The ethical smart grid

Enabling a fruitful and long-lasting relationship between utilities and customers

Le Ray, G.; Pinson, P.

Published in:
Energy Policy

Link to article, DOI:
10.1016/j.enpol.2020.111258

Publication date:
2020

Document Version
Early version, also known as pre-print

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 grids more optimally. One of the smart grid purposes is to integrate a growing share of renewable generation while efficiently accommodating their variability and limited predictability through the actuation of consumer flexibility. Hence, 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. The rollout of smart meters throughout Europe should provide the necessary information to implement them. This is without accounting for a possible backlash of customers in response to bad practices of utilitie when it comes to digitization and smart meter rollout, also associated with the potential distrust of digital products. Beyond legal binds and technical obstacles, the possible ways of handling the rollout of smart meters and metering, which defines the relationship between customers and utilities, are multiple. However, only the practices that exhibit ethical behavior of the utilities towards customers, and consider them as stakeholders in smart grids will lead to a fruitful and long-lasting relationship between customers and utilities.

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. Since 2009 and the 2020 Climate & Energy Package's road map to the 20/20/20 targets (European Parliament, 2009b), the EU has driven towards a *greener* energy sector to achieve energy efficiency, energy independence, and reduction of greenhouse gas emissions.

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

The 2020 Climate & Energy Package's road map requires a modernization of the grids to foresee potential imbalances between generation and consumption, and to have a pervasive control to prevent them by modifying the consumption shape as renewable energy sources can only be curtailed (Farhangi, 2010). It is supported by the deployment of smart meters in 80% of EU households by 2020 (European Union, 2009). Smart meters deployment represents then the most substantial investment of the modernization of the grids and forms the foundations of the smart grid pyramid (Figure 1), which support the more advanced infrastructures of smart grids. Simultaneously, the Third Energy Package, adopted in 2009, restructures 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). On the customer side, metering data theoretically 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[1] side, metering data increase the efficiency and the reliability of grid operations, maintenances, and extensions while the share of renewable energy sources is increasing. According to the smart grid pyramid, smart meters constitute the first fundamental application that involves customers (Figure 1). Hence, smart meters represent smart grids to customers. As such, customers' first perception of smart meters (positive or negative) conditions the development of the future relationship between customers and utilities. Furthermore, the active involvement of customers as stakeholders of smart grids through the use of Demand-Side Management (DSM) constitutes the last step towards the successful deployment of smart grid technology and guarantees its long term development (Bertoldo et al., 2015, Horne et al., 2015, Giordano et al., 2011).

However, concerns are raised about a possible backlash of domestic customers, that could delay and even jeopardize the implementation of smart grid technologies (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 domestic accidents) and legitimate questions about the need for smart meters and their impact on privacy (McKenna et al., 2012). Smart meters can then have different representations from a customer point of view (Criqui and La Branche, 2016):

1. A tool to control the consumption, in-line with utilities usage,
2. A spy-ware - the data are then used by multinational firms to obtain more information,
3. A "*Big Brother*" tool - the data are then used by institutions (related to the state) to control consumption,
4. A danger to health - they generate electromagnetic waves and malfunctions could generate fires,

[1]In this paper, a utility is defined as an entity that is given responsibility for the maintenance and operation of some infrastructure of public value and used for public service.

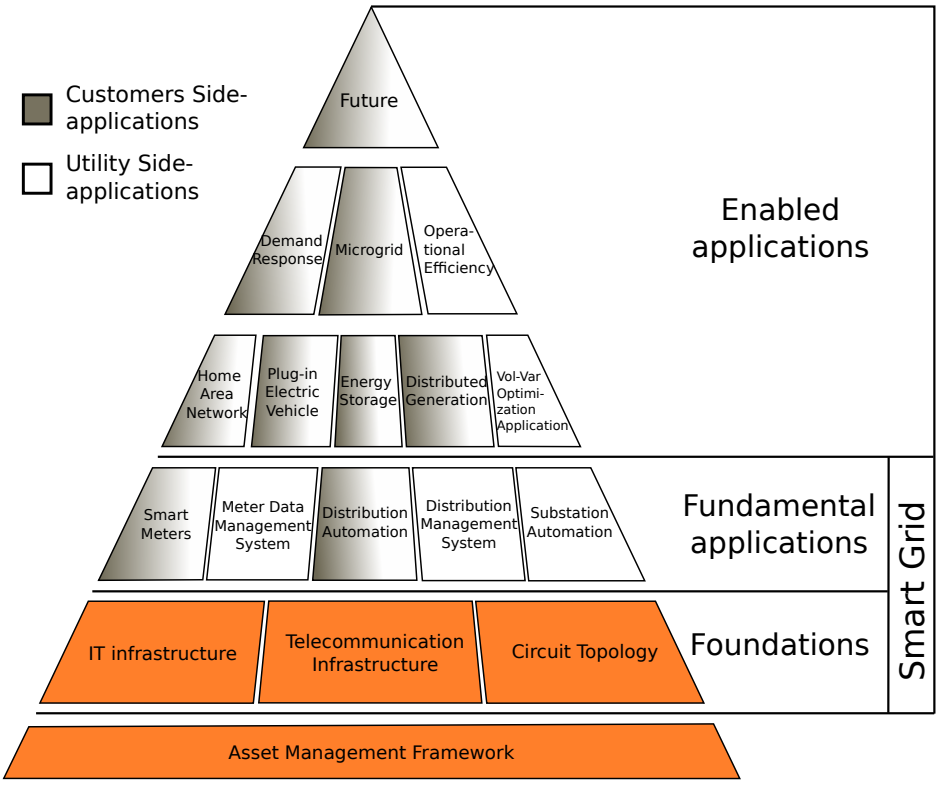

Figure 1: The Smart Grid pyramid (Source: Farhangi (2010)).

5. A tool whose claimed benefits are not understand (in the best case), or even challenged - why change the analog meters that work fine so far?

The representations are multi-factorial and depend on the political (opposition to the state, representation 3; opposition to liberalism, representation 2) and social contexts (general acceptance of new technologies) at different scales (state, region). If we focus on privacy that concerns two of the representations (representations 2 and 3), the concept is vague, and its definition has drastically evolved, from Aristotle making the distinction between the public and the private sphere, to the creation of the right to privacy (Papakonstantinou and Kloza, 2015). The evolution of the legal framework to protect data, and by extension data subjects, has followed with a delay in the evolution of the information and communication technologies. The legislation on data protection and privacy defines the limits of the legal use of data (Tzafestas, 2018). However, even if the utilities' practices are in line with the existing legal framework, these practices can have a substantial (and potentially negative) impact on the future of smart metering and smart grid deployment plans (by extension), as they can push customers towards one the negatively perceived representations of smart meters (Jegen and Philion, 2017). Similarly, the technical choices (i.e. resolution, roll-out scale, ownership) vary from one country to another and limit the range of actions for the utilities in different manners. An example could be the decision to make the installation of smart meter mandatory, which was legally possible but ethically arguable. The case of

the Linky in France is a paragon of how the bad practices (mandatory roll-out operated by subcontractor installing them with only noticing if the meter is accessible) associated with the heritage (Enedis as part of EDF is a national company), low digital trust (Frost & Sullivan, 2018), and the political context (defiance of a part of the population towards the states and/or local institutions) led to an inextricable situation (Ulessi, 2018, Danieli, 2018). The risk and the benefits of smart metering are also unbalanced between utilities and customers. Indeed, customers bear most of the risks (privacy, security) and the utilities collect most of the benefits (lower cost of metering, customers pay for smart meters, and the possibility to monetize the data without mentioning the benefits in terms of grid management). The liberalization of the energy sector may increase or at least maintain this lack of balance. This is difficult to justify considering the new responsibilities customers will have in smart grids.

In the present paper, we conduct a transversal literature review on smart metering supported by practical examples through legal (i.e. right to privacy), technical (i.e. setups), social (i.e. how much data users accept to share) sciences, which then aims at giving a status overview about smart meters and eventually to define the range of utilities' possible practices. It provides policy makers with an understanding of the multi-disciplinary aspect of smart grid implementation beyond technico-economical points of view. The main research question we hence address here is: what are good practices that would lead to a fruitful and long-lasting relationship between utilities and customers? We define good practices as the set of actions non-enforced by law conducted by the utilities that have a positive impact on the customers' perception of smart metering technologies (and inversely for bad practices).

Hence, we argue that ethics should be the basis to develop good practices concerning smart meter deployment and metering data usage and distribute the benefits according to the risks and responsibilities. Our argument and exposition in this paper complements some other recent works related to ethics, as well as technology adoption and acceptance, when it comes to smart grid technologies, e.g., Milchram et al. (2018). We especially focus on pointing at privacy, feelings about privacy and evolving roles of the various actors involved in relation to the main challenges possibly affecting to this thought-after long-term and fruitful relationship between utilities and consumers. The definition of ethics we use in this paper which is *"A system of moral principles, which deals with what is good or bad for individuals and society. It is a collection of fundamental concepts and principles on an ideal human character that enables 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). Good practices based on ethics concerning smart meters would secure the involvement of customers and subsequently, the future of smart grids. Indeed, the foundations of smart grids are put in place today, and utilities need to understand customers' perspective to build a sustainable relationship with them (Jegen and Philion, 2017). Indeed, the long term development of smart grid technology will change the status of consumers to prosumers[2] and they should be treated as stakeholders of the grids. In a time when defiance towards

[2]In this paper we include under the term prosumers, consumers that can provide flexibility, services to

technologies as part of an institution is growing, it is necessary to secure the involvement of customers into smart grids. Securing customers' involvement comes first by defining sets of good practices for utilities to use with customers to keep a fruitful and long-lasting relationship with customers.

The range of utilities' practices is delimited by the legal and technical aspects of the roll-out and smart meter data utilization concerning privacy and data accessibility (Section 2). However, privacy is not only dependent on the legal and technical aspects but also depends on what the citizens are willing to give. As privacy is an unclear concept, it is crucial to understand what we mean today by privacy and what is really at stake when jeopardized in a smart metering context (Section 3). In terms of responsibilities, risks, and benefits, the transition to the smart grid redistributes the cards between utilities and consumers (prosumers) as the latter ones become active stakeholders too. In the new context of the smart grid, Section 4 exposes examples of good practices that utilities should consider to maintain a positive relationship with customers, while Section 5 highlights the imbalance between risk and benefits for customers and utilities. 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, 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 historical 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 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 honor and reputation. Everyone has the right to the protection of the law against such interference or attacks*'. It aims at protecting the right and interests of individuals rather than the data itself as data collection appeared to generate an unexpected impact on an individual's 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 1970s, 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

the grid through DR or high-efficiency program, in addition to consumers that also produce electricity with local generation sources e.g. solar panels.

Europe, which had an impact beyond Europe, as 46 countries ratified it (Council, 1981). 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 Convention aims 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 clarifications 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[3]. The Data Protection Directive has articulated around three points; (i) transparency: information on personal data being processed; (ii) legitimate purpose: specification, explicit and legitimate of the purposes of the data collection; and (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.

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 apply 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 concerning data protection and privacy of the data subject are:

[3]As an EU Directive, it applies to all Member States, but each Member States transposes it in its national law

- 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 conditions (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 law has been updated according to the development of information technologies. Nevertheless, the following discussion on smart meter data and their ethical use is bounded within the EU by this legal framework.

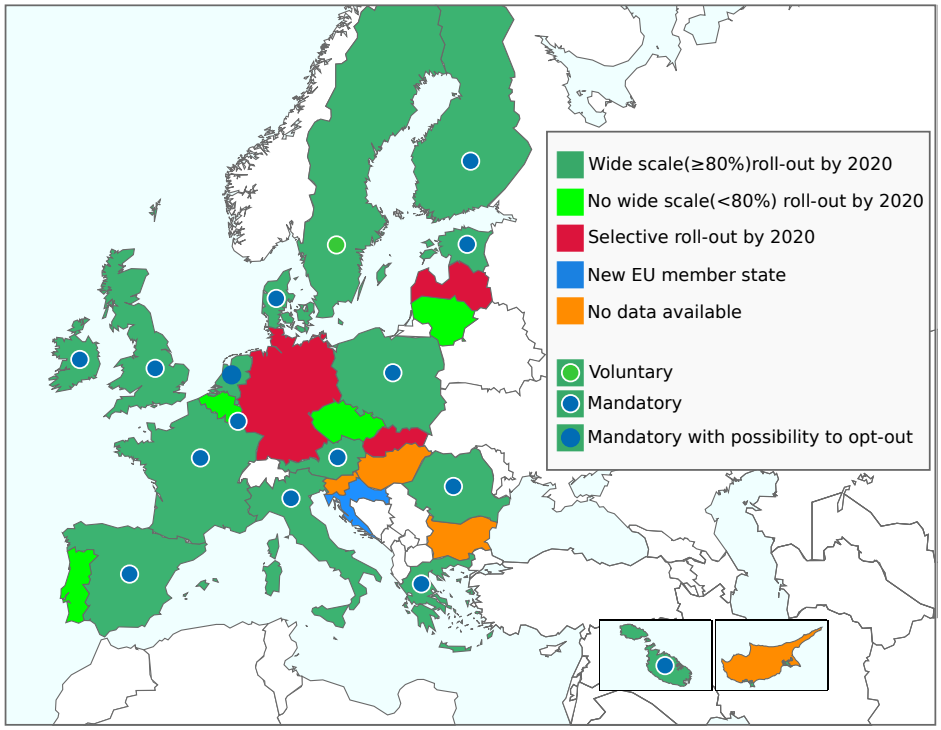

Figure 2: Map of the roll-out of smart meters in Europe (European Commission, 2014).

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 whether the roll-out should be at least 80%, less or just selective. However, the roll-out strategy is left to each EU Member State, which gives a broad 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 the 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 initially mandatory roll-out 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 DSOs and TSOs as they have to handle a large amount of data. Figure 3 is a schematic representation of the flow of data and actions between the different actors. The roles 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 context 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, the data flow as shown in Figure 3, and the capacity of customers 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.

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. As part of the digitization process of the energy sector, metering data (and smart meters by extension) are indissociable from the rest of the digital world, and the perception of digital products influences them grandly. 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 which defines privacy vs. utility[4] norm as in the definition of ethics used in the introduction of this paper (Horne et al., 2015). A discussion is as well open on what is at stake when we talk about privacy breaching.

[4]in the sense of usage/service

Table 1: Overview of the roll-out (in 2014) in the 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

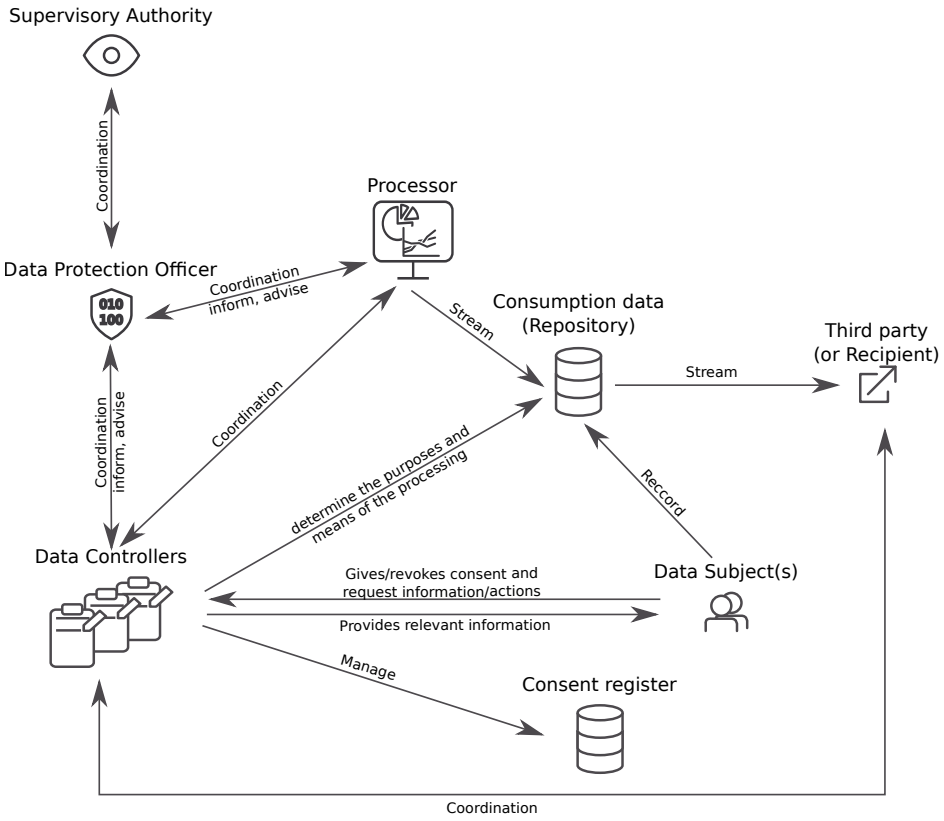

Figure 3: Interaction of actors and flow of smart meter data as described in the GDPR. Source: Smart Grids Task Force Expert Group 1- Standards and Interoperability (2016).

3.1. 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 two 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. As information extracted from data is not data, and information is not protected by the GDPR, which creates a breach in the legal framework. Theoretically, information anonymized and not under the form of raw data could be sold to third parties.

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. The use of navigation information is a good example of how anonymized information can be monetized through advertisement and could illustrate how metering data could be exploited for advertisement purposes. Users' navigation information is then used to generate targeted advertisements. In Europe and until 2011, websites

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 cookies 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 that 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 advertising 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, the use of data for targeted advertising is not much of a problem and can be considered as annoying when it is excessive. The problems come out of the methods used to maximize revenues.

Facebook generates a unique dataset, which appeals to psychometricians studying human behavior. The collection of *likes* from users can be used to generate 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 initially collected with their consent for research. Despite rules and Non-Disclosure Agreements, access was given to Cambridge Analytica, which extended the data to 30 million users using interconnections between *friended* users. Data was after that 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 a 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,' and (ii) that they should know how to restrict access (Liu et al., 2011). The configuration as default to the lowest security settings is questionable from a user perspective, as personal information is not protected by default despite the 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 vast majority does not, as it is a non-trivial operation (Liu et al., 2011).

The use of smartphones and smart city applications (e.g., public transportation card, traffic) like smart metering rely on the use of physical devices and adds a geographical dimension to information collected that anchors it in the physical world. It has been shown, using mobility data from carriers' antennas, that only four spatiotemporal points are needed to identify each carrier (De Montjoye et al., 2013) uniquely. 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 us to identify a person from his data uniquely. In the case of smart meters, the precise location (i.e., address) under the feeder used to invoice customers is disjoint from the metering data used for grid operation, maintenance and extension.

The bad practices operated by the large (and thus most representative) actors of the digital world have made the headlines of the newspapers and have induced in citizens distrust towards digital products (Frost & Sullivan, 2018). In this context, the deployment of smart meters in households, as physical devices (that can be localized) digitizing electricity consumption, is extremely sensitive. Hence, bad practices during the roll-out of smart meters and with metering data can have disastrous consequences on smart grids implementation. The mandatory installation associated with the absence of additional services offered from the installation (or little explanation on how to use it) is acting as a catalyst for customers' defiance toward smart meters.

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 imply that each person should not, in any way, be uniquely identified using the collected data (United Nations, 1949). 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 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 crucial here to understand what is at stake in that context: names have no importance in themselves. However, identities, sets of information that define each person, are precious as well as sensitive. Personal data can be combined with other non-personal data to identify, contact, or locate a *single* person. Discarding all this information is 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 identify users uniquely? 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). In (Barocas and Nissenbaum, 2014), the authors argue that the real value in anonymity is to prevent *reachability*, not to protect privacy. From the collected data, it should not be possible to communicate or reach data subjects physically. This concept is then much more meaningful and also reshapes 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 the social security number of American citizens based on their date and place of birth. They reach success rates from 7% to 61% in predicting the five 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 calls it contextual integrity (Nissenbaum, 2011); data (a type of information) collected in a specific 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.

The perfect flow of information for electricity metering data is represented in Figure 3. In most EU member states, the DSO host the data (see Table 1). The DSOs are historically state-owned companies. Hence, they should not make benefit (i.e., the revenues are reinvested in grid maintenance) so they do not monetize the data. The liberalization of the energy sector could expose metering data to monetization, and thus information extracted from metering data (i.e., anonymized and no pattern could directly be identified) could be sold to third parties.

4. Customers should be treated as stakeholders

The 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 a smart grid context, there are no clear guidelines or rules on how to implement good practices that maintain good relationships with customers. In this section, we aim at giving examples of good practices that rely on ethical behavior to keep customers involved as stakeholders of smart grids to secure investments (Bertoldo et al., 2015).

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

The DSOs are following the roll-out scales decided based on the CBA at the EU level (Figure 2). However, the decision to make the installation mandatory is made at each

state member level and is raising concerns among citizens throughout Europe. Indeed, a mandatory installation in a context of low trust in digital technologies associated with low trust in state institutions just acts as a catalyst of the social insecurity (Danieli, 2018).

From a customer perspective, the roll-out of smart meters, especially when mandatory, is an intrusion to what is perceived as the last sanctuary, 'Home' (Papakonstantinou and Kloza, 2015). A meter (analog or smart) is a foreign object in a household that inhabitants do not own (it is the DSO's property) and cannot remove/modify. The fact that the role of smart meters can be perceived unclear pushes customers not to understand what is smart meters' benefits (representation 5) and then be suspicious about their role (representation 2 and 3). It is well known that the adoption of technology by customers depends on their perception of smart meters (Ponce et al., 2016). However, the European Commission gave limited guidelines on conducting 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 adapted to ensure social acceptance and their effectiveness*' (Papakonstantinou and Kloza, 2015).

If we consider the customers that understand the role of smart meters, two types of customers have been described, 1. they put high expectation in smart meters (technophiles) and get disappointed because of the limitation of featured services or, 2. 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 appropriately considered in 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). Besides 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 customer's 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 to have a smart meter installed (opt-out). In (Gutwirth et al., 2013), the authors considered that there are four factors for the rejection of the smart meter bill by the Senate (i) the high resolution of the data transferred up to the energy providers, (ii) the mandatory roll-out where resistance is sanctioned by high fines or even imprisonment, (iii) lack of explanation of the necessity of smart metering and by extension why customers have to lose some privacy, and (iv) 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 significant misalignment between the reality of smart meters and customers' expectations. From a customer point of view, just the fact that a digitally connected meter is called 'smart' is 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(i) scale down the expectation of customers in explaining clearly what smart meters could do; and (ii) align the technology with the expectation by adding smart thermostats and in-home displays to visualize consumption in real-time. Smart grid frameworks require that customers know what their metering data is used for, even if it is technical, stakeholders have the responsibility of informing clearly and understandably (Bertoldo et al., 2015).

A solution could have been to do a well-marketed roll-out. Following the path of the popular high-tech companies, smart meters should have first tried to convince the technophiles and the technology evangelist into a well built platform-product-service framework. It would have then required to provide, for example, real-time pricing and an easy framework to combine it with smart home equipment as well as user-friendly insights on consumption. After that, the mass of customers would have followed voluntarily.

4.2. Evolution of the roles and relationships

The relationship between utilities and customers is ultimately changing as customers are expected to act as stakeholders of smart grids and have more responsibilities in maintaining a balance between generation and consumption (Khurana et al., 2010). Smart meters are only tools that allow customers to act and modify their consumption according to grids' needs. Hence, they are not anymore simply consumers; they become prosumers providing services to grids. The heritage of utilities, state own monopoly controlling the entire network from generation to distribution, makes it difficult to accept new stakeholders (aggregators or customers) in the grids. The modernization of grids being imposed by the EU and happening almost simultaneously with the restructuration of the utilities to cope with the opening of the energy market to concurrence, the DSOs may have lacked resources to do anything else than a mandatory roll-out From a customer point of view, the former state own monopolistic utilities were simply trusted. The restructuration of the utilities multiplies the number of actors and make their role (producers, DSOs, TSOs, aggregators) more difficult to apprehend for customers and thus can create distrust.

Furthermore, as customers are now stakeholders in maintaining smart grids balanced, they are not at the end of the power system, but a central element. The end goals of the relationship remain unclear to some extent as the benefits, and the expectations of smart metering are not aligned between customers and utilities (Horne et al., 2015). For example, customers are expected to be more active and would like to have more influence in *greening* their electricity consumption, but a smart meter in itself does not provide the functionalities that would facilitate to take action on consumption, it requires at least an additional 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 concerning energy (Horne et al., 2015).

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

4.3. Smart meters to empower customers to become prosumers

Smart grids aim 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 for metering data is almost mechanical. Indeed, a higher share of Renewable Energy Sources (RES) in the generation mix, as promoted by the EU, makes generation less adjustable to the demand. To compensate for the lack of flexibility on the generation side, the demand could be modulated according to some incentives (i.e., price, benefit) broadcast to customers using a two-way communication (Finster and Baumgart, 2014). DSM programs have been studied and implemented based on the idea of exploiting demand-side flexibility to reduce RES spillage (Strbac, 2008). DSM (including Demand Response (DR) frameworks as well as a more complex pricing scheme) rely 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 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.

From a customer perspective, 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, customers must have a positive perception of utilities (Horne et al., 2015). A customer who manages his consumption closely should then be encouraged to get electricity cost reductions (McDaniel and McLaughlin, 2009, Klass and Wilson, 2016).

In the context of the smart grid, new business models and actors (aggregators) are relying on metering data to create portfolios and manage their assets (Bondy et al., 2015). Nevertheless, 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). Beyond the technical aspect of DR, the customers should have the tools to manage their consumption which can be 1. user-friendly insights/interface on consumption,

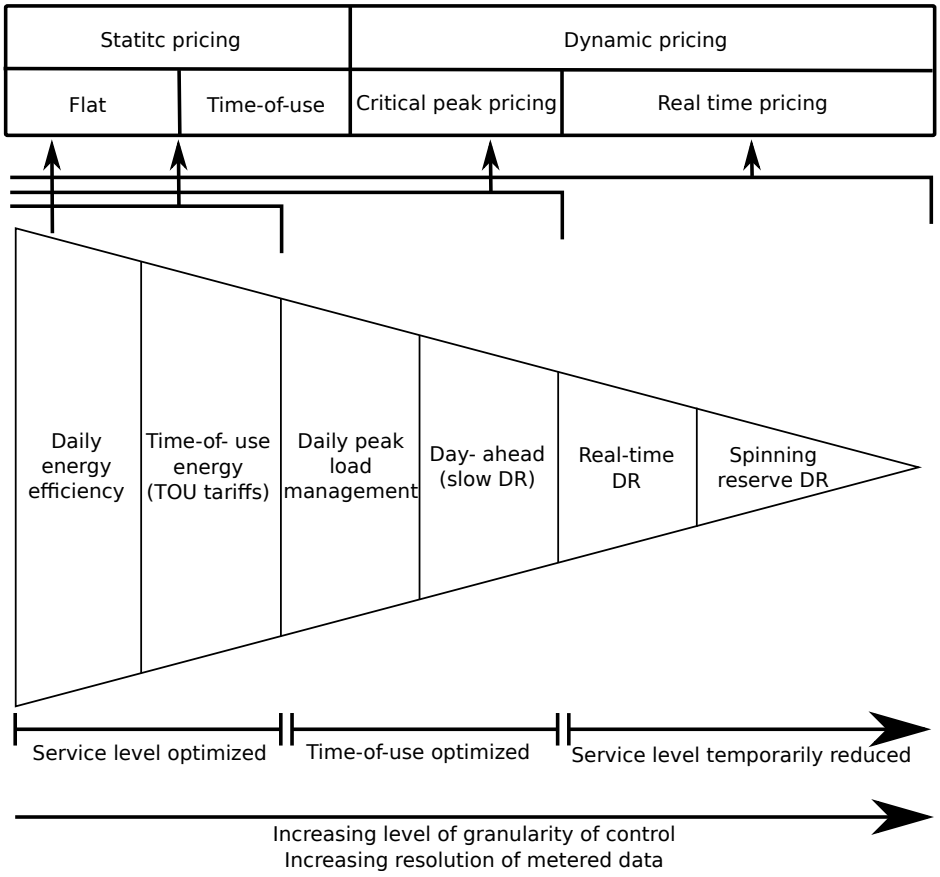

Figure 4: DSM service enabled in function of the resolution of the metering. Source: Siano (2014).

2. accurate forecast of future prices/incentives, 3. rewards according to the value of the service provided.

4.4. Control of access transferred to the data subject

New risk customers are exposed to with smart meters, is that their data are either not used to give them appropriate understandable insights on their consumption, or that data access is granted to an unsolicited third party.

In the actual smart grid data flow, metering data are stored on the data hub or DSO's servers (Table 1 and Figure 3). A consent register can be created to keep a record of which third parties get access to the data and for which period. The consent register is in practice, managed by the data controller (DSO). As customers are the ones that bear the risk with smart meters, it would be ethical that they get control over who can get access to their data. The access control could then have the form of the 'App' system as developed for smartphones where customers directly grant access to solicited third parties (Smart Grids Task Force Expert Group 1- Standards and Interoperability, 2016). 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 otherwise covered by law), it is assumed that customers should have control over what is connected to the port. The risk of abusive use of metering data by a third party is naturally increased if customers are not educated and made aware of how sensitive those data can be (as we can observe with smartphones). The risk could be, for example, that information (e.g., state of white appliances) are extracted from the data and used by unsolicited third parties for sending targeted advertisement suggesting to replace an appliance (Finster and Baumgart, 2014).

The new role of customers as stakeholders requires new responsibilities that utilities must acknowledge. This also means that their choice of joining smart grids must be respected rather than imposed with the consequences of a back-lash. As stakeholders, they have to understand what is their role and how they can manage their consumption. In this process, the utilities must support the customers in providing adequate tools to take meaningful actions. From the day of installation, the customers should be able to obtain access to metering data, high-efficiency programs, and advantageous benefits that are proportional to the services (data, DR) they provide to the grids. The structure with customers at the bottom and utilities at the top is obsolete in smart grids. The following section discusses how the FINISH THE SENTENCE.

5. Ethical balance of the risks and the benefits between utilities and customers

As presented in the previous section, good practices based on ethics can be implemented during the roll-out and on the use of metering data to improve the relationship between utilities and customers. However, the risk and benefits should be balanced following two

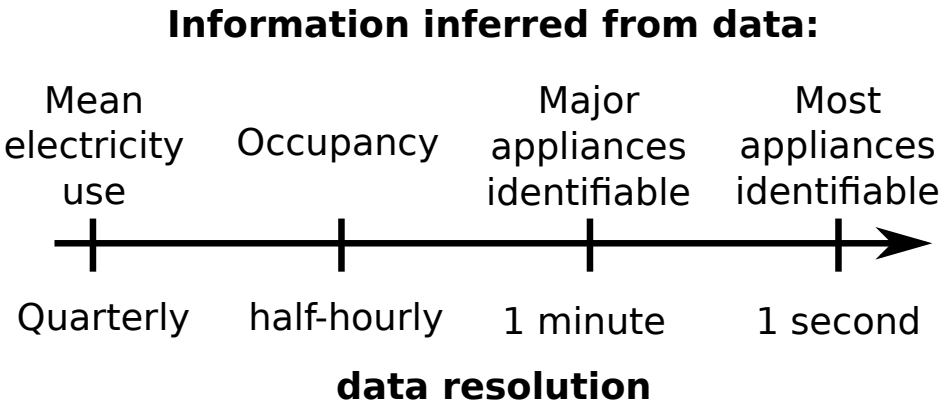

Figure 5: Representation of information that can be inferred from metering data in function of the resolution. Source: McKenna et al. (2012).

global concept parsimony and equity. The risk should be parsimonious and come with a direct benefit to customers. Hence, both parties would be satisfied. In the actual situation, the risks are placed on the customers, and the benefits are going to the utilities. In this section, we highlight identified imbalances and suggest ways to correct them.

5.1. Legitimacy of the task to fulfill

Privacy concerns are often about the high resolution of metering data as the pattern of activities (i.e., cooking or simply the presence or absence of the inhabitant can be detected) can be identified from the raw data (McKenna et al., 2012). Smart meters can provide data at different resolution and the higher the resolution, the more precise the information (See Figure 5). The GDPR covers this problem partially as the data collected should be in accordance with the task to fulfill (principle of parsimony). However, it does not protect information inferred from the data. Hence, machine learning applications using metering data, like Non-Intrusive Load Monitoring (NILM) used to identify activation patterns of individual appliances from the overall electricity consumption, are raising concerns about possible leakage of sensitive information (not data) (Klemenjak and Goldsborough, 2016). In this section, we want to emphasize that the methodology (i.e., machine learning) is not the problem, the legitimacy of the task, its aim as well as the legitimacy of the party that conducts it are the sensitive aspects. Coming back to the perfect flow of information (Figure 3), it would deviate the flow from perfect if the task or the party id not legitimate. NILM application, for example, is implemented in a specific context; it consists of providing detailed information of individual appliances consumption to customers, who are also data subjects so that they can identify appliances with large unnecessary electricity consumption. This information should be provided to the data subject and no one else. But as this information can be anonymized and *dissociated* from the raw metering data, it could be sold to an illegitimate third party without breaking the law.

Another application that would have a genuine purpose, would be the use of NILM by DSOs on data at a lower resolution to identify large and potentially flexible appliances (e.g. EVs without smart chargers, HPs, Electric heating, AC) that could provide services to smart

grids. Hence, DSO could use this information to propose flexibility contracts to owners of such flexible appliances. A fair distribution of the benefits that would reward customers according to the value of the services provided to the DSO, would guarantee its legitimacy and keeps the data flow close to perfect.

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 with the task to fulfill. Like the purpose has to be legitimate, the resolution of the data has to be legitimate. For example, when billing customers under dynamic tariffs, it does not improve anything to use electricity consumption at a higher resolution than the dynamic tariff. Hence, the resolution of the data should be chosen parsimoniously.

5.2. New risks require compensation

Smart meters being connected devices, security issues concerning data leakage at the meter level or server level exist and have to be acknowledged, as with any connected device (e.g., computers, IoT devices). 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 23rd, 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 a digital central control system makes them obvious targets for cyberattacks. However, the attack did not target metering data, but the stability of the grid, which does not affect privacy in this specific case. Nevertheless, a cyberattack could also be conducted by customers on their 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).

In this section, the security we simply acknowledge that a risk of data leakage exists and we do not focus on the origin of the security issue, but rather on what are the utilities doing to compensate this risk. The risk is considered, and efforts on securing communication are made to limit it. As smart meters are, in most EU member state, imposed to customers that pay for them through network tariffs (only Italy, Romania, Slovakia and Sweden are sharing costs between customers and DSO (see Table 1) and bear this risk, the risk should be addressed with compensations/benefits (Wilson et al., 2017). It would then be fair that customers get rewarded according to the amount of information transmitted to utilities (Culnan and Bies, 2003).

An alternative to imposing the same risk to every customer could be to implement a system where the customer chooses the resolution of the data they agree to provide 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 discount according to the resolution of the data collected.

5.3. A fair balance of the benefits

Balancing the benefits resides in a trade-off between the data provided (as a valued service) and increased risk on the customer's side and the need for metering data on the

utility side (Culnan and Bies, 2003). As mentioned earlier, the customers bear the risk. In this section, we show that the utilities gather most of the benefits today. We want to show that it is possible (even necessary) to do it fairly to be sustainable and avoid future backlash (Zachary, 2011).

Today, the benefits of smart metering are going toward the utilities, which 1. save the cost of employing meter readers, 2. get accurate metering data with little delay, 3. process invoice automatically, 4. and get more insights on the grid for fraud detection and maintenance (Hu et al., 2015). A more accurate billing also means 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 billion, compensated by a 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).

As the meters are paid mostly through network tariffs (Table 1), potential savings due to services provided to grids, are, until payment completed, shortened for customers. Besides the benefits mentioned above, little use of data is done in the EU to provide insights to customers. They can access their raw data consumption, but the information is hard to interpret for non-technical persons. Solutions like the green button in the USA (Sayogo and Pardo, 2013) or the research project FLEXIENCY in Europe (Boukir et al., 2017) are proving that solutions exist, but large scale implementation will take time in the EU. In the meanwhile, customers will pay for the technology without having any of the benefits. The access given to consult and analyze electricity consumption, as promoted by the EU, would then have only little impact, as customers could only reduce their consumption to reduce their electricity bill and not provide any services. The misalignment between provided service and expectations can even be larger. In some cases, customers were undercharged because of malfunctioning electromagnetic meters, which is common because of their advanced age and mechanical components, will observe an increase in their electricity bill due to increased metering accuracy (Krishnamurti et al., 2012). Smart meters are part of the Advanced Metering Infrastructure (AMI), which forms the informational backbone of smart grids and makes grids smart. From a DSO perspective, AMI allows them to have precise information about the power flows at a distribution level beyond the substations. The value of metering data is emphasized by the increase of variable RES in the generation mix and decentralized generation (Finster and Baumgart, 2014). This way, it lowers 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. Hence, these benefits can be translated as savings that are made possible thanks to metering data, which can give an estimate of the value of the collected data. In a context of liberalization of the energy sector, it appears to be unlikely that the savings get distributed to the customers.

Whatever the decision made to increase the RES generation, dynamic information on

the demand side will be required to use RES, invoice prosumers optimally, and balance the generation with the demand (Klass and Wilson, 2016). Hence, the roll-out of smart meter from an environmental and grid management perspective is not negotiable, but the way the data is used and how the benefits 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 risks, and the social and economic benefits generated by the installation of smart meters (Culnan and Bies, 2003). The worst scenario could lead to the loss of an important part of metered households.

6. Conclusion and Policy Implication

DSOs must respect the agenda of the Third Energy Package and deploy smart meters in due time following the road map to the 20/20/20 targets. Hence, the mandatory installation of smart meters appears to be the best solution to fulfill the task on time. At the same time, utilities are putting efforts into complying with the GDPR. However, the GDPR only protects the fundamental rights of the data subjects (i.e., customers), though it may not be sufficient to fulfill the expectations of these customers. Smart meters have been advertised to be a tool that will empower customers to control more closely their electricity usage. In reality, they just provide raw consumption data that are difficult to interpret for non-engineers.

The misalignment between expectations and delivered products (also related services), bad practices during the roll-out period, as well as the imbalance of risks and benefits for customers, are generating a negative image of smart grid technologies to customers. The fact that it is required to improve the use of RES, or that it is imposed by the EU, are not proper arguments supporting the implementation of smart grids with little to no ethics towards customers. In addition to the specific ethical problems of smart grid implementation, the general prospect of the digital energy world is not seen as appealing by many customers.

In the current situation, the technological developments and investments are just used to have a more detailed picture of the demand side and not implementing an inclusive solution where customers would be stakeholders contributing to balance generation and consumption. If the customers do not accept the technology, they will not use it to its full proficiency. The risk of backlash where customers reject smart meters and ask to be metered annually is real as illustrated by the case of the Netherlands and France.

The insights from social sciences are necessary for the process of digitization of the energy sector, as the technical-economical of smart grids technologies assume that the customers are rational. Anthropology, for example, could be used to change the meaning of *demand*, originally thought of from an economical perspective, to invest it with a new meaning, a new role in society which will be more in line with the role of a stakeholder (Wilhite, 2005). In parallel, psychology could be used to nudge customers into more sustainable behavior (Newell and Siikamäki, 2014, Lehner et al., 2016). Similarly, behavioral science and sociology may be instrumental in the acceptance of smart meters, and to align the expectations of customers with the actual capabilities of smart meters (Chen et al., 2017, Krishnamurti et al., 2012).

The use of social sciences to support large infrastructure projects negatively appraised by citizens (e.g., construction of a dam, road) has already shown a positive influence on their eventual perception.

In the general context of climate change, citizens have become aware of their responsibilities, possible commitment, as well as how they can influence the outcome. Energy represents one of the fields where awareness is growing rapidly. It seems that customers are ready to become active stakeholders in smart grids, to support the deployment and management of greener electricity generation, but not at any cost.

Acknowledgement

The authors thank the EUDP for funding through the EnergyLab Nordhavn project (EUDP 64015-0055). Reviewers and the Editor are acknowledge for comments and suggestions on previous versions of that manuscript.

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.

Boukir, K., Waestlund, D., Traverson, B., Schwarzlaender, F., Defrancisci, S., 2017. Providing smart metering data services through an eu market place. CIRED-Open Access Proceedings Journal 2017 (1), 2848–2851.

Chen, C.-f., Xu, X., Arpan, L., 2017. Between the technology acceptance model and sustainable energy technology acceptance model: Investigating smart meter acceptance in the united states. Energy research & social science 25, 93–104.

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, o. E., 1981. Convention for the protection of individuals with regard to automatic processing of personal data.

Criqui, P., La Branche, S., 2016. Compteur électrique Linky : comprendre la polémique . URL https://theconversation.com/compteur-electrique-linky-comprendre-la-polemique-59769

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

Danieli, A., 2018. La 'mise en société' du compteur communicant. innovations, controverses et usages dans les mondes sociaux du compteur d'électricité linky en france. Ph.D. thesis.

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.

Frost & Sullivan, 2018. The global state of online digital trust. Tech. rep., Frost & Sullivan.

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
Lehner, M., Mont, O., Heiskanen, E., 2016. Nudging–a promising tool for sustainable consumption behaviour? Journal of Cleaner Production 134, 166–177.
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.
Milchram, C., Van De Kaa, G., Doorn, N., Künneke, R., 2018. Moral values as factors for social acceptance of smart grid technologies. Sustainability 10 (8), 2703.
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
Newell, R. G., Siikamäki, J., 2014. Nudging energy efficiency behavior: The role of information labels. Journal of the Association of Environmental and Resource Economists 1 (4), 555–598.
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.
Sayogo, D. S., Pardo, T. A., 2013. Understanding smart data disclosure policy success: The case of green button. In: Proceedings of the 14th annual international conference on digital government research. ACM, pp. 72–81.
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.
Ulessi, C., 2018. France: CNIL's notice to DIRECT ENERGIE on collection of smart meter data indication

of likely approach of DPAs post-GDPR.
URL https://smartgridawareness.org/2018/04/01/no-legal-basis-for-smart-meter-data-collection/
United Nations, 1949. United Nations Universal Declaration of Human Rights 1948. Office of the Hight Comissioner for Human Rights, 11.
Wilhite, H., 2005. Why energy needs anthropology. Anthropology today 21 (3), 1–2.
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.