Privacy Issues in Smart Grids

Slobodan Bojanić, Srdan Đorđević and Octavio Nieto-Taladriz

Abstract - The smart grid brings an entirely new and complex model of inter-relationships which poses challenges for data privacy. It is an emerging area where new data privacy problems evolve as more smart meters are installed. Since mass rollout of smart meters is already happening, there is urgency how to process personal data and to treat some issues of general concern which warrant serious privacy consideration.

Keywords – Smart Grid, Privacy, Smart Meter, Privacy by Design.

I. INTRODUCTION

The benefits of smart energy use include opportunities for consumers to cut their bills by changing their habits, perhaps using energy at different times to take advantage of lower tariffs, as well as opportunities for industry to more accurately forecast demand, reducing expensive electricity storage costs. The realisation of climate change targets relies to some extent on consumers releasing personal data, but this needs to be achieved in such a way that all parties involved in programmes to introduce smart meters and the development of the smart grid ensure that the fundamental rights of individuals are protected and respected [1]-[5].

Without such protection there is a risk not only that processing of personal data will be in breach of national laws but also that consumers will reject these programmes on the basis that the collection of personal data is unacceptable to them. Such rejection may arise even if there is no breach of the law. While the potential benefits of these programmes are far-reaching and significant, they also have the potential to process increasing amounts of personal data, unprecedented in this industry, and to make that personal data more readily available to a wider circle of recipients than at present.

II. BACKGROUND

A variety of definitions of smart grid have been available. It can be assumed that the Smart grid is an intelligent electricity network that combines information from users of that grid in order to plan the supply of electricity more effectively and economically that was possible in the pre-smart environment. It can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety. In a further step, energy optimization crossing the domains of electricity, gas and heat will be a further challenge.

The electricity networks have provided the vital links between electricity producers and consumers with great success for many decades. The fundamental architecture of these networks has been developed in most countries to meet the needs of large, predominantly carbon-based generation technologies. Europe is committed to the 20-20-20 targets to reduce carbon emissions and to secure energy supply. Energy efficiency and renewable energy are seen as key to reach this goal. Both measures call for changes in the energy supply system leading to smart grids as key enablers for the required innovation.

Smart meters allow for the generation, transmission and analysis of data relating to consumers, much more than is possible with a 'traditional' or 'dumb' meter. Consequently, they also allow the network operator (also known as Distribution Service Operator or DSO), energy suppliers and other parties to compile detailed information about energy consumption and patterns of use as well as make decisions about individual consumers based on usage profiles. Whilst it is acknowledged that such decisions can often be to the benefit of consumers in terms of energy savings, it is also emerging that that there is potential for intrusion into the private lives of citizens through the use of devices which are installed in homes. It also marks a shift in our fundamental relationship with energy suppliers in that consumers have traditionally simply paid suppliers for the electricity and gas that has been supplied.

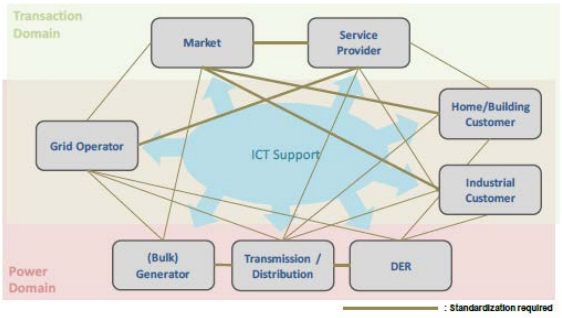

Fig. 1 A conceptual model of the Smart Grid

With the advent of smart meters, the process is more complex in that the data subject will provide suppliers with insights into personal routines. There is a huge variation in

Slobodan Bojanić and Octavio Nieto-Taladriz are with Universidad Politécnica de Madrid, ETSIT Avenida Complutense nº 30, 28040 Madrid, Spain, e-mail: {slobodan, octavio}@die.upm.es.

Srdan Đorđević is with the Department of Electronics, Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, 18000 Niš, Serbia, e-mail: srdjan.djordjevic@elfak.ni.ac.rs.

circumstances between countries, ranging from those where rollout is largely complete following government mandate to those where no meters have been installed.

II. STAKEHOLDERS

As there is no one universal, internationally accepted definition of "privacy," it can mean many things to different people. At its most basic, privacy can be seen as the right to be left alone. Privacy is not a plainly delineated concept and is not simply the specifications provided within laws and regulations. Furthermore, privacy should not be confused, as it often is, with being the same as confidentiality; and personal information is not the same as confidential information. Confidential information is information for which access should be limited to only those with a business need to know and that could result in compromise to a system, data, application, or other business function if inappropriately shared.

The smart metering brings with it the potential for numerous novel ways for processing data and delivering services to consumers. Whatever the processing, whether it is similar to that which existed in the pre-smart environment, or unprecedented, the data controller must be clearly identified, and be clear about obligations arising from data protection legislation including Privacy by Design, security and the rights of the data subject. Data subjects must be properly informed about how their data is being processed, and be aware of the fundamental differences in the way that their data is being processed so that when they give their consent it is valid.

The following Smart Grid stakeholders

- Grid users including/composed of grid operators, grid customers and meter operators
- End customer (domestic or commercial)
- Municipalities including energy retailers
- Politics
- Industries
- Consumer organizations
- Politics/society

can also be viewed through various domains interconnected

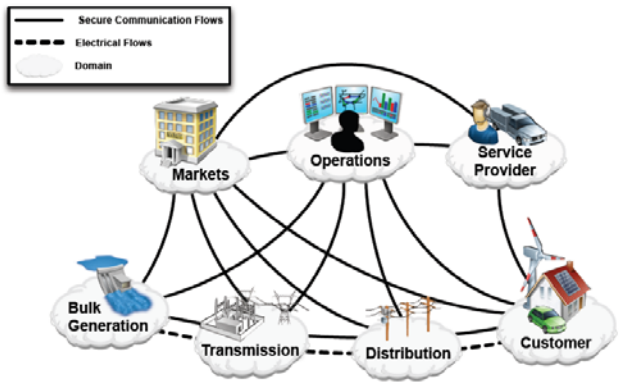

Fig. 2 Interaction among actors in Smart Grid

by secure communication flows and flows of electricity as presented in Fig. 2.

Basicaly the smart meter takes a reading which reflects the energy usage at the property. At some point that reading, along with other information, can be transmitted outside the property. In some models it will be sent directly to a central communications hub where the smart meter data are managed. Once there, it can be accessed by DSOs, suppliers and ESCOs. It appears that the DSOs will have to face the greatest changes to make smart grids a reality. The reasons for that are the growing distributed character (resulting in growing bidirectional power flow at all voltage levels) and variability of generation, customer privacy issues, system security, data and information processing for new applications and concepts such as Virtual Power Plants, etc.

There are also multiple and complex methods of communication, with additional entry points and data paths creating complicated security challenges requiring solutions that encompass them all. Given the complex and disparate landscape, the task of producing privacy solutions is quite challenging, and at this stage it seems that they can only be general, rather than specific.

The disparity of the current position does not allow presenting a comprehensive view on all specific aspects of smart metering programmes across member states. There is a huge variation in circumstances between countries, ranging from those where rollout is largely complete following government mandate to those where no meters have been installed. There is also much variation in the level of involvement from DPAs and in the nature of the market across member states, and where responsibility lies with installation of meters. In some countries, publicly owned utility companies are responsible. Elsewhere, there is a competitive supplier market. Distribution system operators have a more prominent role in some countries.

As the smart grid brings with it an entirely new and complex model of inter-relationships that poses challenges for the application of data protection. This is an emerging area of work where it is fully expected that new data protection problems and solutions will evolve as more smart meters and smart grid components are installed. What is inarguable is that mass rollout of smart meters is already happening, so there is urgency to collectively understand the way that smart meters process personal data, and the issues that this raises. There are some issues of general concern which warrant serious consideration by all those involved in this area.

Given that that data in Smart Grids might contain privacy sensitive information it is advised that principles such as privacy by design and Default should be encouraged. The personal data is being processed by the meters, so data protection laws apply. The smart metering brings with it the potential for numerous novel ways for processing data and delivering services to consumers. Whatever the processing, whether it is similar to that which existed in the pre-smart environment, or unprecedented, the

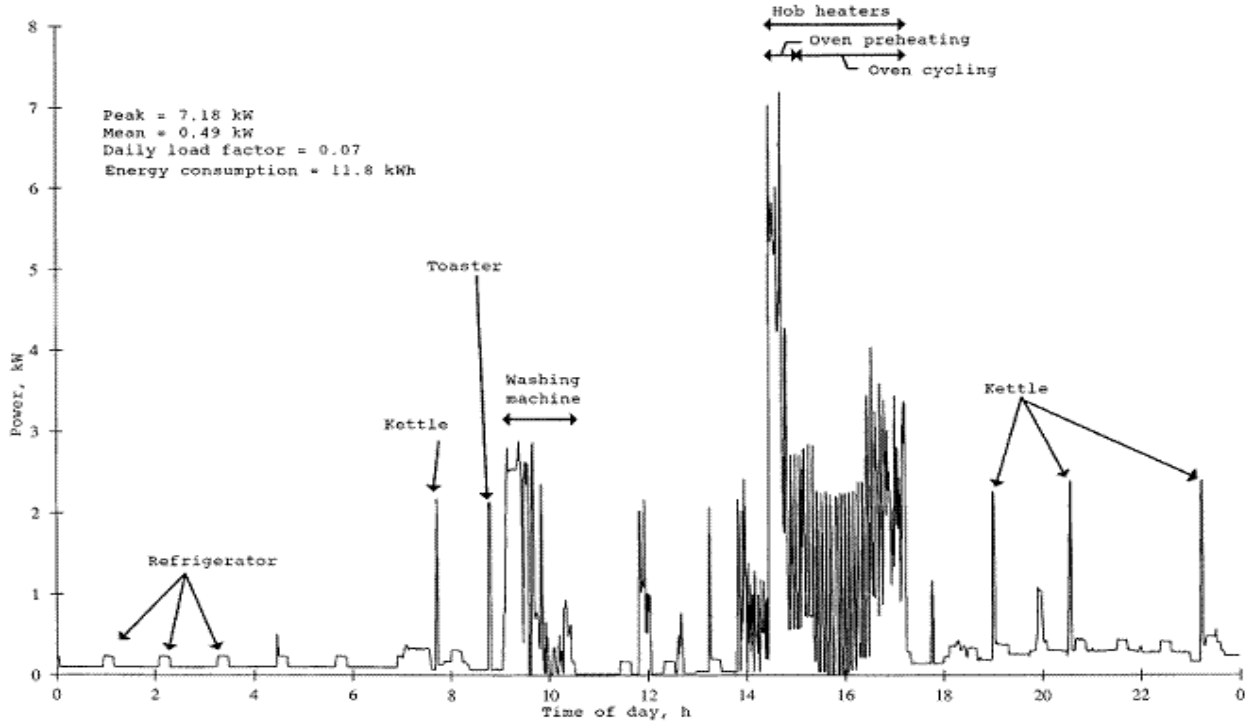

Fig. 3 Consumer profiling by energy

data controller must be clearly identified, and be clear about obligations arising from data protection legislation, security and the rights of the data subject. Data subjects must be properly informed about how their data is being processed, and be aware of the fundamental differences in the way that their data is being processed so that when they give their consent it is valid.

III. Privacy Threats

There are numerous privacy implications identified for smart grid technology deployment centers on the collection, retention, sharing, or reuse of electricity consumption information on individuals, homes, or offices. Fundamentally, smart grid systems will be multi-directional communications and energy transfer networks that enable electricity service providers, consumers, or third party energy management assistance programs to access consumption data. Further, if plans for national or transnational electric utility smart grid systems proceed as currently proposed these far reaching networks will enable data collection and sharing across platforms and great distances [7]-[11].

Consumer privacy is a key aspect in the change towards smart energy systems thus data access and ownership and the permission to gather data need to be very carefully considered. At the same time, consumers should be well-informed about who deals with their data. It has to be remembered that it is the consumer who owns his data, no-one else, and therefore he is entitled to appropriate rights and protections.

A list of potential privacy consequences of Smart Grid systems include:

- Identity Theft
- Determine Personal Behavior Patterns
- Determine Specific Appliances Used
- Perform Real-Time Surveillance
- Reveal Activities Through Residual Data
- Targeted Home Invasions (latch key children, elderly, etc.)
- Provide Accidental Invasions
- Activity Censorship
- Decisions and Actions Based Upon Inaccurate Data
- Profiling
- Unwanted Publicity and Embarrassment
- Tracking Behavior of Renters/Leasers
- Behavior Tracking (possible combination with Personal Behavior Patterns)
- Public Aggregated Searches Revealing Individual Behavior.

Plans are underway to support smart grid system applications that will monitor any device transmitting a signal, which may include non-energy-consuming end use items that are only fitted with small radio frequency identification devices (RFID) tags may be possible.

Whereas, in Europe energy theft and privacy are the most important concerns related to Smart Grid implementation, in other parts of the world (e.g. in the US) it is energy theft and malevolent attacks that are the main concerns.

IV. PRIVACY PRINCIPLES

The increased amount of personal data being processed, the possibility of remote management of connection and the likelihood of energy profiling based on the detailed meter readings make it imperative that proper consideration is given to individuals' fundamental rights to privacy.

Privacy by Design (PbD) is a concept to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems [12]. The objectives of Privacy by Design — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following seven Foundational Principles:

1. Proactive not Reactive; Preventative not Remedial measures by anticipating and preventing privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.
2. Privacy as the Default Setting i.e. ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.
3. Privacy Embedded into design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
4. Full Functionality — Positive-Sum, not Zero-Sum, *by* accommodating all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made such as privacy vs. security, demonstrating that it is possible to have both.
5. End-to-End Security — Full Lifecycle Protection extending securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion.
6. Visibility and Transparency **—** thus its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.
7. Respect for User Privacy — Keeping it User-Centric appropriate notice, and empowering user-friendly options.

Yet, privacy concerns still need to be transposed into specific, precise and non-ambiguous technical requirements if they are to allow the security industry to competitively design and develop privacy-compliant solutions and services. The Privacy by Design concept should, at its turn, be better detailed in order to allow for its practical implementation in concrete cases.

There are also OECD Privacy Guidelines:

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, compete and kept up-to-date.
3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 except— with the consent of the data subject; or by the authority of law.
5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle: An individual should have the right: a. To obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b. To have communicated to him, data relating to him.
8. Accountability Principle: A data controller should be accountable for complying with measures that give effect to the principles stated above. Data can be sent to the controller in real-time or be stored in the smart meter. In both cases however, under the Data Protection Directive, it is considered that the data have been collected by the controller.

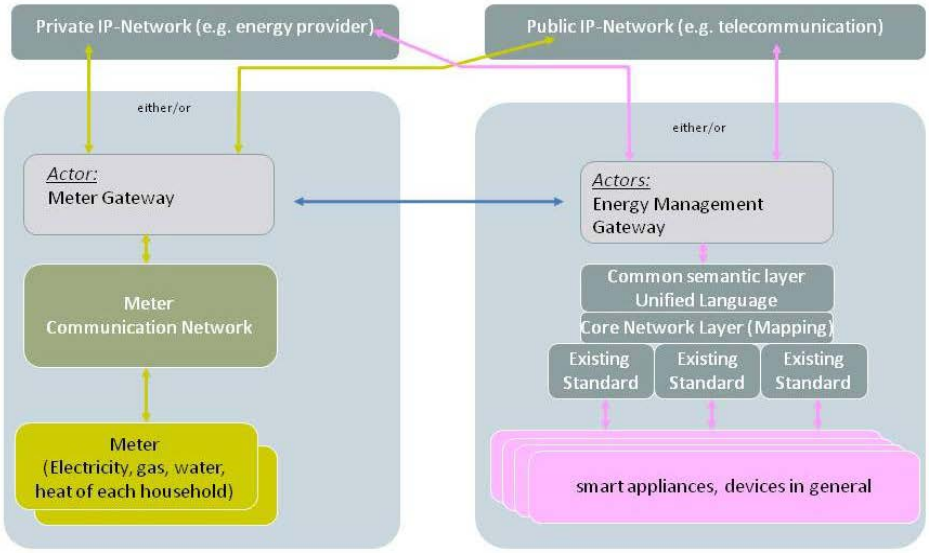

Fig. 4 – Logical separation of metering and energy management

As part of the Privacy by Design process, security and privacy risk assessments will identify the potential risks to data security. Given the novel and vast prospect that is in store with the smart grid and its associated technologies, the task of anticipating security requirements is a challenging one. In order to mitigate risk, the approach should be end-to-end, incorporating all parties and drawing on a broad range of expertise. Security should also be designed in at the early stage as part of the architecture of the network rather than added on later. Appropriately robust security safeguards must be in place that should apply to the whole process including the in-home elements of the network, the transmission of personal data across the network and the storage and processing of personal data by suppliers, networks and other data controllers. Security is a path, not a destination. Security is about risk management and implementing effective counter measures.

The technical and organisational safeguards should cover at least the following areas:

- The prevention of unauthorised disclosures of personal data;
- The maintenance of data integrity to ensure against unauthorised modification;
- The effective authentication of the identity of any recipient of personal data;
- The avoidance of important services being disrupted due to attacks on the security of personal data;
- The facility to conduct proper audits of personal data stored on or transmitted from a meter;
- Appropriate access controls and retention periods;
- The aggregation of data whenever individual level data is not required.

IV. Technical Solutions

The reference architecture for the home/building, pointing out the different logical blocks, and can be easily integrated in the whole system architecture is shown in Fig. 4. It is not related to a specific hardware design, but merely shows a logical separation of functions without predefining where and how those functions are implemented.

Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids [5] presents WAN interface to AMI subsystem & Head-End is used to connect the meter, a Local Network Access Point, or a Neighbourhood Network Access Point to a Central Data Collection system. Typical interface platforms for these interfaces are PSTN networks, public G2 (GPRS) and G3 (UMTS) networks, DSL or broadband TV communication lines, power line communications (PLC), either in narrowband or broadband.

The Head-End systems are the central Data Collection Systems for the Advanced Metering Subsystem. Head-end systems are typically part of an AMR (automatic meter reading) or AMM (automatic meter management) solution. The interface towards the gateways and data concentrators (Network Access Points) is being standardized with Mandate M/441 whilst the interface from head-end systems towards central ERP and meter data management systems is covered by other IEC TCs, e.g. IEC TC 57 (61968-9).

Little work exists on the design of technical solutions to protect privacy in the smart grid [13]. Wagner et al.

propose a privacy-aware framework for the smart grid based on semantic web technologies. Garcia and Jacobs design a multiparty computation to compute the sum of their consumption privately. The NIST privacy subgroup suggests anonymizing traces of readings, as proposed by Efthymiou et al., but also warns of the ease of reidentication. Molina et al. highlight the private information that current meters leak, and sketch a protocol that uses zero-knowledge proofs to achieve privacy in metering. Kumari et al. propose usage control mechanisms for data shared by smart meters connected to web based social networks.

It is equally important to make the principle of privacy-by-design mandatory, including principles of data minimization and data deletion when using privacy-enhancing technologies. As it is currently almost impossible to ensure the full anonymisation of personal data and it is often possible to ’re-identify' or 'de-anonymise' individuals hidden in anonymised data with astonishing ease, only aggregated data should be used to the maximum possible extend. Considering significant privacy threats, we ask for privacy impact assessment to be conducted prior to the smart meter roll out.

Moreover, technical standards and systems should be developed with a focus on upgradeability to safeguard end-to-end security ensuring the overall intelligent metering system is future-proof and ready to cope with future challenges.

Standardization of smart grids is not a business as usual due to the huge number of stakeholders, the necessary speed, the many international activities and the still changing solutions make it a difficult task.

Specific for the data privacy aspects, the European consumer groups are asking for clear regulation around frequency of meter reading and usage of data. It is stressed that only data necessary to perform Smart Grid tasks should be collected and utilised. At the same time, whilst acknowledging benefits, Smart Grid/Meters should be designed for privacy and security.

IV. Conclusion

The smart grid brings with it an entirely new and complex model of inter-relationships which poses challenges for the application of data protection. Because of the wide ranging nature of the issues presented by smart metering, it is not possible to provide an exhaustive list of privacy and security points. It is an emerging area of work where it is fully expected that new data protection problems and solutions will evolve as more smart meters are installed. What is inarguable is that mass rollout of smart meters is already happening, so there is urgency to understand the way that smart meters process personal data, and the issues that this raises. There are some issues of general concern which warrant serious consideration by all those involved in this area.

Acknowledgement

This research was partially funded by The Ministry of Education and Science of Republic of Serbia under contract No. TR32004

References

[1] ANEC/BEUC POSITION ON ENERGY EFFICIENCY, Joint ANEC/BEUC position paper on the Commission's Communication “Energy Efficiency Plan 2011”

[2] Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering, WP 183, 4.4.2011

[3] BEUC Response To CEER Public Consultation On Demand Response Programmes

[4] Cavoukian A., Privacy By Design …Take The Challenge, Book.

[5] CEN/CENELEC/ETSI Joint Working Group, Standards for Smart Grids, Final report, 4 May 2011.

[6] Elster’s White Paper, Privacy Enhancing Technologies for the Smart Grid, 4.10.2011

[7] European Commission, COM(2010) 609, A comprehensive approach on personal data protection in the European Union Brussels, 4.11.2010

[8] European Commission, COM(2011) 202, Smart Grids: from innovation to deployment, Brussels, 12.4.2011

[9] European Technology Platform SmartGrids, Strategic Deployment Document for Europe’s Electricity Networks of the Future

[10] Kursawe, K., Danezis, G. and Kohlweiss, M., Privacy-friendly Aggregation for the Smart-grid.

[11] NISTIR 7628, Guidelines for Smart Grid Cyber Security, September 2010

[12] PbD, SmartPrivacy for the Smart Grid, November 2009.

[13] Rial, R. and Danezis G., Privacy-Preserving Smart Metering, WPES11.