The ethical smart grid: Enabling a fruitful and long-lasting relationship between utilities and customers

G. Le Ray , P. Pinson

Centre for Electric Power and Energy, Technical University of Denmark, Kgs. Lyngby, Denmark

Abstract

The European Union is implementing ambitious programs to tackle energy efficiency, energy independence and climate change challenges. To reach the 20/20/20 targets, the EU aims at modernizing power grids to make them 'smart' by collecting close to real-time data and subsequently operate these grids more optimally. One of the smart grids' purposes is to integrate a growing share of renewable energy sources while efficiently accommodating their variability and limited predictability through actuation of consumer flexibility. To do so, 80% of the customers throughout Europe will be equipped with smart meters by 2020. On the one hand, the success of energy programs relies on customer involvement in altering their energy consumption through the use of analytics and incentive-based demand side management. On the other hand, the utilities are arguably showing limited ethics in the way smart meters are rolled-out and on the use of collected data. Indeed, beyond legal binds and technical obstacles, the deployment of smart meters and the use of collected data is unclear in terms of how to deal with customers. We argue that ethics should be an import driver for decision-making to guarantee the sustainability of smart grid programs which relies on the active participation of customers.

Keywords: Big Data, Privacy, Smart meter, Smart grid, Ethics

1. Introduction

The European Union's (EU) energy policy is facing unprecedented challenges due to increased dependencies on imports, scarce resources and the need to limit climate change (European Parliament, 2012). Ambitious energy efficiency programs have been developed to tackle these challenges. Indeed, since 2009 and the 2020 Climate & Energy Package's road map to the 20/20/20 targets (European Parliament, 2009b), EU has driven towards a *greener* energy sector to achieve energy efficiency, energy independence and last but not least to reduce greenhouse gas emissions.

As most of the issues on power systems are observed at the distribution level, the program requires a modernization of the grid to foresee potential issues and to have a pervasive control to prevent them (Farhangi, 2010). Information and communication technologies forms

Email address: [gleray,ppin]@elektro.dtu.dk (G. Le Ray , P. Pinson)

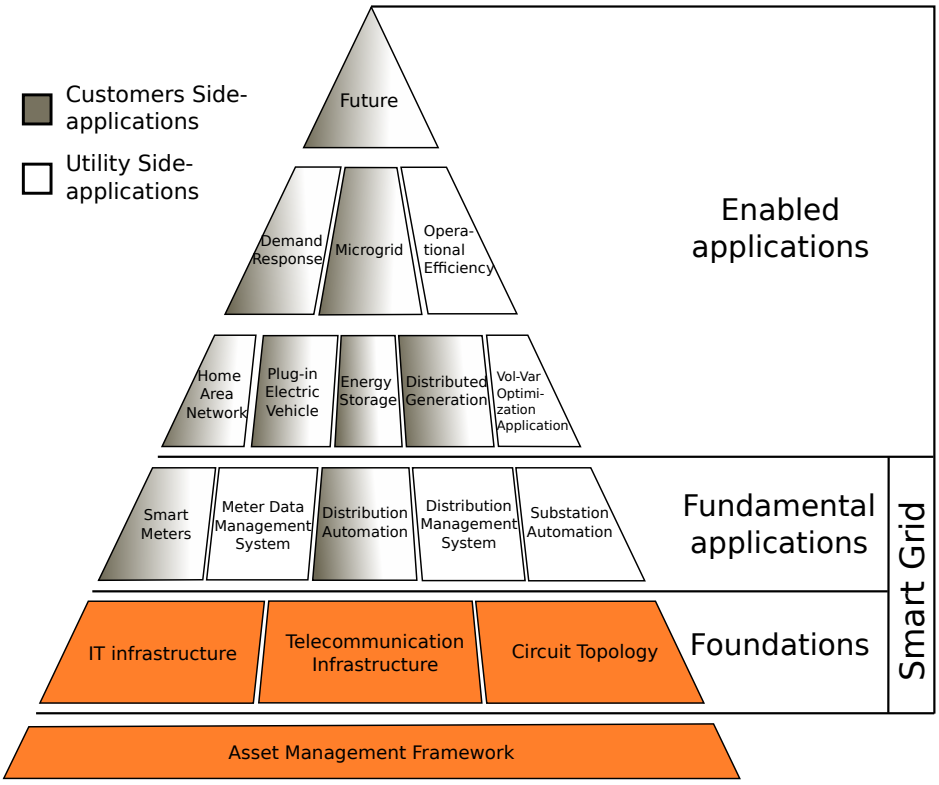

Figure 1: The Smart Grid pyramid (Source: Farhangi (2010))

the foundations of the smart grid pyramid (Figure 1) which support more advanced infrastructures. The Third Energy Package, adopted in 2009, strengthens the internal European market for gas and electricity by securing a competitive and sustainable supply of energy to the economy and the society (European Commission, 2011). To reach this goal, the EU has set the target of 80% of households equipped with smart meters by 2020 (European Union, 2009). Smart meters are deployed to provide more transparency to consumers (billing, price, consumption), to improve awareness on energy consumption and empower the consumers to modify their energy behavior using metering data (European Commission, 2011). On the utility side, smart meters' data will help them to increase the efficiency and the reliability of the grid. In this paper we define a utility as an entity that is given responsibility for the maintenance and operation of some infrastructure of public value and to be used for a public service. As displayed in Figure 1, smart meters constitute the first fundamental application that involves customers. The perception of smart meters by customers will condition the future of smart grids in their capacity to transform customers into actors of the grid through the use of demand side management (Bertoldo et al., 2015, Horne et al., 2015, Giordano et al., 2011).

At the same time, concerns are raised about a possible backlash of domestic customers (Zachary, 2011). Indeed the perspective of having smart meters reporting electricity consumption at high resolution in every home has engendered irrational fear (e.g. health issues and domes-

tic accidents) and legitimate questions about the need of smart meters and their impact on privacy (McKenna et al., 2012). The concept of privacy has drastically evolved, from Aristotle making the distinction between public sphere and private sphere, to the creation of the right to privacy (Papakonstantinou and Kloza, 2015). With the emergence of information technology, the legal framework has evolved to protect data and by extension data subjects. The legislation on data protection and privacy limits the legal use of data but it also defines the limits of a gray area on how to handle customers and their data (Tzafestas, 2018). Even if the decisions made are in line with the existing legal framework, they can have a substantial (and potentially negative) impact on the future of smart metering and smart grid deployment plans by extension (Jegen and Philion, 2017). It is where ethics is fundamental, it is defined as: *"A system of moral principles which deals with what is good or bad for individuals and the society. It is a collection of fundamental concepts and principles on an ideal human character that enable people to make decisions regarding what is right or wrong. Ethics is a code of conduct agreed and adopted by people in a society, which sets the norms of how a person should live and interact with other people."* (Tzafestas, 2018).

Following this definition, an ethical and human perspective has to be placed on the smart grid technology, especially its extensions smart meters and the data they generate. The foundations of the smart grid are put in place today. Hence it is important to understand the perspective of the customers to build an ethical smart grid to build a fruitful and long-lasting relationship between utilities and customers (Jegen and Philion, 2017).

In this paper, we argue that beyond the technical and legal issues, ethics should be the driver for decision-making. The EU regulation defines a legal framework in which the utilities can implement the deployment and exploitation of smart meters with more or less focus on customers. However, the long term development of smart grid technology will change the status of consumers to prosumers and they should be treated as such: collaborators providing services to the grid. In an era where leakage of data is making newspapers' headlines on a regular basis, this is the only reasonable way to build an sustainable relationship between domestic customers and utilities. Hence a balance between the necessity of data to build the smart grid and the respect of the customers as partners has to be determined.

The following discussion is delimited by the legal and technical background of the roll-out and smart meters data utilization in relation to privacy and data accessibility (Section 2). However privacy is not only dependant on the legal and technical aspects but also depends on what the citizens are willing to give. As privacy is the most important issue raised with smart meters, it is crucial to understand what we mean today by privacy and what is really at stakes in this context when it is jeopardized (Section 3). In terms of ethics, the transition to smart grid redistributes the cards between utilities and consumers (prosumers) as the latter have a more important role now than before (Section 4). Customers are also exposed in giving away sensitive data to utilities and it has to be acknowledge and rewarded in an ethical manner (Section 5). The conclusions are gathered in Section 6 while opening up to broader perspectives.

2. Legal and technical background in relation to smart meters' data privacy

The legal framework of data protection and privacy has evolved over time, mainly due to the emergence of new technologies and new threats to privacy they create (Horne et al., 2015). Here we aim at giving the background to both legal and technical aspects that are shaping data collection and use of data generated by smart meters. It scopes what is legally possible in Europe and how the technical setup decided by each Member State shapes the relationship between customers and utilities during the roll-out and after.

2.1. A compact historic review of the right to privacy in EU legislation

The origin of the *right to privacy* can be traced back to the Universal Declaration of the Human Rights (article 12) in 1948 (United Nations, 1949). It states that ' *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*'. It aims at protecting the right and interest of individuals rather than the data itself as data collection appeared to generate unexpected impact on individuals life. Soon after, the Council of Europe strengthened it in the European Convention on Human Rights (European Court of Human Rights, 1950).

The growth of information technology in the 1970's, especially in the public sector and in the banking industry, pushed the Committee of Ministers to the Member States to write 2 recommendations (Resolution 23 and 24) stating that every individual whatever his nationality or residence should have respect for his right to privacy with regards to automatic processing of personal data. These resolutions were received positively and the Council of Europe implemented them in the Data Protection Convention which had impact beyond Europe, as 46 countries ratified it (Council of Europe, 1985). It defines the concept of *personal data* as '*any information relating to an identified or identifiable individual ('data subject')*' and sets the foundation of data protection at an international level. The aim of the Convention is to protect individuals against unjustified collection, use and dissemination of personal data. It then implicitly defines what will later be called *legitimate purpose*.

After years of negotiation between the Member States, the Data Protection Directive (Directive 95/46/EC) was adopted in order to harmonize the legal framework (European Parliament, 1995). Some precisions were added to the definition of *personal data* about what *identifiable* meant; ' *an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*'. It remains broad on purpose to extend its application to future information technologies. Despite being implemented on the same basic principles, it has generated different applications[1]. The Data Protection Directive is articulated around three points; i) transparency: information on personal data being processed; ii) legitimate purpose: specification, explicit and legitimate of

[1] As an EU Directive, it is applicable to all Member States but each Member States transposes it in its national law

the purposes of the data collection; iii) parsimony: adequacy to the purpose of the personal data collected.

Article 7 stipulates the lawful basis to process personal data:

(a) unambiguously consent; or

(b) processing is necessary for the performance of a contract; or

(c) processing is necessary for compliance with a legal obligation; or

(d) processing is necessary in order to protect vital interests; or

(e) processing is necessary for the performance of a task carried out in the public interest; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party.

In order to harmonize the Data Protection Directive among the EU Member States, the European Commission proposed the General Data Protection Regulation (GDPR) in 2012 (European Union, 2016). It generalizes the basic principle of the Data Protection Directive and develops some further rules that are applicable to all data collected inside the EU by European or non-European organizations.

The main changes on the rights of the data subjects and responsibilities of controllers and processors in relation to data protection and privacy of the data subject are:

- Explicit and provable consent (instead of unambiguous consent)(Article 7).
- Transparency and modalities: The data controller should inform and communicate with the data subject in a *'concise, transparent, intelligible and easily accessible form, using clear and plain language'* (Article 12(1)). It should also facilitate the exercise of the data subject rights (Article 12(2)).
- Rectification and erasure: A person has the right: to ask for his data to be erased (Article 17); to restrict the processing under certain condition (Article 18); to transfer personal data from one service to another (Data portability Article 20).
- Right to object to automated individual decision-making (Articles 21 and 22).
- Data Protection by design and by default: The data protection and privacy should be included in the development of the service and the privacy settings should be set to a high level by default (Article 25).
- Communication of a personal data breach to the data subject (Article 34).

From the foundation of the right to privacy to the GDPR, the definition of privacy and data protection had to be updated according to the development of information technologies which is going at a hectic pace. Nevertheless, the following discussion on smart meter data and their ethical use is bounded within the EU by this legal framework.

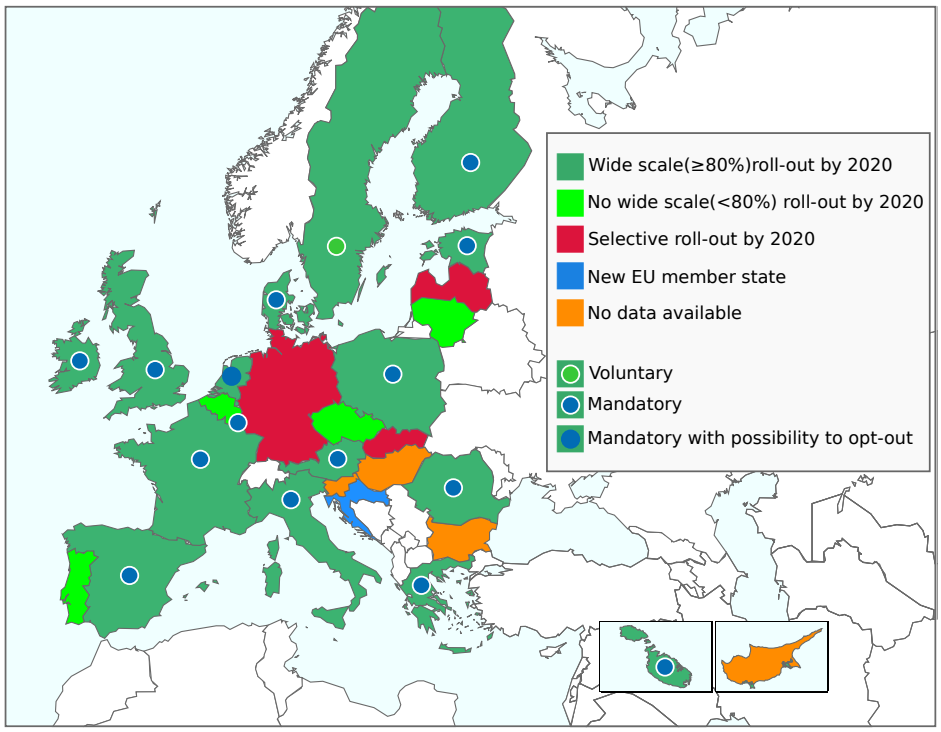

Figure 2: Map of the roll-out of Smart meters in Europe (European Commission, 2014).

2.2. A review of roll-outs and setups of smart metering in the EU

In the case of smart meters, the technological possibilities as well as deployment strategies are directly related to the problem of privacy and ethics . The scale of roll-out is decided based on a cost-benefit analysis (CBA), described in (European Commission, 2011), which concludes wether the roll-out should be at least 80%, less or just selective. However the roll-out strategy is left completely to each EU Member State which gives a large diversity of setups and subsequently different data flows. Table 1 gives an overview of the roll-out status of the different Member States in 2014. The map in Figure 2 presents the roll-out scale as well as the recruitment strategy. Table 1 and Figure 2 give an overview of the diversity and the number of parameters to take into account in the roll-out of smart meters in EU. Temporal disparities are also observed; Italy and Sweden had already completed the deployment of smart meters before the adoption of the directive 2012/27/EU. The Netherlands had planned an early deployment but the roll-out which was originally mandatory has been challenged by consumer protection organizations that sued the State to obtain the possibility to opt-out (Hoenkamp et al., 2011).

Smart metering has also changed the responsibilities of the DSO and TSO as they have to handle large amount of data. Figure 3 is a schematic representation of the flow of data and actions between the different actors. The role of the data controllers, data protection officer and supervisory authority are defined in the GDPR (European Union, 2016) and are taken in most cases by the DSO, TSO or independent organism (Smart Grids Task Force Expert Group 1- Standards and Interoperability, 2016). It could be considered in the con-

Table 1: Overview of the roll-out (in 2014) in EU. Source: European Commission (2014)

Member State	roll-out scale	CBA[a] outcome	resolution	implementation/ownership	storage	Financing of the roll-out
Austria	95%	+	15 min	DSO	DSO	Metering & network tariffs
Belgium	<80%	-	NS[b]	DSO	DSO	Network tariffs
Bulgaria	TBA[c]	NA	NA	NA	NA	NA
Croatia[d]	NA[e]	NA	NA	NA	NA	NA
Cyprus	TBA	NA	NS	DSO	DSO	NA
Czech Republic	1%	-	NS	DSO	Central Hub	NA
Denmark	100%	+	15 min (hourly before 2011)	DSO	Central Hub	Network tariffs
Estonia	100%	+	hourly	DSO	Central Hub	Network tariffs
Finland	100%	+	1 hour (RT optional)	DSO	DSO	Network tariffs
France	95%	+	10-30 min	DSO/municipalities	DSO	NA
Germany	23%	-	15 min	DSO or meter operator	DSO or meter operator	NA
Greece	80%	+	NS	DSO	DSO	NA
Great Britain	99.5%	+	30 min (10s to customer)	Supplier	Central Hub	Funded by suppliers
Hungary	TBA	+	NS	NA	NA	NA
Ireland	100%	+	30 min (10s to customer)	DSO	DSO	Network tariffs
Italy	99%	NA	10 min	DSO	DSO	DSO & Network tariffs
Latvia	23%	-	NS	DSO	DSO	Network tariffs
Lithuania	<80%	-	NS	DSO	DSO	Network tariffs
Luxembourg	95%	+	NS	DSO	DSO	Network tariffs
Malta	100%	NA	NS	DSO	DSO	Network tariffs
Netherlands	100%	+	NS	DSO	DSO	Network tariffs
Poland	80%	+	NS	DSO	Central Hub	Network tariffs
Portugal	<80%	Inconclusive	15 min	DSO	DSO	DSO & Network tariffs
Romania	80%	+	NS	DSO	DSO	Network tariffs
Slovakia	23%	-	15 min	DSO	DSO/Central Hub	DSO & Network tariffs
Slovenia	TBA	NA	NS	NA	DSO	NA
Spain	100%	NA	NA	DSO	DSO	Network tariffs & SM rental
Sweden	100%	+	hourly	DSO	DSO	DSO &Network tariffs

[a] Cost-benefit analysis [b] Not Specified [c] To be announced [d] New Member State [e] missing information

text of smart metering as the perfect flow of data according to Nissenbaum (2011).

Some parameters, like the resolution of the data, the access to metering data and the implementation/ownership, have a direct impact on the setup and thus the data flow as shown in Figure 3 as well as the capacity of the customer to modify its consumption. The range of possibilities makes it difficult to standardize, however most of the DSOs, as responsible authorities of the roll-out, (will) face the same ethical problems with their customers.

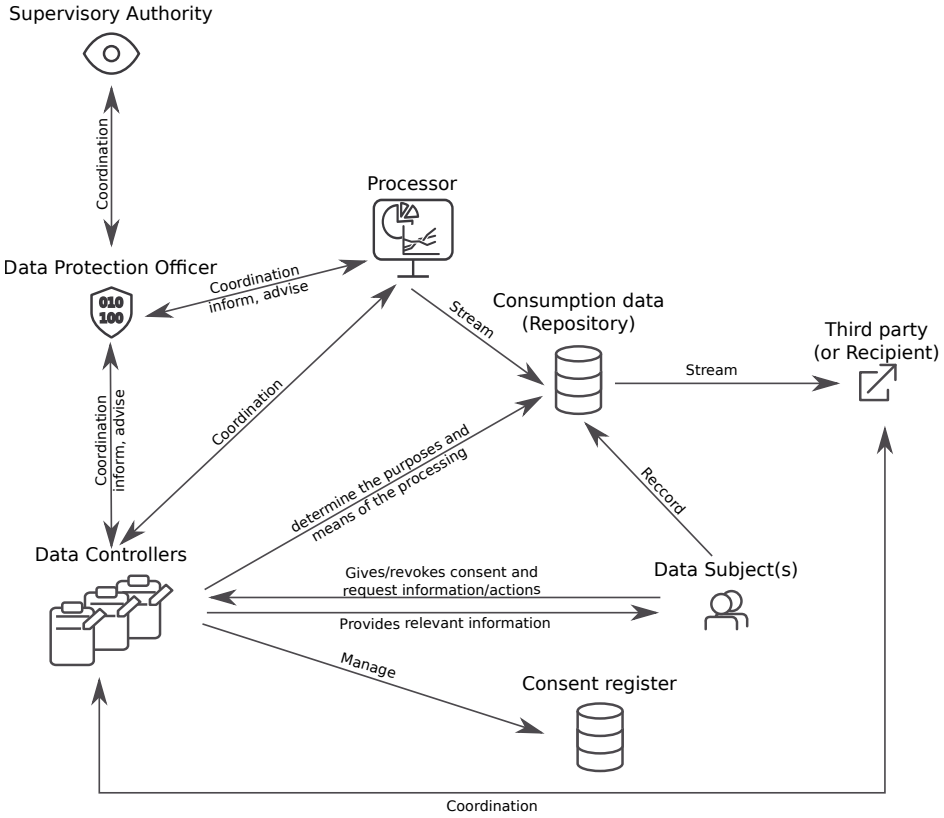

Figure 3: Interaction of actors and flow of smart meter data as described in the GDPR. Source: (Smart Grids Task Force Expert Group 1- Standards and Interoperability (2016)).

3. What privacy today?

Privacy is a generic word used to describe what we perceive as relating to private matters. Nevertheless the definition of privacy is evolving over time. In this section we give some examples revealing today's state of privacy and how much data we accept to give to obtain a service. A discussion is as well open on what is at stake when we talk about privacy breaching.

3.1. The state of privacy in the Big Data era

We have entered a new era called the *'Big Data era'* (Wladawsky-Berger, 2015). Despite the term 'big', the root of Big Data pertains to *(i)* volume: the quantity of data being

collected is growing exponentially (OECD, 2013); *(ii)* velocity: The resolution at which data is being collected increases steadily; and *(iii)* variety: The sources of data are getting more diverse. From the Data Protection Directive, data can be categorized into 2 types, personal data, which are protected by law and the non-personal data (European Commission, 2018). Hence to go around restrictions on the use of personal data, the best way is to collect *more* non-personal data that can be combined to create a unique profile, defining an individual.

On the Internet, the most generic data collected concerns navigation information (i.e. browsing) and clicks. Cookies, saved on each computer, have been used to collect navigation information on users. Users' navigation information are then used to generate target advertisement. In Europe and until 2011, website were not asking for consent on using cookies. In 2011, the so called *'EU cookie legislation'*, Directive 2009/136/EC, detailing the use of cookies was added to Directive 2002/58/EC on digital user rights (European Parliament, 2009a). It stipulates that cookie ID are considered *personal data* from now on, and requires any website to ask for users' consent to retrieve information stored on cookies. Despite the efforts of the European Commission to regulate the exploitation of navigation information, new ways of collecting those information were already implemented. In order to optimize their visual aspect, websites collect information concerning the hardware (e.g. screen, computer) and the software (i.e. the browser type and version) with the genuine aim to give the best user experience. However it can form a unique combination which is called a *'browser fingerprint'* (Laperdrix et al., 2016). To be close to unique the fingerprint of a browser requires approximately 17 parameters. Thereby cookies are becoming obsolete and the online advertisement business is still monetizing browsing information while avoiding legislation.

Google and Facebook emphasize concerns about data privacy as they have always been at the forefront of the data monetizing business models, providing services for free and monetizing data via advertisement. Thanks to the dimensions of their pool of users, they are self-sufficient in data to feed their advertisement algorithm. In 2017, Alphabet's (parent company of Google and Youtube) and Facebook's digital advertisement revenues combined represented a gigantic 191,8 Billion US dollars (respectively 123.5 B$ and 68.3 B$) which represents half of the global digital advertising revenue (Molla, 2018). In itself only, the use of data for targeted advertisement is not much of a problem and can be considered as annoying when it is excessive. The problems comes out of the methods used to maximize revenues.

Facebook generates a unique dataset which appeals psychometricians studying human behavior. The collection of *likes* from users can be used to generate really precise psychological profiles like the *'Big five'* (Kosinski et al., 2013, McCrae and John, 1992, Gosling et al., 2011). The Cambridge Analytica Scandal made citizens aware of how a breach into the security could contribute to private interests. Data from 100 000 of Facebook's users were originally collected with their consent for research. Despite rules and Non-Disclosure Agreements, access was given to Cambridge Analytica which extended the data to 30 millions users using interconnections between *friended* users. Data was thereafter not used for research but to influence opinions through the targeted advertising algorithm of Facebook. The use of the data is thus not as questionable as the purpose. The exploitation of such a unique dataset for research purposes is valuable, however the use of such a dataset for

influencing opinion is a serious law infringement (Kosinski et al., 2015).

The *'privacy by default'* Article in the GDPR, has probably been designed based on the experience with Facebook's default privacy settings. Indeed, Facebook's privacy settings were left to minimum level so that user's profiles could be *searchable*, and partly *visible* to all members, thus increasing traffic (Gross et al., 2005, Liu et al., 2011). From a user's point of view, they have to know i) that access to their account is not restricted to 'friends' ii) that they should know how to restrict access (Liu et al., 2011). The configuration as default to the lightest security settings is questionable from a user perspective, as their personal information are not protected by default despite existence of such parameters. Social networks benefit from data placed in them but they benefit even more of connections created between user profiles (see (Mcdonald and Ackerman, 2000) for more information) and generate their advertisement revenue from the traffic. Usually users become aware of privacy issues, when terms and privacy policies have to be updated and some may modify their privacy settings but the large majority does not, as it is a non trivial operation (Liu et al., 2011).

The use of smart phones and smart city application (e.g. public transportation card, traffic) adds a geographical dimension to information collected that anchors it in the physical world. Using mobility data from carriers' antennas it has been demonstrated that only 4 spatio-temporal points are needed to uniquely identify each carrier (De Montjoye et al., 2013). Using GPS data, the number of points decreases to collect unique patterns. Spatio-temporal data are highly sensitive personal data, information on where an individual is at any time can be used to intercept physical someone. They are personal data as they allow to uniquely identify a person from his data.

The Big Data era has induced in citizens a certain distrust as well as a necessity to stay connected, which create a ambivalent perception of technological products.

3.2. Privacy is not the problem anymore

Privacy comes from the Latin word *privatus* which means 'withdraw from public life'. Indeed the strict definition and application of privacy implies that each individual should not in any way be uniquely identifiable using the collected data (United Nations, 1949). But as the legal framework on data protection and privacy evolves with the emergence of new information technologies, the concept of privacy evolves as well. Privacy is usually guaranteed to data subjects by collecting data anonymously in the sense of *namelessness* (i.e. not identified by name, address, social security number). Examples have been given in Section 3.1 that shows that anonymized data can actually be used to uniquely identify individuals and thus questions the use of anonymity to protect privacy. Indeed, anonymity is used to collect data without naming the data subject but keep them identifiable (Laperdrix et al., 2016, De Montjoye et al., 2013). It is important here to understand what is at stake in that context: names have no importance in themselves. But identities,sets of information which define each individual, are extremely valuable as well as sensitive. Personal data can be combined with other non-personal data to identify, contact or locate a *single* person. Discarding all these information, is actually a way to keep them *anonymous* (i.e. nameless)

but still uniquely identifiable. Google has even created a word to describe these paradoxical IDs, *'anonymous identifier'*, which they use for targeted advertisement (Kitchin, 2016, Barocas and Nissenbaum, 2014).

A question arises then, how many data points are needed to uniquely identify users? Considering the profuseness of possibilities, only a few data points are needed to create a combination that uniquely identifies a user (Laperdrix et al., 2016, De Montjoye et al., 2013). The problem appears when the data collected can provide sufficient information to reach a person physically (e.g. through email, phone, address). Barocas and Nissenbaum (2014) argue that the real value in anonymity is to prevent *reachability*, not to protect privacy. From collected data it should not be possible to communicate or reach physically data subjects. This concept is then much more meaningful and reshapes also the concept of privacy. It does not apply only to personal data but also to non-personal data that could be used to reach a person. In (Acquisti and Gross, 2009) an algorithm is built to predict social security numbers of American citizen based on their date and place of birth. They reach success rates from 7% to 61% in predicting the 5 first numbers (out of 9) using publicly available data depending on the period and state of birth. It proves that *any personal information can be sensitive information* when combined appropriately (Acquisti and Gross, 2009).

Respecting privacy is not respecting secrecy or granting control over personal information. It consists of respecting an appropriate flow of information. Nissenbaum (2011) calls it contextual integrity; data (type of information) collected in a certain context (e.g. finance, health, social norms) flow, following transmission principles (e.g. consent, buying, selling, confidentiality), between different actors (e.g. subject, sender, recipient) in an appropriate manner. Disruptive practices modifying the information flow are evaluated depending on how they move it from the ideal information flow. In other words, it evaluates the impact of disruptive flows on ethical values like fairness, justice, freedom, welfare or any other context specific concepts.

Figure 3 could be a representation of the perfect flow of information in a smart metering context. In the reality, from an ethical perspective, the relationships between utilities and consumers are far from perfect. The major problems are around data collection and the change of status of the actors.

4. Customers should be treated as collaborators

GDPR sets standards for data protection and privacy and the Third Energy Package gives guidelines and objectives for the roll-out and use of smart meters. However in this new context of smart grid there are no clear guidelines or rules on how to work with customers. The main challenge is to keep a positive relationship between utilities and (domestic) customers in order to secure the investment and involve them as actors of the grid (Bertoldo et al., 2015).

4.1. An ethical roll-out to improve acceptance of the customers

The roll-out scales as defined in the CBA (Figure 2) have been decided at the EU level and the DSOs are following the decision in deploying the smart meters. However the decision

to make the installation mandatory is raising concerns throughout Europe. As presented in Section 3 several privacy scandals have raised awareness about privacy issues and this should not be neglected. From a customer perspective, the roll-out of smart meters, especially when mandatory, is an intrusion to what is perceived as the last sanctuary of privacy, 'Home' (Papakonstantinou and Kloza, 2015). Indeed a meter is a foreign object in a household that inhabitants do not own (it is the DSO's property) and cannot remove/modify. The adoption of the technology depends on the perception of the customers (Ponce et al., 2016). The European Commission gave some guidelines on conducing the cost-benefit analysis where '*an assessment of the level of social resistance (or participation) to the project should be presented, including a description of means adopted to ensure social acceptance and their effectiveness*' (Papakonstantinou and Kloza, 2015). The customers are either putting high expectation in smart meters (technophiles) and get disappointed, or they have realistic fears regarding privacy breaching and loss of control (Krishnamurti et al., 2012). Hence both situations lead to a negative perception of smart meters. To have a positive impact, the benefits of smart meters should be clearly stated and visible rapidly after installation to maximize customers' acceptance of the new technology.

The case of the Netherlands can be used as an example of what can go wrong when end-users are not considered properly in the smart metering framework (Hoenkamp et al., 2011). Originally the roll-out was mandatory and refusing the installation was made punishable as an economic offense, with a fine of 17.000€ or imprisonment for a maximum of six months (Gutwirth et al., 2013). Beside privacy concerns transmitted to the Dutch Data Protection Authority on the use of high resolution data, the utilities were not inclined to focus on a customers inclusive solution to stimulate demand flexibility (Hoenkamp et al., 2011). The Minister of Economic Affairs amended the Dutch Data Protection Authority's proposal by stipulating that the network operator could transfer hourly or 15-minute metering data to the energy provider only if the customer gave his consent. To add up to the pile, the Dutch Consumer Union published a report stipulating that a mandatory roll-out of smart meter reporting 15-minute electricity information was an infringement of the right to privacy according to the article 8 of the European Convention on Human Right (European Court of Human Rights, 1950) and was thus not compatible with a democratic society. The problem was finally solved at the Senate by giving the right to customers to refuse having a smart meter installed (opt-out). Gutwirth et al. (2013) considered that there are four factors for the rejection of the smart meter bill by the Senate 1) the high resolution of the data transferred up to the energy providers, 2) the mandatory roll-out where resistance is sanctioned by high fines or even imprisonment, 3) lack of explanation of the necessity of smart metering and by extension why the customers have to loose some privacy 4) the combinations of different functionalities in one meter generating new risk and making the argumentation complex.

Research in social science on the topic of smart meters have also shown large misalignment between the reality of the smart meters and customers' expectations. From a customer point of view, just the fact that a digital connected meter is called 'smart' is actually inducing a wrong idea of what are its capabilities, since it is not a smart home system (Wilson et al., 2017). This is a recipe for backlash. In Krishnamurti et al. (2012), a behavioral study shows that most of the concerns and deceptions from the roll-out of smart meters could be

solved in two ways 1) scale down the expectation of the customers in explaining clearly what the smart meters could do; 2) align the technology with the expectation by adding smart thermostats and in-home displays to visualize consumption in real-time. The smart grid framework requires that the customers know what their metering data is used for, even if it is technical, stakeholders have the responsibility of informing in a clear and understandable manner (Bertoldo et al., 2015).

4.2. Evolution of the roles and relationships

The relationship between utilities and customers is ultimately changing due to potential consequences from two-way communication and deployment of decentralized generation (Khurana et al., 2010). Consumers become prosumers and provide service to the grid, they are actors of the grid and should be considered as collaborators in maintaining stability of the grid. The European utilities have operated in the last decade important restructurations to cope with the opening of the energy market to concurrence. Indeed they (e.g. EDF in France, ENEL in Italy, DONG in Denmark) used to be monopolistic and control the network from generation to distribution. As national companies they had the trust of customers. Today the trust-relationship has to be rebuilt between customers and utilities to operate this transition and find a new balance between the actors of the grid. The goals of the relationship remain unclear to some extend as the benefits and the expectations are not aligned (Horne et al., 2015). For example, the customers are expected to be more active but smart meters alone do not provide this functionality, it requires an additionally smart home device. Additionally the contribution of customers to the stability and reliability of the grid should be highlighted as it can be used to develop new social norms in relation to energy (Horne et al., 2015).

The development of aggregators could play an important role in 'smoothing' the communication between the utilities and the customers as they would have less customers to handle. Indeed beyond their technical role they could act as representatives of the customers to utilities and have more weight in the decision making.

4.3. Smart meters to empower customers to become prosumers

The smart grid aims at transforming a centralized, utility-controlled network into a decentralized, consumer-interactive network allowed by high-resolution monitoring and two-way communication (Khurana et al., 2010). From a utility perspective, the need of metering data is almost mechanical. Indeed, a higher share of RES in the generation mix, as promoted by EU, makes generation less adjustable to the demand. In order to compensate the lack of flexibility on the generation side, the demand could be modulated according to some incentives (i.e. price, benefit) broadcast to the customers using a two-way communication (Finster and Baumgart, 2014).

Demand side management (DSM) programs have been studied and implemented based on the idea of exploiting demand-side flexibility to reduce RES spillage (Strbac, 2008). DSM (including DR frameworks as well as more complex pricing scheme) relies on a marginal dynamic price of generation (Ding et al., 2013). Figure 4 gives an overview of the different price based solutions that can be used depending on resolutions of both price and metered

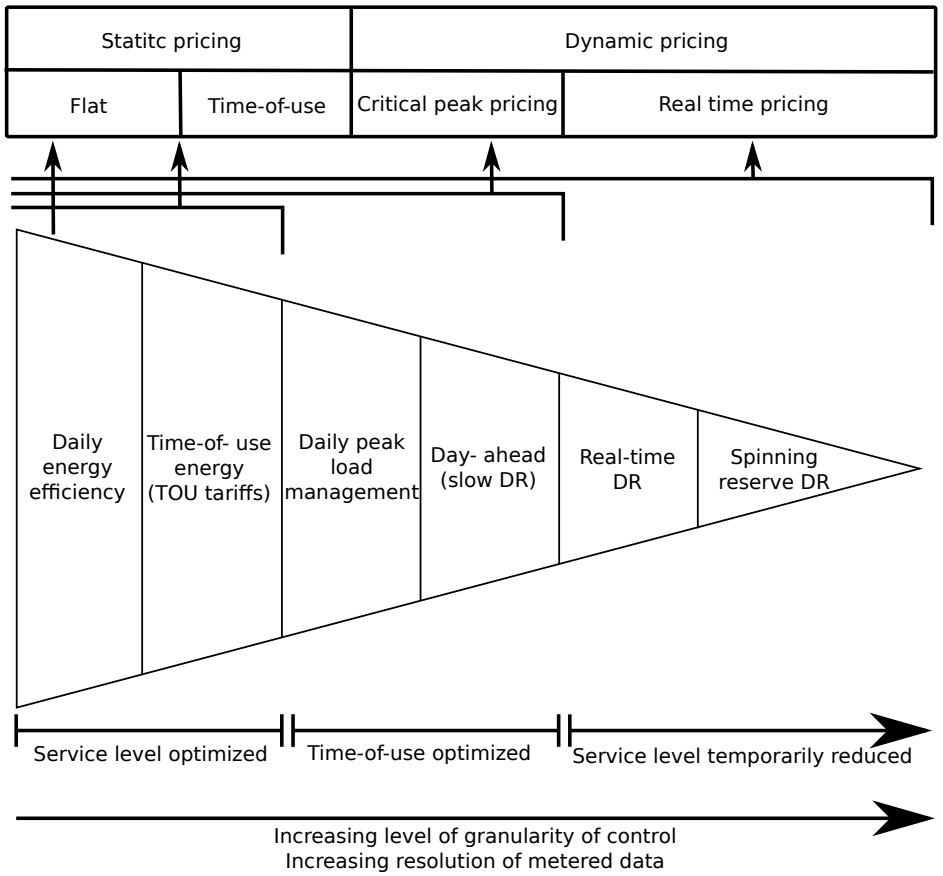

Figure 4: DSM service enabled in function of the resolution of the metering. Source: Siano (2014).

data. To generate the corresponding bill, the energy providers need to know exactly how much power each customer has consumed during each time interval. Hence the resolution of the metered data should then be higher than (or equal to) the one from the dynamic tariff. In such a framework, it is important that customers can access their electricity consumption and dynamic tariff to modify their energy behavior or to automate their white appliances (i.e. dishwasher, washing machine, electric heating) accordingly. High resolution metering is then a way to make customers aware of their energy behavior so that they can shift their consumption from passive (consumers) to active (prosumers) who will provide services to the grid (Chicco, 2016). The incentive used to change the electricity consumption behavior of customers does not have to be financial, social norms are a powerful tool to change behaviors (Allcott, 2011). However, for such incentives to have a positive impact, the relationship between the utilities and the customer has to be positive as well (Horne et al., 2015). A customer who manages correctly his consumption, should then be encouraged in getting electricity cost reductions (McDaniel and McLaughlin, 2009, Klass and Wilson, 2016).

In the context of smart grid, new business models and actors (aggregators) are relying on metering data to create portfolios and manage their assets (Bondy et al., 2015). How-

ever, it has been demonstrated that the success of such frameworks depends heavily on the magnitude of demand response triggered and subsequently active customers (Pepermans, 2014).

4.4. Control of access transferred to the data subject

The electricity metering data are stored on a datahub or on the DSO servers (Table 1). A consent register, as presented in Figure 3, can be created to record which third parties get access to the data. The consent register is here managed by the data controller (DSO) but it could have the form of the 'App' system developed for smartphones (Smart Grids Task Force Expert Group 1- Standards and Interoperability, 2016) where customers directly manage access grants. Hence it will transfer responsibilities, risk assessment and control to the data subject. It could then also generate the same problems as with 'Apps' on smartphones that are asking for access to data which are not useful to the service provided. A third party can access data at high resolution (up to 1s depending on the model) wire or wireless to smart meters using a dedicated port. Again if there is no illegal intrusion to the household, it is assumed that customers should have control over what is connected to the port. The risk of an abusive use of metering data by a third party is increased if the customers are not educated and made aware of how sensitive those data can be (as we can observe with smartphones). The risk being that information in the data, state of white appliances for example, are extracted and used by an unsolicited third parties for sending targeted advertisement suggesting to replace an appliance (Finster and Baumgart, 2014).

The change from consumer to prosumer comes with changes in the distribution of the responsibilities and control between the actors of the grid. Indeed a prosumer needs to control his/her consumption to act as such and provide services to the grid. The hierarchical structure of the actors of the grid, with consumers/prosumers at the bottom and utilities at the top, is actually, changing. The structure is flatter and prosumers are collaborators rather than consumers. Adjustment in terms of consideration have to occur.

5. Requirements in terms of ethics

Good practices can be implemented to make the roll-out and the use of metering data more ethical. It mainly consists of two global concept parsimony and equity. The need of data is acknowledged, nevertheless it should be parsimonious and come with a direct benefit to the data subject. Hence both parties would be satisfied.

5.1. Data resolution in accordance to task to fulfill

Privacy concerns are often about the high resolution of metering data- (McKenna et al., 2012). Obviously the higher the resolution the more precise the information (See Figure 5). By extension, concerns are also related to machine learning algorithm fed with such data like Non-Intrusive Load Monitoring (NILM) (Klemenjak and Goldsborough, 2016). Beyond the potential information that can be extracted, the targeted use of the information is of higher interest. NILM applications, for example, are made in a certain context; it consists of providing detailed information of individual appliances consumption to customers, who

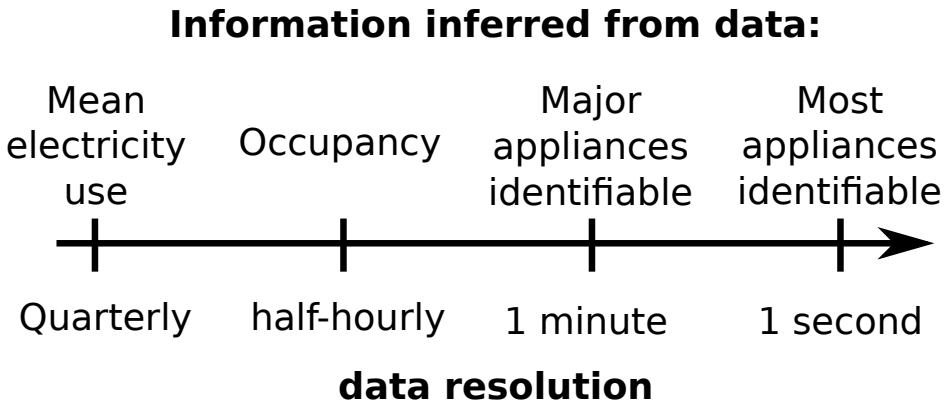

Figure 5: Representation of information that can be inferred from metering data in function of the resolution. Source:McKenna et al. (2012).

are also data subject, so that they can identify appliances with large unnecessary electricity consumption. This information should be provided to no one else. We could also imagine the use of NILM on data at lower resolution to identify large and potentially flexible appliances. Hence DSOs could use this information to propose flexibility contracts to customers; it would be beneficial for every party if the benefits are fairly distributed.

Different tasks can be completed using metering data but they do not require the same level of information (data resolution). The data resolution should therefore be adjusted in accordance to the task to fulfill. In the same way that the purpose has to be legitimate, the resolution of the data has to be legitimate. For example when billing customers under dynamic tariff, it does not improve anything to use electricity consumption at a higher resolution that the dynamic tariff. Hence the resolution of the data should be chosen parsimoniously.

5.2. New risks require compensation

As with any connected device (e.g. computers, Internet of Things devices), a risk of cyberattack exists. It can be organized by a foreign governmental agency, a malicious person or a malicious software (Knyrim and Trieb, 2011). The Russian attack on Ukrainian DSO Kyivoblenergo on December 23, 2015 is the first example of such an organized cyberattack used to temporarily shut down 30 substations of the distribution grid (Lee et al., 2016). The grid is a strategic target and the use of digital central control system makes them obvious targets for cyberattack. However, the attack did not target metering data but the stability of the grid which in this specific case do not affect privacy. Nevertheless, a cyberattack could also be conducted by customers on their own smart meter to steal electricity (McDaniel and McLaughlin, 2009, Colak et al., 2016), or by a malicious person on a specific customer to spy on him (McKenna et al., 2012).

Hence customers are exposed to new risks of privacy breaching in giving access to their metering data. The risk is considered and efforts on securing communication are made to limit it. However, the risk is not null, and it should be addressed with compensations/benefits (Wilson et al., 2017). As utilities transfer the cost of smart meters to the

customers (Table 1), it would fair that customers get rewarded according to the amount of information transmitted to utilities (Culnan and Bies, 2003).

We could imagine a voluntary basis system where customers could chose the resolution of the data provided and would have tariff/remunerations accordingly. The differences between the static tariff (i.e. for non-metered customers) and dynamic tariff (i.e. for metered customers) should then take into account the marginal cost of generation but also a deduction for providing data for the forecast of the demand.

5.3. Balance of the benefits

Balancing the benefits resides in a trade-off between the loss of privacy and increased risk for customer and the need of metering data for utilities (Culnan and Bies, 2003). We want to show that it is possible (even necessary) to do it ethically in order to be sustainable and avoid a future backlash (Zachary, 2011).

Today the benefits of smart metering are going toward the utilities which are saving cost of employing meter readers, process invoice automatically and get more insights on the grid for fraud detection and maintenance (Hu et al., 2015). As the meters are payed mostly through network tariffs (only Italy, Romania, Slovakia and Sweden are sharing costs between customers and DSO see Table 1), the tariff reductions due to potential savings will be, in a first time, shortened on the customer side. Real-time data has not shown that much interest and it seems fair to think that it will take some years before the technology becomes mature enough to deploy large scale DSM application. Hence until dynamic tariffs are generalized to all EU Member States, some customers will pay for the technology without having any of the benefits. The access given to consult and analyze electricity consumption, as promoted by EU, would then have only little impact, as the customers could only reduce their consumption to reduce their electricity bill.

Moreover, customers undercharged because of malfunctioning electromagnetic meters, which is common because of the advanced age of electromagnetic meters, will observe an increase of their electricity bill due to increased metering accuracy (Krishnamurti et al., 2012). A more precise billing means also that it is easier for the energy providers to detect fraud in comparison to annual metering on electromagnetic meters. To give an idea of the cost of electricity theft, it is responsible in 2000 in the US of 0.5% to 3.5% losses of the annual growth revenue which seems low but still represents $10 billions, compensated by higher price on the other customers (Smith, 2004). With smart meters, the risk of undetected frauds decreases which means that theoretically the cost of the fraud is reduced and can be translated into lower prices. Fraud is better monitored, but at the same time, the risk of electrocution in compromising smart meters (i.e. through software) is much lower than with electromagnetic meters and thus less repealing to possible thieves (McDaniel and McLaughlin, 2009).

Smart meters are part of the Advanced Metering Infrastructure (AMI) which forms the informational backbone of the smart grid and makes the grid smart. From a DSOs perspective, AMI allows them to have precise information about the power flows at a distribution level beyond the substations. Again this value of metering is emphasized by the increase of variable RES in the generation mix and decentralized generation down to the distribution

level (Finster and Baumgart, 2014). This way it lower the risks of outages, the DSOs can also anticipate the maintenance and solve problems faster as they do not need customers' calls to be aware of them.

Whatever the decision taken to increase the capacity of RES and subsequently to limit climate change due to electricity generation, dynamic information on the demand side will be required to optimally use RES, invoice prosumers and balance the generation with the demand (Klass and Wilson, 2016). Hence the roll-out of smart meter from a environment and grid management perspective is not negotiable, but the way the data is used and how the benefit of such infrastructure will be shared are still under discussion. If as in the case of the Netherlands (Hoenkamp et al., 2011), an opt-out is negotiated in most of the member states, customers will perform a cost-benefit analysis between the loss of privacy and the social, economical benefits generated (Culnan and Bies, 2003). The worst scenario could lead to the loss of an important part of the metered households.

6. Conclusions and perspectives

Utilities are putting efforts in complying with the GDPR. GDPR however only protects the basic rights of the data subjects (i.e. customers). Nevertheless DSOs must also respect the agenda of the Third Energy Package and deploy smart meters in due time. Hence mandatory installation of smart meters appears to be a good solution. This is not counting on possible backlash of the customers. The Netherlands' case gives us a picture of what could happen in EU during the next years (Hoenkamp et al., 2011).

Bad practices during the roll-out (e.g. installing smart meters without informing customers) are giving a negative image of smart grid technology to the customers. The fact that it is required to improve the use of RES or that it is imposed by EU are not arguments supporting the implementation of smart grid as it is right now. On the contrary, all the technological development and investment would be a vain attempt if customers do not adopt or at least accept the technology in a first time. Problems may not rise during the roll-out but also afterwards as the relationship is dynamic and requires efforts on both side to be fruitful.

It becomes then clear that insights from social science are necessary to understand how customers are perceiving 'smart meters' in *their* home. Indeed, from a engineer point of view, customer as non-rational in its decision making is often seen as a problem. Hence only the technico-economic aspects of the problem are used to evaluate a framework. The use of social science like consumer science, justice research, ethics and anthropology to large infrastructure projects involving citizens has shown positive influence on their perception regarding potentially non-appreciated project (i.e. construction of a dam, road).

In the general context of climate change, citizens have become aware at different levels of their responsibilities as well as how they can influence the outcome. Energy and electricity by extension, represents one of the fields were awareness is growing rapidly. It seems that customers are ready to become actors of the grid and support the development toward a greener electricity generation but not at any cost.

Acknowledgement

The authors thank the EUDP for funding through the EnergyLab Nordhavn project (EUDP 64015-0055).

References

Acquisti, A., Gross, R., 2009. Predicting Social Security numbers from public data. Proceedings of the National Academy of Sciences of the United States of America 106 (27), 10975–10980.

Allcott, H., 2011. Social norms and energy conservation. Journal of public Economics 95 (9-10), 1082–1095.

Barocas, S., Nissenbaum, H., 2014. Big data's end run around anonymity and consent. Cambridge University Press, NY.

Bertoldo, R., Poumadère, M., Rodrigues, L. C., 2015. When meters start to talk: The public's encounter with smart meters in France. Energy Research and Social Science.

Bondy, D. E. M., Heussen, K., Gehrke, O., Thavlov, A., 2015. A Functional Reference Architecture for Aggregators. In: IEEE International Conference on Emerging Technologies and Factory Automation, ETFA. Vol. 2015-Octob. pp. 1–7.

Chicco, G., 2016. Customer behaviour and data analytics. In: Proceedings of the 2016 International Conference and Exposition on Electrical and Power Engineering, EPE 2016. pp. 771–779.

Colak, I., Sagiroglu, S., Fulli, G., Yesilbudak, M., Covrig, C.-F., 2016. A survey on the critical issues in smart grid technologies. Renewable and Sustainable Energy Reviews 54, 396–405.

Council of Europe, 1985. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Culnan, M. J., Bies, R. J., 2003. Consumer privacy: Balancing economic and justice considerations. Journal of social issues 59 (2), 323–342.

De Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., Blondel, V. D., 2013. Unique in the crowd: The privacy bounds of human mobility. Scientific reports 3.

Ding, Y., Pineda, S., Nyeng, P., Østergaard, J., Larsen, E. M., Wu, Q., 2013. Real-time market concept architecture for EcoGrid EU - A prototype for European smart grids. IEEE Transactions on Smart Grid 4 (4), 2006–2016.

European Commission, 2011. Energy Efficiency Plan 2011. Tech. rep., European Commission.

European Commission, 2014. Benchmarking smart metering deployment in the EU-27 with a focus on electricity. European Commission, 1–10.

European Commission, 2018. What is personal data? URL https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data{_}en

European Court of Human Rights, 1950. European Convention on Human Rights. Convention for the Protection of Human Rights and Fundamental Freedoms, 30.

European Parliament, 1995. Directive 95/46/EC. Tech. rep., European Parliament.

European Parliament, 2009a. Directive 2009/136/EC. Official Journal of the European Union 337, 11–36.

European Parliament, 2009b. Directive 2009/29/EC. Official Journal of the European Union 140, 63–87.

European Parliament, 2012. Directive 2012/27/EU. Official Journal of the European Union L315/1 (October), 1–56.

European Union, 2009. Directive of 2009/72/EC. Official Journal of the European Union L211 (August), L 211/55 – L 211/93.

European Union, 2016. Regulation 2016/679. Official Journal of the European Union 2001.

Farhangi, H., 2010. The path of the smart grid. IEEE power and energy magazine 8 (1).

Finster, S., Baumgart, I., 2014. Privacy-aware smart metering: A survey. IEEE Communications Surveys & Tutorials 16 (3), 1732–1745.

Giordano, V., Gangale, F., Fulli, G., Jiménez, M. S., Onyeji, I., Colta, A., Papaioannou, I., Mengolini, A., Alecu, C., Ojala, T., et al., 2011. Smart grid projects in europe. JRC Ref Rep Sy 8.

Gosling, S. D., Augustine, A. A., Vazire, S., Holtzman, N., Gaddis, S., 2011. Manifestations of Personality in Online Social Networks: Self-Reported Facebook-Related Behaviors and Observable Profile Information. Cyberpsychology, Behavior, and Social Networking 14 (9), 483–488.

Gross, R., Acquisti, A., Heinz III, H., 2005. Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM workshop on Privacy in the electronic society. p. 80.

Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y., 2013. European data protection: Coming of age. In: European Data Protection: Coming of Age. Springer Science & Business Media, pp. 1–440.

Hoenkamp, R., Huitema, G. B., de Moor-van Vugt, A. J. C., 2011. Neglected consumer: The case of the smart meter rollout in the netherlands, the. Renewable Energy L. & Policy Rev., 269.

Horne, C., Darras, B., Bean, E., Srivastava, A., Frickel, S., 2015. Privacy, technology, and norms: The case of Smart Meters. Social Science Research.

Hu, Z., Kim, J.-h., Wang, J., Byrne, J., 2015. Review of dynamic pricing programs in the US and Europe: Status quo and policy recommendations. Renewable and Sustainable Energy Reviews 42, 743–751.

Jegen, M., Philion, X. D., 2017. Power and smart meters: A political perspective on the social acceptance of energy projects. Canadian Public Administration 60 (1), 68–88.

Khurana, H., Hadley, M., Lu, N., Frincke, D. A., 2010. Smart-grid security issues. IEEE Security & Privacy 8 (1).

Kitchin, R., 2016. The ethics of smart cities and urban science. Phil. Trans. R. Soc. A 374 (2083), 20160115.

Klass, A. B., Wilson, E. J., 2016. Remaking Energy: The Critical Role of Energy Consumption Data. Cal. L. Rev. 104, 1095.

Klemenjak, C., Goldsborough, P., 2016. Non-Intrusive Load Monitoring: A Review and Outlook. archiv.
URL http://arxiv.org/abs/1610.01191

Knyrim, R., Trieb, G., 2011. Smart metering under EU data protection law. Access 1 (2), 121–128.

Kosinski, M., Matz, S. C., Gosling, S. D., Popov, V., Stillwell, D., 2015. Facebook as a research tool for the social sciences: Opportunities, challenges, ethical considerations, and practical guidelines. American Psychologist 70 (6), 543–556.

Kosinski, M., Stillwell, D., Graepel, T., 2013. Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences 110 (15), 5802–5805.

Krishnamurti, T., Schwartz, D., Davis, A., Fischhoff, B., de Bruin, W. B., Lave, L., Wang, J., 2012. Preparing for smart grid technologies: A behavioral decision research approach to understanding consumer expectations about smart meters. Energy Policy 41, 790–797.

Laperdrix, P., Rudametkin, W., Baudry, B., 2016. Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints. In: 37th IEEE Symposium on Security and Privacy (S&P 2016). pp. 878–894.

Lee, R. M., Assante, M. J., Conway, T., 2016. Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems, 23.
URL https://ics.sans.org/media/E-ISAC{_}SANS{_}Ukraine{_}DUC{_}5.pdf

Liu, Y., Gummadi, K. P., Krishnamurthy, B., Mislove, A., 2011. Analyzing facebook privacy settings: user expectations vs. reality. In: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. ACM, pp. 61–70.

McCrae, R. R., John, O. P., 1992. An introduction to the five-factor model and its applications. Journal of personality 60 (2), 175–215.

McDaniel, P., McLaughlin, S., 2009. Security and privacy challenges in the smart grid. IEEE Security & Privacy 7 (3).

Mcdonald, D. W., Ackerman, M. S., 2000. Expertise recommender: a flexible recommendation system and architecture. In: Proceedings of the ACM conference on Computer supported cooperative work. pp. 231–240.

McKenna, E., Richardson, I., Thomson, M., 2012. Smart meter data: Balancing consumer privacy concerns with legitimate applications. Energy Policy 41, 807–814.

Molla, R., 2018. Google leads the world in digital and mobile ad revenue.
URL hhttps://www.recode.net/2017/7/24/16020330/google-digital-mobile-ad-revenue-world-leader-faceb

Nissenbaum, H., 2011. A Contextual Approach to Privacy Online. Daedalus 140 (4), 32–48.
OECD, 2013. Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data". OECD Digital Economy Papers no. 222.
Papakonstantinou, V., Kloza, D., 2015. Legal Protection of Personal Data in Smart Grid and Smart Metering Systems from the European Perspective. In: Smart Grid Security. London: Springer, Ch. 2, pp. 41–129. URL http://link.springer.com/10.1007/978-1-4471-6663-4
Pepermans, G., 2014. Valuing smart meters. Energy Economics.
Ponce, P., Polasko, K., Molina, A., 2016. End user perceptions toward smart grid technology: Acceptance, adoption, risks, and trust. Renewable and Sustainable Energy Reviews 60, 587–598.
Siano, P., 2014. Demand response and smart grids – A survey. Renewable and Sustainable Energy Reviews 30, 461–478.
Smart Grids Task Force Expert Group 1- Standards and Interoperability, 2016. My Energy Data. Tech. rep., European Commission.
Smith, T. B., 2004. Electricity theft: A comparative analysis. Energy Policy 32 (18), 2067–2076.
Strbac, G., dec 2008. Demand side management: Benefits and challenges. Energy Policy 36 (12), 4419–4426.
Tzafestas, S. G., 2018. Ethics and law in the internet of things world. Smart Cities 1 (1), 98–120.
United Nations, 1949. United Nations Universal Declaration of Human Rights 1948. Office of the Hight Comissioner for Human Rights, 11.
Wilson, C., Hargreaves, T., Hauxwell-Baldwin, R., 2017. Benefits and risks of smart home technologies. Energy Policy.
Wladawsky-Berger, I., feb 2015. The Big Data Era Is Here.
Zachary, G., 2011. Saving smart meters from a backlash. IEEE Spectrum 8 (48), 8.