how long?</td>
<td>In a worker’s compensation hearing: How is it, with your disabled back, you were able to turn on the TV in the upstairs of your home less than a minute after turning off the lights downstairs?</td>
</tr>
<tr>
<td>Alabama recently passed a tax provision requiring obese state employees to pay for their health insurance unless they actively work to reduce their body mass index. So: why haven’t you used your treadmill at home any time in the last week? You clearly have not been out of the house and</td>
<td>Do clinically depressed or bipolar individuals have distinctive energy profiles? What about people with behavioural disorders? Could you tell if someone hadn’t been taking his or her medication?</td>
</tr>
</tbody>
</table>

From: Brown 2014
Failures of public policy

• Lack of attention to important public matters in standard-setting processes
• Identified as failures of design:

All in all, procedural safeguards are provided for at the EU level, where in the Dutch case procedural design was practically absent. Although better in

A key requirement of privacy by design is that privacy options are considered as early as possible in the development of policies and technologies. However, little attention was paid to privacy in the early phases of Britain’s smart metering programme. An
• *key decisions* were seen to have been made by ministries of economy, energy, and technical standardisation bodies.

• *standards* were based on the interests of large organisations: grid operators and energy utilities.

• *Absence of parliaments and publics*: these actors were merely informed after the decisions had been made.

other companies from the market." Hence, standards can never be regarded to be purely technical and neutral. They often are an expression of commercial or political interests of the companies concerned.¹⁰ Because the main driving forces are business interests, it is unlikely that public interests such as safety, privacy protection or environmental protection (apart from the possible “essential requirements”) will be promoted."¹¹
**Good governance as design principle?**

- "The best lesson that can be learned from the Dutch case is that a pre-set framework is needed to guide the process ... reliance on principles of good governance could help to form an appropriate reference frame to guide the standardization process" (Hoenkamp et al. 2012, 280)
Styles of reasoning and designing

<table>
<thead>
<tr>
<th>Network</th>
<th>Design logic</th>
<th>Main actors</th>
<th>Emblematic site(s)</th>
<th>Main threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civic/activist</td>
<td>Stop the intrusive meters!</td>
<td>Citizens and public mobilisation</td>
<td>Public arenas; parliament</td>
<td>To public and private life</td>
</tr>
<tr>
<td>Law</td>
<td>Fundamental rights directing purpose of information</td>
<td>Legal</td>
<td>Courts, legal assessors</td>
<td>To fundamental rights</td>
</tr>
<tr>
<td>Privacy engineering</td>
<td>Design patterns and strategies</td>
<td>Engineers, organisational managers, CEOs</td>
<td>Business corporations, large organisations</td>
<td>To the reputation of the organisation</td>
</tr>
<tr>
<td>Regulation</td>
<td>Good governance</td>
<td>Parliaments, publics, regulatory and standard-setting bodies</td>
<td>Standards committees</td>
<td>To legitimacy of public institutions</td>
</tr>
</tbody>
</table>
Paradox of multidisciplinary collaborations

- Concepts and practices such as privacy by design bring people together in multidisciplinary collaborations

- Yet as collaborations tighten, people have to also rely more strongly on their basic field

- Tensions and (seeming) contradictions appear
Civic society actors versus privacy assessors

Privacy Impact Assessments are becoming a way of making it hardly possible for opposers to raise up the issue that some elements infringe fundamental rights because it is said “well now we did Privacy Impact Assessments”

(Dutch civil society representative, CANDID interview data)

The problem has been dealt with in a good way

(Dutch PIA practitioner)
Regulation versus law

The trouble ... is what is meant with data protection by design. If it is really confined to data protection, then in many/some cases it is possible to provide transparency regarding compliance with the GDPR. It is for instance certainly possible to show the purposes of data processing, and details about the data in question....

If DPbD is supposed to cover rights (beyond data protection), then things are much more complicated. How to provide transparency that the user is treated fairly or that their autonomy is not harmed? (academic lawyer, DPIA)
Corporations versus users and citizens

*NL gov did a very poor job in protecting these rights bcs they protected business*

(Dutch civil society representative, CANDID interview data)
Concluding question: Moving too fast to standardise solutions?

Some organisations, including private actors ... say: The Regulator or the government should take a leadership. ... a lot is conferred to standardisation processes

You want to have interoperability among systems and btw sub-systems. That is a sine qua non condition for the market to happen

*Templates is the only way to go because there are 1000 methods to develop an impact assessment

(PbD practitioner)
Technologies of consensus

• 'the overwhelming appeal of quantification in business, government, and social research'

• Makes sense if we ‘... regard numbers, graphs and formulas first of all as strategies of communications ...'
Controlling possible futures

• Cuijpers and Koops (2012, Hoehnkamp et al. (2012): if Privacy by Design is implemented, controversies like the Dutch case can be avoided
• Knowledge economy: increasingly trying to control and pre-empt possible futures
• According to pragmatist philosophers morality and law evolves from dealing with consequences
• Should we, and can we, seek to preempt any possible future public risk?
References

• Brown, I. (2014) Britain's smart meter programme: a case study in privacy by design. International Review of Law, Computers and Technology. 28(2)
• EC: Smart Grid Task Force Mandate, 2011