Smart metering and privacy in Europe

Cuijpers, C.M.K.C.; Koops, E.J.

Published in:
European data protection

Publication date:
2012

Document Version
Peer reviewed version

Smart metering and privacy in Europe: lessons from the Dutch case

Colette Cuijpers and Bert-Jaap Koops

Tilburg Institute for Law, Technlogy, and Society (TILT), Tilburg University, The Netherlands

{cuijpers, e.j.koops}@tilburguniversity.edu

Abstract. The future of energy supply lies in smart grids, which enable energy supply to and from consumers. These two-way energy networks require smart energy metering systems. The vision of smart grids will require one or more decades yet to be fully realised, but since a roll-out of smart meters is a lengthy process, countries are already starting to implement smart metering legislation, following the European legal framework on energy efficiency. Rolling out smart meters, however, requires smart legislation. The Dutch example, where the Senate blocked two smart metering bills in 2009, demonstrates that introducing smart meters can be significantly delayed if the underlying legislation is flawed. In particular, the Dutch case shows that privacy is a crucial element in smart metering legislation. Energy consumption reveals details of personal life, in the most privacy-sensitive place – the home, and therefore smart metering has to strike a careful balance between detailed energy metering and privacy protection.

In this paper, we present the recent developments in smart metering and describe the Dutch case in detail. From this, we draw key lessons for countries that want to introduce smart metering. In terms of substance, the level of detail of smart meter readings and the mandatory or voluntary character of smart meters are crucial issues to take into account. Legislators must make a trade-off between the 'smartness' of the meter versus a comprehensive, mandatory roll-out. In terms of procedure, a privacy impact assessment is vital, and pitfalls of function creep should be avoided by resisting the temptation of making a meter 'too smart' all at once. From the outset, privacy and data protection law must be taken into account as an important requirement for the design of smart metering systems.

Keywords: Smart metering, energy, privacy, data protection, Europe, the Netherlands

adfa, p. 1, 2011.

1 Introduction

In 2009, the European Union enacted the Electricity Directive and the Natural Gas Directive.[1] These directives recommend the implementation of smart metering systems, in order to promote energy efficiency and to help consumers in saving energy. If an economic assessment of the long-term costs and benefits to the markets and the individual consumers is positive, the Electricity Directive stipulates that at least 80 per cent of consumers shall be equipped with smart meters by the year 2020.[2]

The foreseen smart metering system has several functionalities, which are well captured in the following description:

"a new generation of advanced and intelligent metering devices which have the ability to record the energy consumption of a particular measuring point in intervals of fifteen minutes or even less; communicate and transfer the information recorded in real time or at least on a daily basis by means of any communications network to the utility company; enable a two-way communication between the meter and the central system of the utility company, the so called distribution systems operator (DSO) allowing for remotely control functionalities of the meter such as switch off from the delivery of energy."[3]

The implementation of smart metering at national levels can come in conflict with the legal framework regarding privacy and data protection. Energy consumption reveals details of personal life, in the most privacy-sensitive place – the home, and therefore smart metering has to strike a careful balance between detailed energy metering and privacy protection. A relevant case in point is the Netherlands, where in 2009, the First Chamber rejected two Smart Metering Bills because of privacy concerns, significantly delaying the large-scale introduction of smart metering. The Dutch case shows that a privacy impact assessment is vital for the introduction of smart metering.

In this paper, we present the recent developments in smart metering and describe the Dutch case, in order to draw lessons about assessing privacy compliance for countries that want to introduce smart metering.

We will start in section 2 with a sketch of developments in smart grids and smart metering, as well as of the European legal framework regarding privacy and data protection. Next, in section 3, we present the Dutch case of smart metering, analyzing the privacy aspects of the first smart metering Bill that was rejected by the First Chamber and of the repair legislation that was subsequently adopted. We pay particular attention to a report that put the initial smart metering Bill to the privacy test of Article 8 of the European Convention of Human Rights (ECHR). Based on the Dutch

---

[1] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, OJ 14.08.2009, L211/55. Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC, OJ 14.08.2009, L211/94.

[2] Directive 2009/72/EC, Annex I, art. 2.

[3] Rainer Knyrim and Gerald Trieb, "Smart metering under EU Data Protection Law", *International Data Privacy Law*, March 1, 2011, p. 121.

case, we conclude in section 4 with a framework that can be used to assess the privacy implications of smart metering implementation.

2. Background

2.1. Smart Grids and Smart Metering

"Smart grids have an essential role in the process of transforming the functionality of the present electricity transmission and distribution grids so that they are able to provide a user-oriented service, supporting the achievement of the 20/20/20 targets and guaranteeing high security, quality and economic efficiency of electricity supply in a market environment."[4]

In 2009, the European Commission set up a Task Force Smart Grids to lay the foundations for smart grids in Europe. Its task is to identify and procure a set of regulatory recommendations to ensure EU-wide consistent and fast implementation of smart grids, while achieving all expected services and benefits for users.[5] The Task Force consists of three Expert Groups, of which the first (EG1) will identify functionalities of smart grids and smart meters. In their final report, a smart grid is defined as:

"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 – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety".[6]

In contrast to traditional electricity networks, smart grids facilitate two-way energy traffic, enabling consumers with energy generators such as solar panels to transfer excess energy to the grid. Smart grids encompass a much wider area than smart metering, but smart metering is an important first step towards a smart grid as they "bring intelligence to the 'last mile' between the grid and the final customer".[7] EG1 even states that without this key element, the full potential of a smart grid will not be realized.[8] The two-way energy traffic requires two-way communication with the grid both for billing purposes and for optimising energy efficiency. Another key functionality of smart meters is that they provide detailed feedback to consumers on their energy consumption, which raises awareness and should incite them to save energy where possible.

---

[4] Task Force Smart Grids, Expert Group 1 (EG1), *Functionalities of smart grids and smart meters*, December 2010, p. 4. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group1.pdf.

[5] Knyrim and Trieb, p. 127.

[6] Task Force Smart Grids, Expert Group 1 (EG1), p. 6.

[7] Idem, p. 16.

[8] Idem.

Smart metering standardization is covered by a specific Mandate (M/441) by the Commission to the European Standardization Organisations (ESOs).[9] The work within the M/441 Mandate is overseen by the Smart Meters Co-ordination Group (SMCG).[10] The general objective of this mandate is: *"To create European standards that will enable interoperability of utility meters (water, gas, electricity, heat) which can then improve the means by which customers' awareness of actual consumption can be raised in order to allow timely adaptation in their demands"*.[11]

The legal framework regarding smart meters in Europe can be described as an ongoing process. The obligation to provide individual meters to end users was prescribed in Directive 2006/32/EC on energy efficiency.[12] This Directive is the basis of the initial proposals for the Dutch smart meters we discuss below. Although the Dutch proposals assumed that smart meters were mandatory to install, no such explicit obligation can be derived from Directive 2006/32/EC. The Directive also does not prescribe how specific the smart metering should be.

In 2009, the Electricity Directive 2009/72/EC and the Natural Gas Directive 2009/73/EC were adopted. These Directives prescribe smart meters in similar wordings as Directive 2006/32/EC: *"In order to promote energy efficiency, Member States (...) shall strongly recommend that electricity undertakings optimise the use of electricity, for example by (...) introducing intelligent metering systems or smart grids, where appropriate".*[13] Both Directives are supplemented with an Annex regarding measures on consumer protection. These Annexes include a requirement that at least 80 per cent of consumers shall be equipped with smart meters by the year 2020, if an economic assessment by 3 September 2012 is positive.[14] This assessment should determine *"all the long-term costs and benefits to the market and the individual consumer or which form of intelligent metering is economically reasonable and cost-effective".* A time-path of 10 years is foreseen for the implementation of intelligent metering systems. In the European Commission Digital Agenda for Europe the goal is

---

[9] Standardization mandates can be retrieved from:
http://ec.europa.eu/enterprise/standards_policy/mandates/database/
The three standardization Mandates relevant in view of the Smart Grids Task Force are Mandate M/490 for Smart Grids (issued 1 March 2011), Mandate M/468 for electric vehicles (issued 4 June 2010) and Mandate M441 for smart meters (issued 12 March 2009), http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

[10] Task Force Smart Grids, Expert Group 1 (EG1), , p. 5.

[11] Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability, p. 1,
http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2009_03_12_mandate_m441_en.pdf

[12] Directive 2006/32/EC of the European Parliament and of the Council of the European Union of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC, OJ 27.04.2006, L114/64. The latest date for implementation was 17 May 2008.

[13] Art. 3(11) Directive 2009/72/EC; similarly, art. 3(8) Directive 2009/73/EC.

[14] Directive 2009/72/EC, Annex I, art. 2.

set for the member states to agree on common additional functionalities for smart meters by the end of 2011.[15]

In 2011, a new directive on energy efficiency was proposed that will repeal Directive 2006/32/EC.[16] The explanatory memorandum concludes that smart meters have economic benefits: *"Other options with a considerable positive impact compared to their costs are those that (...) provide improved and more frequent information to households and companies on their actual energy consumption through billing and smart meters (...). The [Impact Assessment] shows that all these measures are valuable in reducing the information gap that is one of the barriers to efficiency and could yield major energy savings"*. Voluntary measures are considered insufficient to tap all the available potential for savings, hence the need for a revised directive.

While the legal framework is still taking shape, smart meters have been developed and rolled out in several countries. The SmartRegions project published a European Smart Metering Landscape Report in February 2011. This report concludes that, due to a regulatory push by the EU's Third Energy Market Package, a majority of European countries have or are about to implement some form of legal framework for the installation of smart meters.[17] Some countries are labelled 'dynamic movers' because they already have decided about a mandatory rollout, or major pilot projects are paving the way for such a decision.[18] Besides the Netherlands, countries such as Denmark, Finland, France, Ireland, Italy, Malta, Norway, Spain, Sweden and the UK are 'dynamic movers.' A second category, comprised of Germany, the Czech Republic, Estonia, Slovenia and Romania, is named 'market drivers' where rollout is not based on legal requirements but on internal synergetic effects or because of customer demands. Some countries are labelled ambiguous movers, as the debate is still ongoing without any clear decisions, such as Portugal, Belgium and Austria. The remaining member states are categorised as 'waverers' and 'laggards', as the debate on smart metering has not at all, or just yet, started.[19]

2.2. European Legal Framework on Privacy and Data Protection

Privacy can be seen as an umbrella concept, covering different dimensions of private life. The territorial dimension relates e.g. to respect for the home, bodily integrity concerns the right to privacy in relation to the body, the right to choose which relationships to enter into is known as relational privacy, and informational privacy con-

---

[15] COM (2010) 245 final/2, 26.8.2010.

[16] Proposal for a Directive on energy efficiency and repealing Directives 2004/8/EC and 2006/32/EC, COM(2011)370, 22.06.2011, http://ec.europa.eu/energy/efficiency/eed/eed_en.htm.
For an elaborate description see: *Steering through the maze #5. Your eceee guide to following the approval process of the proposed Energy Efficiency Directive*, http://www.eceee.org/EED.

[17] Stephan Renner et al., *European Smart Metering Landscape Report SmartRegions Deliverable 2.1.*, 2009, p. 1, http:// www.smartregions.net.

[18] Idem.

[19] See for a graph of these categories: http://www.smartregions.net/default.asp?SivuID=26927.

cerns the protection of personal data. Because of the importance of data protection in current society, the concepts of privacy and data protection are often used as synonyms, in a sense that people speak of privacy when they mean informational privacy or the protection of personal data. However, it is important to remember that privacy is a broader notion, encompassing more dimensions than just protection of personal data. This is captured in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which covers the right to respect for private and family life, home and correspondence. This includes many aspects of data protection.[20] The Charter of Fundamental Rights of the European Union includes separate articles stipulating the right to private and family life, home and communications (art. 7) and the right to protection of personal data (art. 8).[21]

Since smart meters potentially involve both personal data and private life, home and communications, they require a comprehensive privacy impact assessment. In the European context, the major legal instruments for such an assessment are the Data Protection Directive for informational privacy and article 8 ECHR for privacy in general.

2.2.1. Directive 95/46/EC[22]

With regard to the informational privacy dimension, several legislative initiatives have been taken in Europe. Within the information society free flow of information is very important. Differences in national data protection legislation can hamper the internal market and from a human rights perspective a high level of protection is desired to protect individuals' personal data. These two pillars form the basis of Directive 95/46/EC, which stipulates the main rights and obligations to be respected when processing personal data.

The Directive constitutes a layered system consisting of three levels. The first level is the general level that applies to every processing of personal data. The second level, which needs to be applied on top of the first level, applies when sensitive data are being processed. The third level is applicable when personal data are being transferred to third countries. Hence, if sensitive data are being transferred to third countries, all three levels apply.

---

[20] Cf. Paul De Hert and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action", In *Reinventing Data Protection?,* ed. Serge Gutwirth et al., (Berlin: Springer, 2009), 3-45.

[21] The Lisbon Treaty makes the EU Charter of Fundamental Rights a binding and legally enforceable part of EU law, see http://europa.eu/lisbon_treaty/glance/index_en.htm. For a downloadable copy of the Charter see: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_303/c_30320071214en00010016.pdf.

[22] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50. The Directive has its roots in Convention 108 and the OECD privacy principles, http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

First, it must be determined whether or not Directive 95/46/EC is applicable, on the basis of the first four articles of the Directive. The main questions to be answered are: are *personal* data being processed, i.e., 'data relating to an identified or identifiable natural person' (data subject), and if so, whether an exception applies that makes the processing fall outside of the scope of the Directive.[23] If the Directive applies, personal data *"may only be processed fairly and lawfully'* (art. 6(a)). What this entails, can be derived from the other provisions in the Directive. The main aspects concern the requirement of a specified purpose for processing personal data, the requirement to have a legitimate basis for processing personal data, and the requirement only to process data in a way that is compatible with the specified purpose. Regarding the quality of the data it is determined that data must be relevant, accurate, not excessive and up to date. Besides, sufficient security measures need to be taken in order to protect data from being leaked, corrupted, or destroyed. Furthermore, the data controller (i.e., the one who determines the purposes and means of the processing of personal data) has the obligation to inform data subjects (and in some cases the Data Protection Authority,[24] art. 18) regarding data processing. Data subjects have the right to access, rectification, erasure, blocking, and the right to object to data processing. The Directive obliges Member States to put in place effective sanctioning mechanisms.

The second level lays down an extra strict regime for the processing of sensitive data, being data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life' (art. 8). Even though on the surface this prohibition might not seem relevant in view of smart meter data, examples can be given where these data do provide an insight into, e.g., religious beliefs, as energy consumption can reveal patterns of, for example, observing Ramadan or getting ready for morning prayers.

The third level of the Directive concerns the transfer of data to third countries, which is only allowed if the receiving country ensures an adequate level of protection (art. 25-26). This is not immediately relevant for smart metering, except if suppliers outsource their data processing to non-EU countries or to the cloud.

Besides the general provisions of Directive 95/46/EC, there are also some sector-specific rules and regulations, such as Directive 2002/58/EC and Directive

---

[23] See art. 3: '(1) This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. (2) This Directive shall not apply to the processing of personal data:
in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law; [or] by a natural person in the course of a purely personal or household activity.'

[24] The Directive obliges all Member States to establish a supervisory authority, also known as Data Protection Authority.

2006/24/EC which apply to electronic communications.[25] These Directives could play a role when electronic communications services are used for data processing in smart metering systems.[26] These services might, depending on the technologies used and the specifications of the system, process not only personal data but also location data. An analysis of these Directives in relation to smart metering is beyond the scope of this paper; we recommend further research into the applicability of Directive 2002/58/EC to smart metering and, if it applies, into the consequences of this legal regime for smart metering systems.

Finally, the general and specific legislation is supplemented by sector-specific soft law, such as codes of conduct. Such supplementary instruments need to be taken into account as it can influence upon whether and how data may be processed. In the case of smart metering, the underlying contracts between consumers and energy suppliers can contain specific provisions regarding whether and how personal data may be processed.

2.2.2 Proposed Regulation for data protection

On Data Protection Day 2012, a Proposal was presented for a new EU General Data Protection Regulation.[27] There is no scope in this paper for elaborate reflection on the consequences of this proposal, since it is a draft that will be much debated and possibly amended in the coming years, and the large-scale roll-out of smart metering may take place prior to the entry into force of the proposed changes. Moreover, a substantial part of the Regulation clarifies and harmonizes existing concepts, rights and obligations of the current EU legal framework on data protection. Some important new rights are proposed, such as the right to be forgotten and a right to data portabil-

[25] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.

[26] The definition of an electronic communications service is: 'a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks' (art. 2(c) Directive 2002/21/EC, OJ L108/33, 24.4.2002).

[27] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM (2012) 11 final 2012/0011 (COD). Available from: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

ity (art. 17 and 18). 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. Establishing an obligation for the controller to implement appropriate technical and organisational measures and procedures to meet the requirements of the Regulation and to ensure the protection of data subject rights. These mechanisms must ensure by default that only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes.

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. Several situations are mentioned, including *"a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual"* (art. 33, section 2, under a).

As will be discussed in section 4.1, smart metering data can offer sharp insights into our daily lives. Therefore, under the proposed new EU legal framework, the introduction of smart metering systems will require not only privacy by design and by default, but also a Data protection impact assessment prior to the implementation of such a system.[28] This is a development to which the developers of smart metering systems should adapt in any case, as will become clear from the Dutch smart metering case in section 3.

2.2.3. The triple test of art. 8 ECHR

As explained above, processing personal data according to data protection legislation is no guarantee that privacy will not be infringed. In smart metering, the consequences of data processing go beyond the informational privacy dimension, as insight can be given into patterns of living, at what times of the day and days of the week someone is at home or away, how many people make up the household, and incidental and structural changes in these patterns over time. If smart metering comes with supply regulation functions, for example 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.

[28] Conducting a PIA is also a core recommendation in the NIST *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, NISTIR 7628, August 2010. Available from: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

For European countries, article 8 ECHR is the most important codification of the fundamental human right to privacy. A significant body of case-law helps to apply art. 8 ECHR to new cases and developments. Therefore, a privacy test can best be conducted along the lines of Article 8 ECHR. This article states:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

The text of article 8 displays a triple test regarding whether or not the right to privacy is invaded. For smart metering, this test translates into the following four questions:

1. Does the smart meter interfere with privacy? If so, the next questions must be answered.
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?

Although the first three questions can usually be answered rather easily in respect of smart metering,[29] the fourth question requires to check whether the infringement of privacy caused by the smart metering system is necessary in view of a pressing social need, relevant to meet its purpose, does not go beyond what is necessary to meet its purpose, and whether there are no less invasive alternatives to meet its purpose (subsidiarity) and its benefits are in a reasonable proportion to the costs (proportionality). This is not easy to assess in general as this closely depends on the specific implementation of smart metering, e.g., whether or not a smart meter is mandatory, the purposes for which it is implemented, and the functionalities that will be given to the smart metering system.

[29] See also Paul de Hert and Dariusz Kloza, "The challenges to privacy and data protection posed by smart grids", In *Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts*, ed. E. Schweighofer and F. Kummer (Wien, 2011), 194.

3. The Dutch Case[30]

3.1. The 2008 smart metering bills

The introduction of smart meters was envisioned by the Netherlands in 2006, with a view to ensuring the smooth operation of the retail energy market.[31] The introduction was also a consequence of the compulsory implementation of the Directive on energy efficiency.[32] This Directive, whose primary aim is to bring about energy savings, prescribes that end users should have energy meters that provide information about actual use. End users must also regularly receive information about this use.

To ensure timely implementation of the Directive, it was decided that this would take place in two stages. The transposition of the Directive would take place in the Implementation of the EC Directives on Energy Efficiency Bill. This bill was submitted to the Second Chamber in January 2008.[33] When another bill, amending the Electricity Act 1998 and Gas Act to improve the operation of the electricity and gas markets,[34] would enter into force, the provisions with respect to electricity and gas from the Implementation Bill would lapse.

Together, these two smart metering bills provided for the mandatory introduction of so-called smart meters in every Dutch household. Not accepting the installation of a smart meter was made punishable as an economic offence, sanctioned with a fine of up to 17,000 euro or imprisonment for a maximum of 6 months. The smart meter would record and forward to the network operators (also called grid managers) data about consumers' energy consumption at detailed interval periods, namely hourly measurements for gas and quarter-hourly measurements for electricity. These data would be forwarded to the energy suppliers, who would then use these data to provide consumers with detailed information about their energy consumption, so that the consumers could adapt their energy-consuming behaviour accordingly.

Besides the measuring and communication functionalities, the initial Dutch proposals also included signaling, switching and regulatory functions. The signaling function enables the network operator to detect energy quality remotely. The switching function enables network operators to remotely switch energy capacity off and on, in order to deal with fraudulent or non-paying customers, or in case of disasters. Fi-

---

[30] For the complete parliamentary history of the Dutch implementation of Directive 2006/32/EG see:
http://www.eerstekamer.nl/wetsvoorstel/31374_verbetering_werking#p4,
http://www.eerstekamer.nl/wetsvoorstel/31320_wet_implementatie_eg,
http://www.eerstekamer.nl/wetsvoorstel/32373_novelle_wet_implementatie_eg (only available in Dutch).

[31] Parliamentary Documents Second Chamber 2005/06, 28 982, No. 51.

[32] Directive 2006/32/EC. See supra s. 2.1. The Directive had to be implemented by 17 May 2008.

[33] Parliamentary Documents Second Chamber 2007/08, 31 320, No. 2.

[34] Parliamentary Documents Second Chamber 2007/08, 31 374, No. 2.

nally, the regulatory function entails the possibility to add options to the meter so that it can carry out additional supportive functions.[35]

Since some privacy concerns were raised after the 31374 Bill had been submitted to parliament, the Dutch Data Protection Authority (DDPA)[36] was asked to advise on the Bill. The DDPA deemed the initial proposal for the Dutch smart metering act to violate the Dutch Data Protection Act (Wet bescherming persoonsgegevens). Their main concerns related to a lack of consent or any other legitimate processing ground and obscurities regarding which parties have access to what measuring data.[37] The Minister of Economic Affairs amended the proposal by providing that the network operator could only transfer the hourly or quarter-hourly readings of energy consumption to energy suppliers if consumers have given explicit consent for this; daily readings would, however, still be mandatorily forwarded to energy suppliers. The Minister also emphasised that all conditions of chapter 2 of the Dutch DPA would apply, including the requirements of purpose specification and use limitation, data subjects' right of access, data removal after use, and suitable security measures. After the amendment, the Dutch Data Protection Authority deemed the legislation compliant with the Dutch Data Protection Act. Reassured by the amendments, in July 2008, the Second Chamber passed both smart metering bills without any further substantial privacy debate.[38]

3.2. Privacy assessment report

As data protection is only one dimension of the broader right to privacy, the Dutch Consumer Union was not convinced that all privacy concerns had been addressed. After the bills had been passed by the Second Chamber, the Consumer Union commissioned a study to test whether the proposed smart metering legislation was in conformity with article 8 ECHR. This study was conducted by us and published in October 2008.[39]

The report observed that the generation of quarter-hourly/hourly and daily readings from which information can be derived about lifestyles and the presence or absence and numbers of persons, along with the compulsory use of smart meters that generate detailed readings and pass them on to grid managers, as well as the imposition of a severe security obligation on grid managers, are aspects of the bill that infringe privacy. Smart meters put pressure not only on informational privacy, but also on the

---

[35] Parliamentary Documents Second Chamber 2007/08, 31 374, No. 3, p. 14.

[36] In Dutch: College Bescherming Persoonsgegevens (CBP), www.cbpweb.nl. English website: http://www.dutchdpa.nl/Pages/home.aspx.

[37] Wetgevingsadvies, 17 juni 2008, z2008-00769, available from: www.cbpweb.nl.

[38] Parliamentary Proceedings Second Chamber 3 July 2008, 105-7642.

[39] Colette Cuijpers and Bert-Jaap Koops, *Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 EVRM* [The 'smart meters' bill: a privacy test based on article 8 ECHR], Study commissioned by the Dutch Consumers' Association, October 2008. The Dutch version is available from: http://www.consumentenbond.nl/morello-bestanden/209547/onderzoek_UvT_slimme_energi1.pdf. An English version can be obtained from the authors.

right to inviolability of the home and the right to respect for family life. For these reasons, the report performed a strict privacy-compliance test as laid down in art. 8 ECHR.

The report concluded that the following characteristics of the proposed Dutch smart metering system were 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; and the compulsory roll-out of smart meters to all households. Therefore, the report concluded that the introduction of the smart meter on these points would violate article 8 of the ECHR.

Moreover, the report found that the government had provided too little evidence to assess the 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. To meet the test of article 8, more empirical evidence should be provided about the prevalence of energy fraud, to substantiate the necessity of building in these functionalities for all consumers. After all, these functionalities introduce new opportunities of abuse, e.g., by malevolent hackers, and thus constitute a security and privacy risk.

The main reason for these conclusions was that the bills, particularly the points concerning detailed metering data and compulsory use, provide insufficient substantiation as to why these steps would be necessary in a democratic society. It is not clear whether it would actually foster energy savings – the primary purpose of the Directive – if consumers have to consult their energy consumption on a website provided by their supplier or a third party; it could be equally or more effective if consumers consult their real-time energy use on a display in the house itself, without meter readings having to leave the privacy of the home. In as far as the smart meter was intended to increase efficiency, this aim could be achieved by the proposal, but this is not a pressing social need. There are alternatives that entail less invasive infringements of privacy, again meters with in-home displays can be mentioned, as well as the use of statistical and anonymised data, which might also effectively serve the intended aims. These alternatives had not been sufficiently researched, meaning that the compulsory introduction of smart meters did not meet the requirements of subsidiarity and proportionality. With the bills, insufficient consideration had been given to the fact that the smart meter is a measure that constitutes a significant breach of the right to inviolability of the home and the right to respect for family life. To justify such a breach, much more substantiation with convincing arguments and empirical data was required. In the absence thereof, so the report concluded, the proposal in its current form would therefore have to be rejected.

The report recommended to study suitable alternatives that would infringe privacy to a lesser extent while still contributing to achieve the intended objectives. With respect to installing the switching and signalling functions, additional empirical research could be performed to determine whether these need to be introduced on a large scale.

3.3. Rejection by the First Chamber

The Dutch First Chamber discussed the privacy concerns that had been raised by the report and by criticisms that had been voiced in the media. Senators voiced criticism that an ex ante assessment of art. 8 ECHR had not been conducted, observing that the Dutch DPA had only looked at compliance with the Dutch Data Protection Act, and they questioned the Dutch additions to the requirements of the Directive, in the detailed readings of the meter that had to be provided to the network operator and (in daily measurements) to the energy supplier, which consumers could not opt out of. The Senate was not convinced by the Minister's argumentation that art. 8 ECHR was not violated by the proposal. Most importantly, the Senate was particularly alarmed by the mandatory character of the roll-out, and by the far-reaching sanction of 6 months' imprisonment for consumers refusing to have a smart meter installed. Therefore, on April 7 2009, the First Chamber decided not to accept the proposed legislation unless it were changed in several respects.[40] Constitutionally, the First Chamber can only accept or reject bills, but not amend them. In cases like this, the First Chamber can – under threat of rejecting a bill altogether – induce a minister to promise to introduce a new bill, called a 'novella' (*novelle*), in the Second Chamber that amends the bill at issue. This construction allows the First Chamber to accept the original bill as it will be amended by the *novelle*.

3.4. The 2010 *novelles*

The *novelles* (one for each bill) were introduced in the spring of 2010.[41] Four changes were implemented by the *novelles* that are relevant in view of privacy. Two have only minor privacy implications. First, a so-called supply model (*Leveranciers-model*) was introduced, i.e., a system where end users no longer receive separate bills from the grid manager and the energy supplier. With the introduction of the supply model they only receive one combined bill from their energy supplier. This change is relevant in view of privacy as this change creates coherence between the administrative processes of grid operators, energy suppliers, and measuring companies regarding the management of end-user data.

A second minor improvement for privacy is the duty for the energy sector to address in their annual reports how they have dealt with the requirements regarding data processing. Although it does not enhance the level of privacy as such, it does improve transparency and awareness.

A major change enhancing the privacy-friendliness of the Dutch smart metering landscape concerns cancelling the obligatory roll-out of smart meters. The *novelles* explicitly grant end users the right to refuse a smart meter, without risking a fine or imprisonment, as the sanction is lifted. Besides declining a smart meter, consumers are offered a possibility to request the operator to 'administratively shut down' the

[40] See Parliamentary Proceedings First Chamber, 24 March 2009, 26-1316/1331, 26-1343/1359, and 26-1381/1389; 7 April 2009, 28-1413/1427.

[41] Parliamentary Documents Second Chamber 2009/10, 32 373, No. 2, and 32 374, No. 2.

smart meter. This means that a grid operator will stop reading measuring data of an end user. A grid operator is legally obliged to honour this request.

A second considerable improvement for privacy is a clarification and codification of the terms and conditions under which personal data can be processed by the parties involved in the process of energy supply. The collection of end-user metering data by the grid manager and energy suppliers is now explicitly tied to their legally prescribed tasks, such as billing by suppliers and network management by the grid operator. This is a refinement of the rules regarding the processing of measuring data. Previously, only the conditions under which grid operators were allowed to transfer measuring data of end users to suppliers were laid down. The conditions now in place regarding the collection and use of such data by grid operators provide more checks and balances to protect the privacy of consumers.

Dutch Parliament was satisfied with the privacy improvement of making the smart meters voluntary. The Second Chamber passed the *novelles* in November 2010 and the First Chamber accepted the original smart metering bills, including the amendments made by the *novelles*, in February 2011.[42]

3.5. Privacy re-assessment

The new Dutch smart metering legislation has clearly responded to the privacy concerns that were one of the main reasons for the First Chamber to reject the earlier proposals. The current Dutch legislation can be described as a four-choice-model, as end users/customers are in a position to choose between four options to measure their energy consumption.

1. No smart meter, hold on to the traditional ('stupid') meter.
2. A smart meter that can be administratively shut down.
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.[43]

Not only the possibility to decline a smart meter is a step towards a more privacy-friendly system, also the fact that grid operators are not allowed to collect a continuous stream of measuring data certainly is an improvement for privacy.[44] In the standard measurement regime, only the following data are allowed to be processed: once a year for the annual invoice; at an intermediate time in case of relocation of the end user or if the end user switches from one energy supplier to another; bi-monthly for an insight into the actual energy consumption; and, finally, all data processing that is relevant for technical management and necessary in view of the legal obligations for grid operators. Data processing thus is also allowed to check for the proper and secure functioning of meters. Moreover, legislation stipulates that grid operators may only

[42] Parliamentary Proceedings Second Chamber, 9 November 2010, 19-18; First Chamber, 22 February 2011, 19-2-2.

[43] Parliamentary Documents Second Chamber 2009–2010, 32 374, No.. 3, p. 8-9.

[44] Colette Cuijpers, "Slim kiezen bij slimme meters", *Privacy & Informatie*, June 2011, p. 134.

transfer data to energy suppliers that are necessary in view of the suppliers' tasks.[45] Hence, daily measurements no longer form part of the standard measurement regime. More frequent and detailed readings of metering data are only permitted if end users have given their unambiguous consent. This consent can be withdrawn at any time without negative consequences for the end user.[46]

Although the scope of this paper does not allow us to assess in-depth the amended legislation's compliance with art. 8 ECHR, for the moment we incline to thinking that the Dutch law is now more in line with privacy requirements. Important factors are that very detailed regular readings are no longer part of the standard measurement regime and that consumers have the right to refuse a smart meter. This significantly reduces the infringement of individuals' privacy.

There is one caveat, however, in that Directives 2009/72/EC and 2009/73/EC foresee a mandatory 80% coverage if a cost/benefit analysis is positive for a member state. According to the Minister, five factors will be taken into account: how often consumers switch to other (presumably more cost-efficient) energy suppliers, the roll-out percentage, roll-out efficiency, the costs of distance-readable meters, and energy savings by consumers. All factors will be closely monitored during the initial small-scale and subsequent large-scale roll-out.[47] The caveat is that the cost/benefit assessment could turn out positive while less than 80% of consumers accept smart meters. In that case, pressure could be put on unwilling consumers to accept a smart meter after all, jeopardising the voluntary nature of the roll-out. One could question whether a mandatory 80% roll-out target (conditional upon a cost/benefit analysis) is necessary in a democratic society, if a member state bases its art. 8 ECHR compliance on voluntary smart metering. However that may be, the abolition of very detailed readings – which is the main privacy-sensitive issue in smart metering – in the standard measurement regime, with consumers having to give unambiguous consent if quarter-hourly or hourly readings are to be transferred to operators or suppliers, seem to take the largest privacy sting out of the Dutch law.

4. Lessons for Assessing the Privacy Aspects of Smart Metering

From the Dutch smart metering case, two factors can be highlighted as having been predominant in the rejection of the smart metering bills by the First Chamber: 1) the very detailed readings of smart meters and the transfer of these readings from consumer to grid operator and (of less but still) detailed readings from operator to energy supplier; 2) the compulsory nature of the roll-out, sanctioned by a hefty fine or even

[45] These tasks are listed in article 16 of the *Elektriciteitswet* (Electricity Act) and article 10 of the *Gaswet* (Gas Act).

[46] Parliamentary Documents Second Chamber 2009–2010, 32 374, No. 3, p. 8-9.

[47] Parliamentary Documents First Chamber 2010-2011, 32 373, C. Note that some criticism has been voiced against the assumptions of a KEMA report that serves a basis for the cost/benefit assessment, debating to what extent benefits of energy savings or supplier switching can be uniquely attributed to smart metering. See Sjak Lomme (2010), 'Commentaar', http://www.energeia.nl/column.php?ID=108.

imprisonment. Compounding these factors, two other aspects can be highlighted as underlying the problematic introduction of smart metering legislation: 3) a lack of substantiation why the privacy infringement and the compulsory roll-out were necessary; 4) the combination of different functionalities in one smart meter, creating a complex hybrid involving new risks and also confusing the argumentation for the necessity of such a smart metering system. In this section, we will discuss these factors in some more detail.

4.1. The level of details of meter readings

Smart metering data can offer sharp insights into our daily lives. The intensity of this vision 'through the walls of our home' becomes clear from several recent studies. Molina-Markham et al. indicate that it is possible to extract complex usage patterns from smart meter data: knowledge of an appliance's power signature enables identifying individual appliance usage within the aggregate data of a smart meter. Future data mining will likely enable even more refined identification of appliances, such as particular brands or models[48] Quinn points out that the privacy issue is all the more important as smart meters enable real-time monitoring of energy consumption.[49] Elaborating on this research, Greveler et al. show that smart meter data, when measured in intervals of 4 hours, exactly reveal when a person is at home, when he is sleeping and when he is preparing his meals. When using shorter intervals, of minutes or seconds, electric devices can be identified on the basis of use profiles, such as a fridge, coffee machine, washing machine, toaster, microwave, and TV.[50] These data can reveal if someone eats a cold or a hot breakfast, when laundry is done, or whether the kids are alone at home. It is even possible to determine which channel a TV is tuned to, through an analysis of the broadcast programs, particularly if the TV is tuned to a longer program such as a movie. The interfering noise in the meter data of other energy-consuming devices can most likely be filtered out in case movies are watched of 90 minutes or longer.[51]

This demonstrates that the more detailed smart meters readings are, the more privacy-sensitive the data become. Real-time readings in intervals of minutes can reveal many details of home life and paint a disturbingly clear picture of people's behaviour and preferences. Quarter-hourly or hourly measurements also reveal a rather privacy-sensitive picture, showing behaviour patterns and perhaps some insight in the type of

---

[48] Andrés Molina-Markham et al., "Private Memoirs of a Smart Meter", *BuildSys* November 2, Zurich, Switzerland 2010: 1, http://www.cs.umass.edu/~kevinfu/papers/molina-markham-buildsys10.pdf., p. 1.

[49] Elias Quinn, "Smart Metering & Privacy: Existing Law and Competing Policies", *Report for the Colorado Public Utilities Commission*, Spring 2009: 11. http://cospl.coalliance.org/fez/eserv/co:7930/reg72m562009internet.pdf. p. 11.

[50] U. Greveler, B. Justus, and D. Löhr, "Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz" ", *Arbeitspapier1 – Technischer Report, Status: ENTWURF, Version 0.6.*, 2011, p. 3. http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf.

[51] Idem.

household appliances used. While daily readings are less privacy-sensitive, they are still relevant from a privacy perspective, as they reveal patterns of being at home or away from home, and the number of people at home on a specific day. Here, privacy risks go hand-in-hand with security risks, threatening the inviolability of the home, as would-be burglars could determine on the basis of smart meter data when residents are away from home, and even whether or not they have an electronic security system.[52] More in general, security risks of smart metering systems emerge from automated two-way communication relationships with heterogeneous partners, requiring strong authentication and authorisation mechanisms to secure the transfer of smart meter data.[53]

The lesson here is that smart meters in today's homes not only measure the amount of energy consumption, but also have great potential to reveal what people do when, within the sanctity of their home. The more detailed the readings, the more privacy-sensitive the data become. This is a major factor to take into account when deciding which measurements have to be transferred from smart meters to network operators and energy suppliers. Privacy-sensitive data – such as quarter-hourly or hourly readings but also daily readings – should probably be processed only within the house itself (e.g., in an in-home display that enables consumers to monitor their energy consumption in real time). If detailed measurements are necessary to transfer outside of the home, a very high level of information security must be provided, and compelling reasons must be provided to do so in light of art. 8 ECHR's requirement of 'necessity in a democratic society'.

4.2. Mandatory or voluntary roll-out

The largest stumbling block in the Dutch case was the mandatory nature of the roll-out. It was foreseen that every household would receive a smart meter over the course of a few years, and consumers could not refuse. The smart meter bills included a provision that refusing a smart meter would count as an economic offence, which could be sanctioned with up to six months' detention. Although the Minister said in the First Chamber that she would deal with this 'in a practical way', she did not exclude the possibility that network operators would denounce a consumer's refusal with the police and that the Public Prosecutor would then decide how to deal with this economic offence.[54] The combination of mandatory roll-out and the threat of a very serious – indeed, disproportionate – sanction for people who did not want a privacy-infringing smart meter was too much for the bill to survive.

The proposed new Directive on energy efficiency[55] does not seem to require a mandatory roll-out of smart meters. Article 8(1) rather suggests voluntary acceptance

---

[52] Quinn 2009: 18.

[53] M. Jawurek and M. Johns, "Security Challenges of a Changing Energy Landscape", In *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Convention*, ed. N. Pohlmann, H. Reimer and W. Schneider, (Wiesbaden: Springer Fachmedien 2011), p. 255.

[54] Parliamentary Proceedings 24 March 2009, 26-1385/1386.

[55] COM(2011)370, http://ec.europa.eu/energy/efficiency/eed/eed_en.htm.

of smart meters by end users: "Member States shall ensure that final customers (...) *are provided with* individual meters that accurately measure and allow to make available their actual energy consumption and provide information on actual time of use" (emphasis added). It is questionable that should be interpreted as an obligation on end-users to accept the smart individual meter; the wording suggests they should be provided with the opportunity. Article 8(1) moreover clarifies that certain functionalities are only triggered on request of the final customer: "In the case of electricity and *on request* of the final customer, meter operators shall ensure that the meter can account for electricity produced on the final customer's premises and exported to the grid. Member States shall ensure that *if final customers request it*, metering data on their real-time production or consumption is made available to a third party acting on behalf of the final customer" (emphasis added).

High-frequency interval periods for measurements such as those proposed in the initial Dutch bills are not required on the basis of Annex VI of the proposed Directive. For billing purposes, monthly measurements are foreseen for Electricity and bi-monthly measurements for Gas. For private data exported through the interface to the end user – to better control their energy consumption – the end user must be offered the possibility to consult her historic consumption levels in the last seven days, day by day. This requires daily measurements. However, the Annex does not require such data to be exported outside of the house: it only requires secured transport of these data from the meter to the end user. For meters placed within a house, an in-home display would therefore suffice to show these daily measurements. Moreover, additional information allowing for more detailed self-checks by customers, such as graphic evolutions of consumption and benchmarking information) should be provided to customers according to Annex VI, but these do not require more detailed than daily readings and these should be accessible to customers "either directly through the interface or via the internet". Hence, the smart meter that seems mandated by the proposed Directive is therefore restricted to one that is capable of at least daily measurements and that has an interface showing readings to the customer. Additional functionality or more detailed readings are not required for a roll-out of smart meters.

This suggests that if countries want to introduce 'smarter' meters than those required by the Directive – particularly if they entail more detailed readings or involve high-frequency transfer of readings to network operators or suppliers – this requires consent of the end users. Knyrim and Trieb, however, have argued that user consent is not necessarily the only possible legal basis for installing smart meters.[56]

"The legitimacy of [smart meter data] transfers has to be based, for example, on a broad interpretation of Articles 7(b) and 7(f) of the Data Protection Directive[57]*. Nevertheless, taking into account that (according to almost all academic studies carried out so far) the rollout of new metering technology is economically feasible only if the vast majority of households is furnished with a smart meter, the establishment of a*

[56] Knyrim and Trieb, p. 122.

[57] Art. 7(b) refers to execution of a contract and 7(f) to legitimate interests of the data processor that outweigh the privacy interest of data subjects [authors' footnote].

valid legal obligation, either at the European or national level, might serve as the clearest, safest, and most sustainable way of securing successful implementation."[58]

Basically, these authors argue that there is a pressing social need for rolling-out smart meters to a large majority of households, and hence that national legislation mandating end users to accept smart meters would therefore pass the test of art. 8 ECHR. We are not immediately convinced by this argument, first because it requires careful analysis of the studies into the economic aspects of smart metering (something that is lacking in Knyrim and Trieb's article itself), and second because economic arguments are not necessarily strong enough to outweigh privacy interests. Whether legislation mandating smart meters is art. 8 ECHR-compliant will depend on how privacy-infringing they are and on how convincingly a legislator demonstrates that, in the context of the particular country, the economic arguments favouring a comprehensive roll-out of mandatory meters are indeed sufficiently pressing.

For the time being, it seems that European law in itself does not require mandatory smart meters, except for a minimum functionality of daily readings and direct accessibility of these readings to end users, which can be fulfilled through in-home displays. This lays a significant burden of proof on countries that want to roll-out 'smarter' meters than the European minimum on a mandatory basis, to show a 'pressing social need'[59] for this. The experience of the Dutch case suggests it might be a safer strategy to start with a voluntary roll-out and then to closely monitor how the factors evolve that are relevant for assessing the societal costs and benefits of smart meters.

4.3. Two underlying problems

Although the Dutch case ostensibly revolved around the level of detail of measurements and the mandatory character of the meter, two more general problems can be identified that lay beneath the initial legislative failure.

The first problem is a significant underestimation of the importance of privacy. The drafters of the initial smart metering bills and the Second Chamber focused almost exclusively on the economic and environmental aspects of smart grids and smart meters. No privacy impact assessment had been made. Only when the Dutch Consumer Association pointed out possible privacy concerns to the Minister, did she request the Data Protection Authority to advise on the Bills. When some adjustments had been made following the DPA's advice, the Second Chamber was easily satisfied with the privacy compliance of the smart metering legislation. Throughout this entire process, art. 8 ECHR was overlooked. Only when the privacy assessment report commissioned by the Consumer Association was drafted, did parliamentarians become aware that privacy is more than just compliance with the national Data Protection Act. The fact that smart meters have the capacity to reveal quite privacy-sensitive information, thus affecting not only informational privacy but also privacy of the home and of family life, seems to have been disregarded until the First Chamber,

[58] Knyrim and Trieb, p. 128.
[59] ECtHR 24 November 1986, *Gillow* v *The United Kingdom*, App.no. 9063/80, §55.

armoured with the privacy assessment report, started questioning the Minister about this. A tell-tale sign of privacy misapprehensions was a complete confusion in the First Chamber discussion whether the Dutch DPA had advised on the basis of compliance with the Dutch Data Protection Act or whether it had checked compliance with art. 8 ECHR. While the Minister initially stated the latter had been the case, subsequently it became clear that it had been the former.[60]

Perhaps because the privacy implications of smart meters had been underestimated, the argumentation for the very detailed readings and the mandatory roll-out had been superficial. An important element of the privacy impact assessment report was that the need for such mandatory 'smartness' had not been substantiated; many claims suffered from a lack of empirical evidence, such as the claim that consumers would become more energy-saving if they received information about their energy consumption from an energy supplier on a website.

The lesson to draw here is not only that privacy implications, of course, should never be underestimated, but also that an ex ante assessment of privacy implications can help to prevent legislative proposals from stumbling over privacy concerns further down the line. Countries considering smart metering legislation should conduct a privacy impact assessment, carefully analysing the privacy implications, and substantiating where appropriate, based on empirical evidence, how and why privacy infringements are deemed necessary in a democratic society. An important element of such a privacy impact assessment is looking at alternatives that are less privacy-invasive but that still serve the intended purposes of smart metering.

The second problem underlying the Dutch case is function creep – the expanding of functionality beyond the original purpose. While the European legislation required smart meters to provide feedback to end users, thus helping them to become more energy-saving, the Dutch bills added several functionalities to the proposed smart meter. Apart from providing information to consumers for energy-saving purposes, smart meters also had to provide distance-readable measurements to monitor network functioning and to combat fraud. Moreover, the meter also had to be controllable at a distance to regulate energy delivery, both for fraud-combating and disaster-management purposes.[61] The combination of all these functionalities led to a smart meter with a potential of very high frequency of two-way traffic between the meter and the grid. The transfer of very detailed measurements to the network operator, and daily measurements to energy suppliers, fitted well in the picture of such a hybrid smart meter, leading to a neglect of privacy-friendly alternatives, such as in-home displays or aggregation of individual meter data in the grid, that could likely equally well have served the purposes of energy-saving or network management. Also, the legitimate need for combating fraud, which can be served well by smart meters, does

[60] See Parliamentary Proceedings First Chamber, 24 March 2009, 26-1329, 26-1349f; 7 April 2009, 28-1416.

[61] In Italy, the introduction of smart metering by ENEL was strongly driven by the desire to combat fraud. See in this respect: Rob van Gerwen, Saskia Jaarsma and Rob Wilhite, *Smart Metering*, KEMA, The Netherlands, July 2006. Available from: http://www.idc-online.com/technical_references/pdfs/electrical_engineering/Smart_Metering.pdf.

not necessarily imply that comprehensive, wide-scale processing of detailed meter readings is necessary to identify occasional illegal activity.[62]

The lesson here is that smart meters have a wide range of functionalities,[63] which harbours a risk that too many functions are combined in a smart meter in a way that makes privacy implications less visible or less weighty in the overall assessment of the need for a smart meter.[64] This can backfire if the privacy assessment of a resulting hybrid smart meter concludes that the smart meter as a whole, with all its functionalities, is economically necessary, while disregarding whether privacy infringements are really necessary in light of each separate purpose. In other words, countries proposing complex smart meters with many functionalities may tend to overlook that simple purposes, such as inducing consumers to become more energy-saving or peak-load reduction in network management, can also be achieved by privacy-friendly alternatives.

5. Conclusion

The future of energy supply lies in smart grids, which enable not only energy supply to consumers but also energy supply from consumers. These two-way energy networks require smart energy metering systems. The vision of truly smart grids will require one or more decades yet to be fully realised, but since a roll-out of smart meters is a lengthy process, countries are already starting to implement smart metering legislation, following the European legal framework on energy efficiency. Rolling out smart meters, however, requires smart legislation. The Dutch case, where the Senate blocked two smart metering bills in 2009, demonstrates that introducing smart meters can be significantly delayed if the underlying legislation if flawed.

More in particular, the Dutch case shows that privacy is not to be underestimated. The failure of doing an ex ante privacy impact assessment backfired, as the proposed laws required mandatory installation in every household of smart meters that would send quarter-hourly/hourly measurements to network operators and daily measurements to energy suppliers. This level of detail creates privacy-sensitive data, and the necessity of smart meters infringing people's privacy in this way had not been substantiated by the government.

Several lessons can be learned from the Dutch case for countries considering smart metering legislation. In terms of substance, the level of detail of smart meter readings and the mandatory or voluntary character of smart meters are crucial issues to take

---

[62] Cf. Article 29 Working Party, "Opinion 12/2011 on smart metering", WP 183, April 4, 2011: 21.

[63] For an overview see: Smart Meters Co-ordination Group (SMCG), *Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the develop-ment of an open architecture for utility meters involving communication protocols enabling Interoperability M/441*, FINAL REPORT 2009, http://www.piio.pl/dok/SMCG_Sec0013_DC.pdf.

[64] The addition of extra functionalities over and above the requirements of the European Directives was also an issue for the First Chamber in questioning the acceptability of the smart metering bills. See, e.g. Parliamentary Proceedings First Chamber, 24 March 2009, 26-1325.

into account. In terms of procedure, a privacy impact assessment is vital to identify at an early stage the potential effects on individuals' privacy and to choose the least privacy-infringing modalities of smart metering. Pitfalls of function creep should be avoided by resisting the temptation of making a meter 'too smart' all at once, which could easily lead, as the Dutch case demonstrates, to choosing privacy-invasive instead of privacy-friendly settings; such settings are unnecessary to achieve the primary purpose of the current European energy-efficiency regulation, namely to provide consumers with sufficient feedback on their energy consumption to induce energy-saving behaviour.

The procedural lessons also highlight the need for privacy by design. This principle concerns the need to integrate, at practical level, data protection and privacy from the very inception of new information and communication technologies.[65] The purpose, design, functionalities and implementation of the smart metering system determines to a large extent whether or not it will comply with privacy and data protection legislation. Therefore, from the beginning, privacy and data protection law must be taken into account as an important requirement for the design of smart metering systems.[66] It is a promising development that the proposed Regulation on data protection explicitly establishes obligations for privacy by design and default, and an ex ante obligation for data protection impact assessments in cases where data processing has specific risks.[67]

The substantive lessons can also be formulated in the form of a key trade-off for legislators: the 'smartness' of the meter versus a comprehensive, mandatory roll-out. The smarter a meter is, i.e., the more detailed its readings are – up to quarter-hourly or even less – and the more functionalities it has, the more likely is it to be privacy-invasive. Current research already shows how revealing smart meter data can be of people's daily life in their homes, and findings such as the capacity to derive which TV channel one is watching from real-time energy readings[68] suggest that the privacy-sensitivity of energy consumption data will only increase in the future. This implies that if countries opt for smart meters with detailed readings that leave the privacy of the home, this can hardly be considered necessary in a democratic society, and hence, such smart meters can only be rolled out on a voluntary basis, as now will happen in the Netherlands. And conversely, if countries choose a relatively 'dumb' meter that conforms to the minimum requirements of European legislation (capable of at least daily measurements and with an interface showing readings to the customer), they can likely make the roll-out of such meters mandatory for consumers, in terms of compliance with art. 8 ECHR.

---

[65] Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, Brussels 2010, p. 2, available from: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf

[66] See also Knyrim and Trieb, 2011.

[67] Art. 23 and 33 of the Proposed General Data Protection Regulation, COM(2012) 11 final 2012/0011 (COD).

[68] Greveler, Justus, and Löhr, p. 1 and 3.

We would like to end with two concerns that remain even if legislators adopt smart legislation about smart meters. One is the role of consent. If countries opt for a voluntary roll-out of smart meters, are consumers sufficiently informed about what a smart meter entails? In the Dutch case, they can choose not only between keeping their 'dumb' meter and accepting a smart meter, but also, if they accept a smart meter, they can opt for administratively shutting off the detailed readings by the network operator or, at the other end of the privacy spectrum, give consent to forwarding detailed readings to energy suppliers or third parties. Whether consumers can make informed decisions about this depends greatly on the information provided to them by the network operator that asks them to have a smart meter installed, and on the way this information is provided. Should operators present the meter without informing consumers that they have a right to refuse, and should they suggest that providing detailed readings to third parties is a normal default setting ('just tick the box here'), then consent would lose its meaning. Moreover, average consumers will not be aware of the privacy impact of smart meter measurements; few will realise – if they are not informed explicitly of this – that daily readings offer insight into when they are away from home, and hardly anyone will be aware of the technical possibilities of deriving life patterns and appliance use from more detailed readings.[69] In short, an important element of a privacy-compliant roll-out of smart meters will be to make sure that consumers are adequately informed of the implications of smart meters.

Our second concern is a more general one. The house is rapidly losing its character as privacy's fortress, with directional microphones recording in-house conversations, cameras seeing through walls, thermal imagers detecting heat emissions, household appliances incorporated in the Internet of Things, the home computer permanently connected to the Internet, and private information such as personal texts, photos, books and music no longer stored in desks or on shelves but instead in the cloud.[70] Smart meters are yet another addition to this increasing transparency of the home. This requires careful consideration of the cumulative effect of the various developments that allow insight into how people live, in the one place where people most of all must feel free to do what they like. If our home will no longer be our castle, the house may be energy-efficient but it will be a cold place to live.

Bibliography

Article 29 Working Party, *Opinion 12/2011 on smart metering*, WP 183, 4 April 2011.

Cuijpers, Colette. "Slim kiezen bij slimme meters". *Privacy & Informatie*, 14-3

[69] Greveler, Justus, and Löhr, p. 4. http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf.

[70] B.J. Koops and M.M. Prinsen, "Houses of Glass, Transparent Bodies: How New Technologies Affect Inviolability of the Home and Bodily Integrity in the Dutch Constitution", *Information & Communications Technology Law*, 16 (3) 2007: 177-190.

(2011): 131-141.
Cuijpers, Colette, and Martin Pekárek. "The regulation of location-based services: challenges to the European Union data protection regime." *Journal of Location Based Services*, DOI:10.1080/17489725.2011.637081, 2011.
De Hert, Paul and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action." In *Reinventing Data Protection?*, edited by Serge Gutwirth et al., 3-45. Berlin: Springer, 2009.
De Hert, Paul, and Dariusz Kloza. "The challenges to privacy and data protection posed by smart grids." In *Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts*, edited by E. Schweighofer and F. Kummer. Tagungsband des 14. Internationalen Rechtsinformatik Symposions IRIS 2011, Wien 2011, 191-196.
ESMA. *Annual Report on the Progress in Smart Metering 2009*. http://www.esma-home.eu/UserFiles/file/ESMA_WP5D18_Annual_Progress_Report_2009%281%29.pdf
Greveler, U., Justus, B. and D. Löhr. *Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz",* Arbeitspapier1 – Technischer Report, Status: ENTWURF, Version 0.6., 2011. http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf.
Jawurek, M. and M. Johns. *Security Challenges of a Changing Energy Landscape*, In *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Convention*, edited by Pohlmann, N., Reimer, H. and W. Schneider. Wiesbaden: Springer Fachmedien 2011, p. 249-259.
Knyrim, Rainer and Gerald Trieb. "Smart metering under EU Data Protection Law", *International Data Privacy Law*, 1-2 (2011): 121-128. doi: 10.1093/idpl/ipr004.
Koops, B.J. and M.M. Prinsen. "Houses of Glass, Transparent Bodies: How New Technologies Affect Inviolability of the Home and Bodily Integrity in the Dutch Constitution". *Information & Communications Technology Law* 16-3 (2007): 177-190.
Molina-Markham, Andrés et al. *Private Memoirs of a Smart Meter*, BuildSys. Zurich, Switzerland, 2010. http://www.cs.umass.edu/~kevinfu/papers/molina-markham-buildsys10.pdf.
NIST Smart Grid Interoperability Panel – Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, NISTIR 7628, August 2010. Available from: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.
Quinn, Elias. *Smart Metering & Privacy: Existing Law and Competing Policies.* Report for the Colorado Public Utilities Commission, Spring 2009. http://cospl.coalliance.org/fez/eserv/co:7930/reg72m562009internet.pdf.
Renner, Stephan et al. *European Smart Metering Landscape Report SmartRegions Deliverable 2.1.,* 2009. http:// www.smartregions.net.
Smart Meters Co-ordination Group (SMCG) *Standardization mandate to CEN,*

CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling Interoperability M/441, FINAL REPORT, Version 0.7 – 2009-12-10. http://www.piio.pl/dok/SMCG_Sec0013_DC.pdf.

Task Force Smart Grids, Expert Group 1 (EG1). *Functionalities of smart grids and smart meters.* Final Deliverable, December 2010. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group1.pdf.

Task Force Smart Grids, Expert Group 2 (EG2). *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection*, 6 June 2011, FINAL DRAFT (for approval). http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_draft.pdf.