Smart Meters in Europe: *Privacy by Design* at its Best

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner,
Ontario, Canada

Foreword by Alexander Dix, LL.M.
Commissioner for Data Protection and Freedom of Information
Berlin, Germany

April 2012

Acknowledgements

The IPC is grateful to have had the cooperation of Vattenfall Berlin in providing a case study for the implementation of smart meters. Vattenfall Berlin has taken a consumer-focussed approach to meter installation and has also taken privacy seriously. We also thank Dr. Joerg Klose, Associate Partner at IBM's Global Center of Competency for Energy and Utilities for his valuable contributions to this paper. We appreciate that Bram Reinders, Alliander, brought to our attention their recent accomplishment of a successful privacy and security certification effort which we have added to this paper.

The author would also like to thank Michelle Chibba, Director, Policy and her team, for their contributions to this paper.

Information and Privacy Commissioner, Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Table of Contents

Foreword

As Commissioner for Data Protection and Freedom of Information of Berlin, Germany, I am pleased to be able to provide the foreword to the following paper on privacy and the modernization of the electrical grid. This paper focuses on the aspect of the Smart Grid that will have most immediate impact on individuals – the smart meter. It looks at the privacy issues related to the smart meter from European and North American perspectives, and borrows from the leadership path that Ontario has paved in *Privacy by Design*[1] to present a means of building privacy into this technology from the design stage.

Privacy involves the right to control one's personal information, and the ability to determine if and how that information should be obtained and used. In Germany, the Constitutional Court ruled that all citizens have the right to "informational self-determination" (an individual's ability to determine the uses of one's information). While such an explicit constitutional guarantee to privacy is not always present, most countries with privacy laws have the notion of self-control as one of the goals of their legislation.

I am fortunate to have in place a strong legislative framework for privacy in my jurisdiction, which has just been extended to the Smart Grid. A recent resolution from the Data Protection Commissioners of Germany demanded "legal regulation for the collection, processing and use of information on consumption collected by digital meters."[2] The regulation must ensure data subjects' legitimate interests are taken into account, stipulate strict purpose limitations for data use, and ensure transparency of data processing. Data protection must also be built into the planning and design of the metering infrastructure. I recommend that all national and international Smart Grid regulatory frameworks should be similarly influenced by the principles of *Privacy by Design*, in order to further motivate the adoption of privacy-friendly smart meters and applications.

Without a doubt, we are at a critical point in time in the process to address privacy issues in the Smart Grid, by building protections into both its associated technologies and regulatory frameworks. I am happy to see that a broad spectrum of organizations, including regulators, utilities, and academic researchers are coming together on efforts such as this paper to show that the Smart Grid can be a positive-sum technology, concurrently protecting privacy, reducing energy consumption, and modernizing the electrical grid.

Alexander Dix, LL.M.
Commissioner for Data Protection and Freedom of Information
Berlin, Germany

1 On October 29, 2010, Dr. Ann Cavoukian's concept of "*Privacy by Design*" reached a tipping point. At the 32nd annual International Conference of Data Protection and Privacy Commissioners, a worldwide assembly of regulators unanimously agreed to adopt what has been described as a "landmark" resolution regarding *Privacy by Design.*

2 Resolution of the 80th Conference of the Data Protection Commissioners of the Federation and of the Länder of 3 / 4 November 2010. Available online at: http://www.datenschutz-berlin.de/attachments/823/Appendix_2.pdf

Introduction

With the ongoing growth of the Smart Grid, the role of the utility is changing. Historically, energy providers focused on distribution, aiming to maintain a low-cost, safe, efficient, and reliable supply of electricity. In this role, interactions with customers largely involved billing and minimizing credit risk. However, with the current redesign of electrical systems, utilities' approaches are being radically re-thought, as smart meters allow the collection of information about the usage patterns of their residential customers at a level of detail that was previously unavailable. This has allowed for intricate load-balancing operations, energy efficiency programs, variable pricing, and an array of other systems and services.

These advanced metering infrastructures are requiring that a new relationship emerge between utilities and individuals, centred on customer engagement. The European Regulators' Group for Electricity and Gas (ERGEG), for instance, states that "it is of utmost importance that the customers' opinions of [a] smart metering system are positive, and not a source of anxiety," and that "[f]or ERGEG, it is of the utmost importance that the privacy of customers is protected."[3] Consumer trust and confidence will be essential factors in the success of any new consumer-utility relationship.

Fortunately, concurrent to this change in the consumer-utility relationship is the global adoption of the principles of *Privacy by Design* (*PbD*). From its origins with the Information and Privacy Commissioner of Ontario, Canada (IPC) in the mid-90s, *PbD* has become a worldwide standard, and was recognized as "an essential component of fundamental privacy protection" through an International Resolution unanimously passed at the International Data Protection and Privacy Commissioners' Conference in October 2010. *PbD* shows organizations that, by considering privacy from the outset, they can achieve a positive-sum scenario – meeting both privacy and functionality requirements. In fact, the Smart Grid, in its current nascent state, is at an ideal stage for the application of *Privacy by Design* (though, as the recent *Privacy by ReDesign*[4] initiative shows, it is never too late to build in privacy). The European Commission's Expert Group 2 (EG2) has concluded that compliance with privacy legislation will depend on, among other things, the design, functionality, and implementation of the technologies that enable the Smart Grid.[5] Accordingly, it must be shown how such technologies include data privacy and security considerations from the very beginning of design.

The IPC has produced numerous white papers on the topic of the Smart Grid.[6] In these papers, a set of Best Practices for Smart Grid *Privacy by Design* have been defined, and the implementation of these

3 European Regulators Group for Electricity & Gas (Jun. 10, 2010) "An ERGEG Public Consultation Paper on Draft Guidelines of Good Practice on Regulatory Aspects of Smart Metering for Electricity and Gas," online: http://www.smartgrids-cre.fr/media/documents/100610_ERGEG_SmartMeteringGuidelinesGoodPractice.pdf

4 Cavoukian, A. and Prosch, M. (2011) *Privacy by ReDesign: Building a Better Legacy,"* online: http://privacybydesign.ca/content/uploads/2010/03/PbRD.pdf

5 Task Force Smart Grids Expert Group 2 (2011) "Regulatory Recommendations for Data Safety, Data Handling and Data Protection," online: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

6 IPC Ontario. (2009) SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation. Online: http://www.privacybydesign.ca/content/uploads/2009/11/pbd-smartpriv-smartgrid.pdf; IPC Ontario (2010) *Privacy by Design*: Achieving the Gold Standard in Data Protection for the Smart Grid. Online: http://www.privacybydesign.ca/content/uploads/2010/03/achieve-goldstnd.pdf; IPC Ontario (2011) Operationalizing *Privacy by Design*: The Ontario Smart Grid Case Study. Online: http://www.privacybydesign.ca/content/uploads/2011/02/pbd-ont-smartgrid-casestudy.pdf; Cavoukian, A. (2011) *Privacy by Design*: Best Practices for Privacy and the Smart Grid. Pohlmann, N., Reimer, H., Schneider, W. (Eds.) ISSE 2010: Securing Electronic Business Processes.

practices for the Hydro One distribution network (the largest in Ontario) has been examined. Here, we broaden the scope of our examination of Smart Grid initiatives. As noted, *Privacy by Design* is a global movement; it is thus instructive to describe implementation strategies in multiple jurisdictions. In this paper, we take an international perspective (focusing on developments in Europe) in examining both the Smart Grid – a network that will be interconnected across jurisdictional boundaries – and the development/deployment of smart metering initiatives, looking at both the mandates informing them and the technologies and policies through which *Privacy by Design* has been implemented.

Background and Definitions

Similar to the situation found in many areas of the world, in Europe there is a need to renew electricity networks, meet the challenges of a growing demand for electricity, enable a trans-European electricity market and integrate more sustainable generation resources into the power grid. This has led to the European Commission establishing the European Technology Platform for the Electricity Networks of the Future (ETP SmartGrids), to develop a joint vision for Europe's future electricity networks. Traditional reliance on fossil fuels has been called into question, due to concerns about future energy security and the environmental impacts of greenhouse gases. The European Union (EU) has signaled its desire for a shift toward renewable energy sources through its commitment to the "20/20/20 objectives" – a 20 per cent reduction in emissions, a 20 per cent increase in renewable generation, and a 20 per cent improvement in energy efficiency by 2020. The drive for these changes to lower-carbon generation technologies and improved demand-side efficiency will require significant changes in the design and control of the electricity network at the regional, national, and European levels. As a result, planning and development of the Smart Grid is occurring widely throughout the European Union,[7] with Smart Grid technology being supported by significant public and private investment. The scale of the changes for EU Member States has been estimated to be over €750 billion in power infrastructure over 30 years.[8]

While there is no universal definition for the term "Smart Grid," for the purpose of this paper we use the definition given by the German Commission for Electrical, Electronic and Information Technologies (DKE), which states:

"The term 'Smart Grid' (an intelligent energy supply system) comprises the networking and control of intelligent generators, storage facilities, loads and network operating equipment in power transmission and distribution networks with the aid of Information and Communication Technologies (ICT). The objective is to ensure sustainable environmentally sound power supply by means of transparent, energy- and cost-efficient, safe and reliable system operation."[9]

7 See, for instance, European Smart Metering Landscape Report. Available online: http://www.smartregions.net/GetItem.asp?item=digistorefile;253415;1522&params=open;gallery, or the EURELECTRIC and European Commission's Joint Research Centre's Interactive Smart Grid projects map at http://www.smartgridsprojects.eu/map.html

8 European Technology Platform SmartGrids (2007) Strategic Research Agenda for Europe's Electricity Networks of the Future, p. 8. Online: http://www.smartgrids.eu/documents/sra/sra_finalversion.pdf

9 German Commission for Electrical, Electronic and Information Technologies of DIN and VDE. (2010) The German Roadmap – E-Energy / Smart Grid. Online: http://www.smartgrids-cre.fr/media/documents/regulation/Feuille_de_route_Allemagne.pdf

Further clarity for this discussion is taken from a December 2010 Task Force Smart Grids, Expert Group 2 (EG2) report, which proposed definitions of key terms in the context of the Smart Grid.[10] For instance, in order to establish a common framework, the report refers to the definition of "personal data" given in the EU Data Protection Directive: "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); 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."

EG2 also found that a data type may be classified based on the use of the data, and defined two new data types in the context of Smart Grids. Technical data is defined as data "gathered from metering, distribution, or transmission assets in order to assess the performance of the energy network, network problems, or potential problems, security breaches or energy theft" and used for "safety, revenue protection, and security of supply purposes." The collection of technical data "would be based on aggregated and anonymous data e.g. street or building-related and could not be retraced to the individual end consumer."[11] In contrast, consumer data is defined as data "gathered from individual metering points with the intent to use this data for billing purposes or to provide value added services to consumers with their consent." The EG2 report specifies that since consumer data can be linked with the point of consumption, such as a household or an individual consumer, it is considered to be information about "personal or material circumstances of an identified or identifiable natural person" and therefore must be treated as personal data.[12]

In April 2011, two other important documents were released in the EU – the European Commission's communication titled "Smart Grids: from innovation to deployment,"[13] and the Article 29 Data Protection Working Party's "Opinion 12/2011 on smart metering."[14] In the former, the European Commission identifies five challenges that must be tackled in order to accelerate Smart Grid deployment, along with actions required to meet each one. The challenges are:

1) Developing technical standards

2) Ensuring data protection for consumers

3) Establishing a regulatory framework to provide incentives for Smart Grid deployment

4) Guaranteeing an open and competitive retail market in the interest of consumers

5) Providing continued support to innovation for technology and systems.

Meeting these challenges, through elements such as *Privacy by Design*, is noted as a means by which technological leadership and future competitiveness can be assured.

10 Task Force Smart Grids, Expert Group 2: Regulatory Recommendations for Data Safety, Data Handling and Data Protection, Report, Version 1.2, July 29, 2010.

11 Task Force Smart Grids Expert Group 2 (2011), p. 9, 29.

12 Ibid.

13 European Commission (Apr. 12, 2011) "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Smart Grids: from innovation to deployment," online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:EN:PDF

14 Article 29 Data Protection Working Party (Apr. 4, 2011) "Opinion 12/2011 on smart metering," online: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

The Article 29 Working Party opinion, on the other hand, addresses the definition of personal data in the context of smart metering as well as the issue of data controllership, and reviews legitimate grounds for the processing of information. It is found that information generated by smart meters does, in many cases, meet the criteria of 'personal information' (as per the EG2 report, above), and that the data controller (which must be clearly delineated, if multiple parties are involved in the collection/processing of data), has an obligation of care for that data.

The Article 29 Working Party opinion also notes that "smart metering implementation should take place with privacy built in at the start, not just in terms of security measures, but also in terms of minimizing the amount of personal data processed." This principle of *Privacy by Design* can, in fact, be found in each of the reports mentioned above. In the following sections, we will examine the ways in which smart metering initiatives have actualized this principle by incorporating privacy into their development and deployment phases, as well as describe why this is a necessary task.

Finally, in September 2011, the 50th Meeting of the International Working Group on Data Protection in Telecommunications (IWGDPT) adopted a paper titled "*Privacy by Design* and Smart Metering: Minimize Personal Information to Maintain Privacy,"[15] upon which the current paper is an expansion. While the recommendations found in the IWGDPT paper and the current paper are largely consistent, the IWGDPT added another consideration: that, in addition to building privacy into Smart Grid technologies, regulatory frameworks should be designed to foster the introduction and use of privacy-friendly smart meter and Smart Grid applications. Though this concept is wholly supported, it is not explored further within the current paper.

Smart Metering

Though the Smart Grid has many facets, the one that will be most apparent to consumers will be the smart meter – the "essential first step" toward the implementation of a broader Smart Grid.[16] These meters, which incorporate two-way communications and enhanced individual usage information, will allow energy consumers to regulate their own consumption and utilities to enable demand response and load balancing functions. They will also play a key role in the development of improved power savings strategies to support the international fight against global warming, while allowing consumers to reduce consumption through information and feedback systems.[17] This technology is also very immediate, with numerous pilot projects related to smart metering taking place around the world. Pike Research states that over 17.8 million smart meters were shipped in Q4 of 2011,[18] and that the

15 Available online at: http://www.datenschutz-berlin.de/attachments/842/675.43.18_WP_Privacy_and_Smart_Metering.pdf?1321458912

16 Commission Staff Working Paper (2010) Interpretative Note on Directive 2009.72/EC Concerning Common Rules for the Internal Market in Electricity and Directive 2009/73/EC Concerning Common Rules for the Internal Market in Natural Gas, p. 8. Online: http://ec.europa.eu/energy/gas_electricity/interpretative_notes/doc/implementation_notes/2010_01_21_retail_markets.pdf

17 Pacific Northwest National Laboratory. The Smart Grid: An Estimation of the Energy and CO2 Benefits. http://energyenvironment.pnnl.gov/news/pdf/PNNL-19112_Revision_1_Final.pdf

18 Pike Research. (2012) Smart Grid Deployment Tracker 4Q11. Online: http://www.pikeresearch.com/research/smart-grid-deployment-tracker-4q11

global penetration rate of smart meters is expected to reach 59 per cent by 2020.[19] These meters will play an integral role in utilities' overall Advanced Metering Infrastructures, which, while not further discussed here, will also require the incorporation of appropriate privacy protections at the system level.

In the European Union (EU), Directive 2009/72/EC (of the Third Legislative Package) was adopted in July 2009, which provides that in order to promote energy efficiency, Member States will ensure the implementation of "intelligent metering systems" to assist active consumer participation in the electricity supply market, though such implementation may be subject to an economic assessment of long-term costs and benefits. Such assessments must be completed by September 3, 2012. Where the roll-out of smart meters is positively assessed, Member States must ensure that at least 80 per cent of consumers will be equipped with smart meters by 2020.[20] The Directive also includes measures to ensure that customers have access to their consumption data, and are properly informed of actual electricity consumption and costs frequently as to enable them to regulate their own consumption.[21] Furthermore, a recast of Directive 2010/31/EU on energy performance of buildings states that Member states shall encourage the introduction of intelligent metering systems whenever a building is constructed or undergoes major renovation.[22]

Smart meters represent a significant change in data collection practices for utilities. 'Dumb' meters collect consumption information for the purpose of billing; data from 'smart' meters, on the other hand, can play a significant role in load management and energy conservation efforts. This change should not, however, be approached as a simple expansion of current practices; rather, as with any modernization effort, an opportunity is presented for utilities to re-think their data usage, collection, and retention policies, and not just replicate existing ones in a new domain. For instance, Gurses, Troncoso and Diaz (2008) describe a five-step process[23] to engineer *Privacy by Design*. "Re-thinking" data policies is the first step – a fundamental requirements analysis. Such an analysis allows utilities to determine what information flows are necessary, as opposed to beneficial (with the individual maintaining full control of the latter). As will be shown later in this paper, many utilities and researchers are showing that significant innovation is possible with regard to consumer privacy and data security when system requirements are understood at this simplest possible level.

What is a Smart Meter?

There is no standard definition for the term "smart meter"; in fact, the term has been applied to a variety of devices that incorporate different functionalities. There are, though, certain basic characteristics shared by most smart meters currently deployed. The most fundamental of these qualities is the digital metering of household energy consumption at a relatively fine level of granularity – hourly readings

19 Pike Research. (2011) Smart Meter Market Forecasts. Online: http://www.pikeresearch.com/research/smart-meter-market-forecasts

20 EU Third Package for Electricity and Gas Markets.

21 Ibid.

22 OJ L 153, 18.6.2010, online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:153:0001:0012:EN:PDF

23 1) Functional Requirements Analysis; 2) Data Minimization; 3) Modelling Attackers, Threats and Risks; 4) Multilateral Security Requirements Analysis; 5) Implementation and Testing of Design.

of energy used, for instance. This granularity allows for the collection of "interval consumption" data which enables the possibility of Time-of-Use billing, by which different energy rates are applied based on the time at which energy was consumed. A digital readout displaying household energy consumption data (such as current or historic interval consumption) will generally be present, along with a means of communicating this information to another device (e.g. a smartphone or television). Smart meters may also be equipped with internal memory sufficient to enable the storage of all readings for at least a six-month period.

Typically, smart meters are also equipped with bi-directional communication functionality. This allows utilities to remotely read the meters (at a significantly reduced cost, compared to the onsite reading of meters by a utility employee), and increasingly is enabling consumers to monitor their historic interval consumption via online web portals. In some jurisdictions, this bi-directional communication may allow the consumer to install a special device on an appliance that automatically controls its energy consumption based on the network load. For example, during a heat wave (or other peak demand period), a utility may communicate with a smart meter to request a two-degree Celsius shift in temperature setting for any air conditioning system associated with the meter, in order to better maintain the balance between energy supply and demand.

Some smart meters with bi-directional communication capabilities may also be equipped with remote enablement and disablement of supply functionality, enabling a utility to remotely connect or disconnect the consumer. This feature allows utilities to enable energy supply to new accounts and to disable energy supply to existing accounts without having to send a service technician to the account site. It also enables the application of a pre-pay tariff system.

Finally, although smart metering to date has been focused on electrical power consumption, it is anticipated that smart meters may also be used for water, gas, and heat. Accordingly, some smart meters are being designed to support metering of multiple utilities in order to avoid unnecessary duplication of infrastructure.

Privacy and the Smart Meter

Since its introduction, numerous groups and regulatory agencies have focused on the need to protect consumer privacy in the Smart Grid. This need arises from the increased data flows in this system – the Smart Grid is expected to generate up to eight orders of magnitude more data that the current power network,[24] which in some cases, could reveal detailed information about a person. This increase in electrical consumption data is paired with remote reading and collection of the data, raising issues with regard to transparency and consumer control of data.[25]

Research suggests that as the Smart Grid matures, consumer lifestyles could be gleaned from the information generated. Through energy signatures, inferences about time-of-use, and other factors, it may be possible to determine whether individuals tend to cook microwavable meals or meals on the

24 "Accenture Launches Smart Grid Data Management Solution to Reduce Risks and Costs of Smart Grid Deployments," Mar. 18, 2010, online: http://newsroom.accenture.com/article_display.cfm?article_id=4971

25 Resolution of the 80th Conference of the Data Protection Commissioners of the Federation and of the Länder (Nov. 3-4, 2010), "Data protection in connection with digital metering and control of energy consumption."

stove; whether they have breakfast; the time at which individuals are at home; whether a house has an alarm system and how often it is activated; when occupants usually shower; when the TV and/or computer is on; whether appliances are in good condition; the number of gadgets in the home; if the home has a washer and dryer and how often they are used; whether lights and appliances are used at odd hours, such as in the middle of the night; and/or whether and how often exercise equipment such as a treadmill is used.[26] In combination with other information, it may be derived, for instance, that the homeowner tends to arrive home shortly after the bars close, the individual is a restless sleeper and is sleep deprived, the occupant leaves late for work, the homeowner often leaves appliances on while at work, the occupant rarely washes his/her clothes, the person leaves their children home alone, the occupant exercises infrequently, or numerous other lifestyle characteristics.[27]

Even if electricity use is not recorded minute by minute, or at the appliance level, ongoing monitoring of electricity consumption may reveal the approximate number of occupants in a household, when they are present, as well as when they are awake or asleep.[28] This may threaten the notion of the "sanctity of the home," where such intimate details of daily life should not be accessible without the knowledge of the occupant(s).

It is not yet clear who along the grid will have access to a user's personal information and where on the grid such access will be possible. Some utilities have indicated that they have no need or desire for device level electricity usage for their grid management needs. On the other hand, a recent study out of the Cambridge University Computer Laboratory notes that in the U.K., the government wants gas and electricity meter reading from every household in the country every half hour.[29] Further to this, there is a risk that personally identifiable information could be used for purposes other than that for which it was originally collected.[30]

26 Hart, George: Nonintrusive Appliance Load Monitoring. Proceedings of the IEEE, Vol. 80, No. 12, December 1992; Leo, Alan: The Measure of Power: Non-Intrusive Load Monitoring Gives Detailed Views of Where Power is Going, With Payoffs for Utilities, Consumers, and maybe Big Brother. Technology Review Magazine, June 28, 2001; Lisovich, Mikhail and Wicker, Stephen: Privacy Concerns in Upcoming Residential and Commercial Demand-Response Systems. IEEE Proceedings On Power Systems, Vol. 1, No. 1, March 2008; Laughman, Christopher; Lee, Kwangduk; Cox, Robert; Shaw, Steven; Leeb, Steven; Norford, Les and Armstrong, Peter: Power Signature Analysis. IEEE Power & Energy Magazine, March/April 2003; Quinn, Elias Leake: Privacy and the New Energy Infrastructure. Centre for Energy and Environmental Security, Working Paper Series, 2009.

27 Quinn, Elias Leake: Privacy and the New Energy Infrastructure. Centre for Energy and Environmental Security, Working Paper Series, 2009

28 Jamieson, Alastair: Smart meters could be 'spy in the home.' Tony Gallagher: The Telegraph, October 11, 2009; Martin, Peter (J.A): R. v. Gomboc. 2009 ABCA 276, 247 C.C.C. (3d) 119. 2009; Maykuth, Andrew: Utilities' smart meters save money, but erode privacy. The Philadelphia Inquirer, September 6, 2009.

29 Anderson, Ross and Fuloria, Shailendra: On the security economics of electricity metering. In: Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS 2010), 2010.

30 California Public Utilities Commission: Decision Adopting Requirements For Smart Grid Deployment Plans Pursuant To Senate Bill 17 (Padilla), Chapter 327, Statutes Of 2009. California Public Utilities Commission, 2010.

Smart Metering and *Privacy by Design*

In February 2011, the European Commission's Expert Group 2 stated that "in Europe energy theft and privacy are the most important concerns related to Smart Grid implementation.[31] It has suggested that "the dilemma the energy sector needs to address up-front is how best to deliver appropriate levels of security and privacy, which are essential to facilitate the consumer's buy-in."[32] In particular, a key recommendation of the EG2 Report details the need for additional pilots in the area of data handling to "propose a list of high level principles tuned to the Smart Grid environment, by which Smart Grid Operators can design their systems and processes."[33]

Fortunately, as noted in the introduction to this paper, we have entered the era of international acceptance of the principles of *Privacy by Design*. The *PbD* standard of designing protections in from the outset has become a hallmark of privacy and security analyses of the Smart Grid and Smart Metering. For instance, as previously noted, in September 2011 the International Working Group on Data Protection in Telecommunications (IWGDPT) adopted a paper titled "*Privacy by Design* and Smart Metering: Minimize Personal Information to Maintain Privacy" (upon which the current paper is an expansion). Focusing again on Europe, other instances of *PbD* adoption include:

- **Expert Group 2:** "If privacy is addressed at the design phase of the Smart Grid ('privacy by design'), it is possible to derive user and business friendly solutions;" "Be aware of future function creep and incorporate privacy and security considerations early on in the development by applying 'privacy (and security) by design' principles"[34]
- **Article 29 Working Group**: "Smart metering implementation should take place with privacy built in at the start, not just in terms of security measures, but also in terms of minimising the amount of personal data processed"[35]
- **European Commission**: "The Smart Grids Task Force has agreed that a 'privacy by design' approach is needed. This will be integrated in the standards being developed by the ESOs [European Standards Organizations]"[36]
- **European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) / Bureau Européen des Unions de Consommateurs (BEUC):** "Privacy should be designed into smart meter systems right from the start as part of the compliance life-cycle and include easy to use privacy-enhancing technologies.We urge to make the principle of privacy by design mandatory, including principles of data minimization and data deleting"[37]

31 Task Force Smart Grids Expert Group 2 (2011), p. 4.

32 Ibid. p. 14.

33 Ibid. (2011), p. 6.

34 Task Force Smart Grids Expert Group 2 (Feb. 16, 2011) "Regulatory Recommendations for Data Safety, Data Handling and Data Protection," online: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

35 Article 29 Data Protection Working Party (Apr. 4, 2011) "Opinion 12/2011 on smart metering", online: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

36 European Commission (Apr. 12, 2011) "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Smart Grids: from innovation to deployment," online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:EN:PDF

37 ANEC/BEUC "Smart Energy Systems for Empowered Consumers," online: http://www.anec.org/attachments/ANEC-PT-2010-AHSMG-005final.pdf

- **Public Interest Energy Research (PIER) Program:** "Privacy considerations must drive architectural and information flow design decisions within the network, as well as the policies that cover Smart Grid data held by the growing array of entities that will help reap the benefit of this investment. Because privacy must be embedded in technical design, it cannot be addressed adequately by policies created once technologies have matured" [PIER Report]
- **Trans-Atlantic Consumer Dialogue (TACD)**: [The EU and US government should] "Encourage privacy and security by design, including data minimization, anonymization, and aggregation, and models that focus on consumers' maintaining control of their utility consumption data"[38]

The following comments were offered in response to an ERGEG consultation paper on smart metering[39]:

- **Netbeheer Nederland**: "At least the following privacy & security fundamentals need to be addressed, based on a risk analysis: End-to-end security; Privacy by design"[40]
- **Bureau Européen des Unions de Consommateurs (BEUC):** "To significantly minimise the risks and to secure users' willingness to rely on smart meters, it is crucial to integrate, at practical level, data protection and privacy from the very inception of the Smart Metering Project and at all stages of its development: security and privacy by design. We would like to point out the importance of privacy by design particularly when implementing the principle of data minimisation, ensuring the safe disposal of data and the limitation of data retention"[41]

In response to ERGEG consultation paper on Smart Grid:[42]

- **Consumer Focus**: "Privacy by design should be a key requirement. This means that the security architecture and standards should be built in at the outset for the hardware and software, as well as any systems and processes, rather than bolted on later"[43]

Privacy by Design is providing organizations with a means to, by considering privacy from the outset, achieve a positive-sum scenario – meeting both privacy and functionality requirements. The movement towards the Smart Grid and, in particular, smart metering, in its current nascent state, is at an ideal stage for the application of *Privacy by Design*. In 2010, the Information and Privacy

38 Trans Atlantic Consumer Dialogue (June 2011) "Resolution on Privacy and Security Related to Smart Meters," online: http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=294&Itemid=

39 European Regulators Group for Electricity & Gas (Jun. 10, 2010) "An ERGEG Public Consultation Paper on Draft Guidelines of Good Practice on Regulatory Aspects of Smart Metering for Electricity and Gas," online: http://www.smartgrids-cre.fr/media/documents/100610_ERGEG_SmartMeteringGuidelinesGoodPractice.pdf

40 Netbeher Nederland (Aug. 30, 2010) "Aggregation of the response of Dutch Distribution System Operators (DSO's) on the ERGEG Smart Metering Guidelines concept," online: http://www.energy-regulators.eu/portal/page/portal/EER_HOME/EER_CONSULT/CLOSED%20PUBLIC%20CONSULTATIONS/CUSTOMERS/Smart%20metering/RR/GGP%20Smart%20Metering_Netbeheer%20Nederland.pdf

41 BEUC "BEUC draft response on ERGEG public consultation paper on draft guidelines of good practice on regulatory aspects of smart metering for electricity and gas," online: http://www.energy-regulators.eu/portal/page/portal/EER_HOME/EER_CONSULT/CLOSED%20PUBLIC%20CONSULTATIONS/CUSTOMERS/Smart%20metering/RR/GGP%20Smart%20Metering_BEUC.pdf

42 ERGEG (Dec. 10, 2009) Position Paper on Smart Grids: An ERGEG Public Consultation Paper."

43 Consumer Focus (Mar. 2010) "Consumer Focus response to the ERGEG Position Paper on Smart Grids," online: http://www.energy-regulators.eu/portal/page/portal/EER_HOME/EER_CONSULT/CLOSED%20PUBLIC%20CONSULTATIONS/ELECTRICITY/Smart%20Grids/RR/smart%20grids_Consumer%20Focus.pdf

Commissioner of Ontario, Canada introduced *Best Practices for Privacy on the Smart Grid*. These practices are a means by which parties can use *Privacy by Design* to achieve the gold standard of privacy protection in Smart Grid projects. Below, we offer a number of recommendations for smart metering initiatives, based on these *Best Practices*, which we feel should be incorporated into national and international regulatory frameworks where this is not already the case.

PbD Recommendations for Smart Metering[44]

1) Smart metering initiatives should feature privacy principles in the overall project governance framework and proactively embed privacy requirements into their design, in order to prevent privacy-invasive events.

Utilities should conduct Privacy Impact Assessments (PIAs) or similar types of assessments as part of the requirements and design stages of smart metering initiatives. Within this evaluation, two important considerations must be made. First, utilities must make a determination of what smart meter-based information is *required* to meet legitimate objectives (and at what level of identifiability), rather than of what information is made *available* by smart metering. Mechanisms must then be put in place to allow consumers to maintain control over any available, non-necessary information.

Secondly, as little information as possible should leave the consumer's home via the smart meter. To achieve as little personal data flow as possible, utilities may use techniques such as anonymization, pseudonymization, or data aggregation.[45] Local gateways for individual buildings or small neighbourhoods, which allow the consumer to gain insight into their energy usage without the need for transmission of information about identifiable consumers to the utility, should be applied. Such gateways should generally not be externally accessible and work with defined access protection profiles, while communication should be push-based (initiated by the gateway). Other measures, such as larger intervals between individual readings, can also prevent a detailed profile about the consumer's lifestyle from being generated. Of course, high technical standards for securely storing and accessing the data will be essential.

Many utilities and researchers are showing that significant innovation is possible when system data requirements are understood at the simplest possible level, stripping away personal information where possible. Examples include:

- **Radboud University (Netherlands)**, which showed that total energy consumption for a neighbourhood can be securely determined without revealing individual readings through a homomorphic encryption scheme, which allows encrypted individual meter readings to be summed without first being decrypted.[46]

44 These recommendations are also found in "Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy," presented at the 50th International Working Group on Data Protection in Telecommunications (IWGDPT).

45 For instance, see Kursawe, K., Danezis, G, and Johlweiss, M. (2011) Privacy-Friendly Aggregation for the Smart-Grid; and Jawurek, M., Johns, M., and Kerschbaum, F. (2011) Plug-in privacy for Smart Metering billing; both in Fischer-Hübner, S. and Hopper, N (Eds): Proceedings of the 11th Privacy Enhancing Technologies Symposium, Waterloo, ON, July 2011.

46 Garcia, F. and Jacobs, B. (2010) Privacy-friendly Energy-metering via Homomorphic Encryption. 6th Workshop on Security and Trust Management (STM 2010). Online: http://www.cs.ru.nl/~flaviog/publications/no-leakage.pdf

- **Radboud University and Microsoft Research**, who have developed protocols to privately compute aggregate meter measurements over defined sets of meters, allowing for fraud and leakage detection as well as network management and statistical processing, without revealing any additional information about the individual meter readings.[47]
- **NEC**, which developed a system that adds random values to each meter reading, such that over a large number of readings they will sum to zero. The parameters of the random distribution are chosen to maximize precision when successive meter readings are aggregated, while achieving individual readings that are as "blurry" as possible. In addition, aggregation of these readings for a particular area of interest to a utility would be assigned to a trusted third party (an aggregation proxy).[48]
- **Toshiba** created a system that reduces the quality of smart meter readings (to prevent clear inferences of lifestyle information) by partially powering active devices with batteries, effectively masking their energy consumption signatures.[49]

2) Smart meters must protect privacy by default, with no action required on the part of the consumer.

In order to ensure its presence, privacy should always be protected as the default condition. Privacy should be in a "no action required" mode; consumer actions should allow *disclosure*, not ensure *protection*, of personal information (information collected for core utility services notwithstanding). At least two particular considerations must be made here. First, where multiple options (with regard to either the type of meter or its initial settings) are presented to the consumer, the default option must be the more privacy-protective one. Secondly, even where consumers have opted to have detailed consumption information collected by the smart meter, the informed, positive consent of those individuals must be sought prior to each separate use or disclosure of this information for non-primary purposes.

3) Privacy must be an essential design feature for smart meter systems and practices.

As smart metering initiatives are seen in an increasing number of jurisdictions worldwide, a number of industry best practices and legislative requirements are under development. These will enhance the efforts of utilities and third parties to create privacy-friendly practices for the collection, use, and disclosure of smart meter-based information. However, privacy cannot be solely reliant on legislative or administrative protections; it must also be designed into the technology itself. As the point of collection, smart meters can play a clear role in defining what data will enter the larger Smart Grid ecosystem, and the form in which it will do so.

Underlying the requirements of *Privacy by Design* is the concept of data minimization – the idea that the collection, use, disclosure, and retention of personal information should be minimized wherever, and to the fullest extent, possible. This concept has become a leading approach to the protection

47 Kursawe, K., Danezis, G, and Johlweiss, M. (2011) Privacy-Friendly Aggregation for the Smart-Grid. Fischer-Hübner, S. and Hopper, N (Eds): Proceedings of the 11th Privacy Enhancing Technologies Symposium, Waterloo, ON, July 2011, pp. 175-191.

48 Bohli, J-M., Ugus, O., and Sorge, C. (2010). A Privacy Model for Smart Metering. In Proceedings of the First IEEE International Workshop on Smart Grid Communications (in conjunction with IEEE ICC 2010).

49 Kalogridis, G. et al. (2011) Privacy protection system and metrics for hiding electrical events. International Journal of Security and Networks, 6:1, pp. 14-27.

of privacy in the Smart Grid. Amongst many similar opinions, the California (USA) Public Utilities Commission has found that "Data minimization is a 'best practice' in a strategy to protect and secure usage data of electric utility consumers."[50]

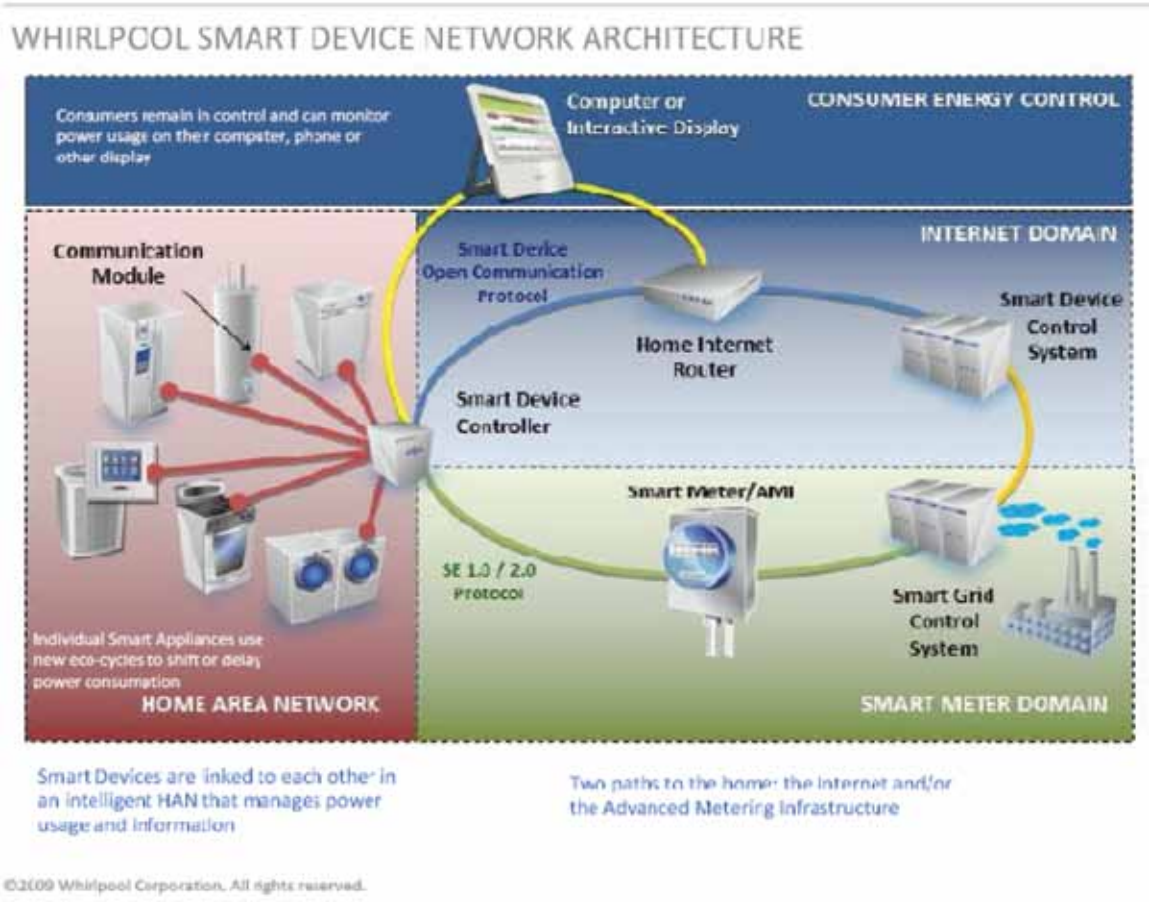

Figure 1 – Home area network communication with smart meter, Internet

Such data minimization cannot come at the cost of functionality, however; it is important that utilities strive to achieve a positive-sum solution, in which both privacy and functionality requirements are met. As such, there is significant research underway to determine the most effective means by which the benefits of the Smart Grid can be achieved with minimal release of personal information. Microsoft, for instance, has proposed a smart metering system in which the meter itself (or a home server or online service) is delegated the responsibility of calculating the user's energy bill, using energy readings from the meter in combination with tariff policies supplied by the utility, both cryptographically-signed to prevent forgery. The system can also, as authorized by the user, selectively disclose fine-grained energy consumption data.[51] This system is designed to still allow, among other functions, aggregated readings and load management.

50 California Public Utilities Commission (2011) Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company. Online: http://docs.cpuc.ca.gov/efile/PD/134875.pdf

51 Danezis, G., and Rial, A. Privacy Preserving Metering for Smart-Grids. Online: http://research.microsoft.com/en-us/projects/privanon/privacy-preservingsmartmetering-execsummaryv3.pdf.

Manufacturers of smart appliances have also been examining means by which user data remains inside consumers' control of homes. For instance, Whirlpool's Smart Device Network Architecture, as depicted in Figure1, describes a means by which a Home Area Network can be used to communicate with a smart meter or Internet service, both controlling "smart" appliances and allowing the user to control how and when data is released.

In both of these examples, potentially sensitive information regarding energy usage is still generated; it does not, however, leave the local network to be transmitted to a utility. Restricting data to a home area network is, though, only a single aspect of an overall approach to data minimization. The strongest protection available to information is to not create or record it; as such, prior to determining how it is used, utilities should give consideration to what data (type, granularity, etc.) needs to be generated at all.

4) Smart metering initiatives must avoid unnecessary trade-offs between privacy and other legitimate objectives.

When privacy is considered to be "at odds" with functionality or other system requirements, organizations will find themselves facing unnecessary trade-offs, with protections being described in terms of "instead of" rather than "in addition to." They may also present consumers with choices between their privacy and energy efficiency/conservation. These approaches run directly counter to the philosophy of *Privacy by Design*, which looks to ensure that all legitimate objectives are met in smart metering initiatives. In the words of EG2, "Smart Grid/Meters and wider related infrastructure should be designed for both privacy and security to levels that are in line with the risks for concerning stakeholders, as well as ensure the realisation of potential benefits of Smart Grids/Meters."

5) Privacy and data security must be maintained end-to-end.

Smart meter-based information – particularly personally identifiable information – must be strongly protected throughout its lifecycle, both at rest and in transit, having regard to the technical requirements of individual countries around security.[52]

There are at least three distinct stages through which Smart Grid consumption data may pass – collection (and potentially processing) in the home, transmission, and use/retention on the utility's (or a third party's) servers. When addressing security of information in the home, the utility's key priority must be the smart meter. It should store only the minimal amount of data necessary and be, to the extent possible, tamperproof – both to ensure correct billing, and to protect the resident(s) of the home. Penetration testing on the devices should be undertaken, to ensure that the smart meter itself is not the "weak link" in the security of energy consumption information.

When data is "in motion" – that is, being transmitted – there is little that a utility can do to ensure that it will not be intercepted. Thus, the focus should be on minimizing the *value* of information in transit. A first level of security would be encryption of any personally identifiable information communicated wirelessly or over networks. Second, where possible, sensitive customer information

52 For example, the "Common Criteria for Information Technology Security Evaluation" (ISO/IEC 15408) form the basis of smart meter security requirements in Germany's Energie Wirtschafts Gesetz (EnWG) (Energy Industry Act, 2011). The requirements relate to firewalls, pseudonymization, access, authentication, encryption, etc. See also, German Federal Office for Information Security, "Protection Profile for the Security Module of a Smart Metering System" (www.bsi.bund.de).

should not be transmitted; for instance, a unique numeric ID (different than any visible serial number on the smart meter) might be included instead of an identifier that can more easily be linked to an individual. It is further preferable that this number vary on occasion, so as to avoid the creation of a static identifier. Thought should also be given on how to minimize any inferences that can be made through the observation of transmissions or transmission patterns – for instance, if a system transmits more frequent, or larger, messages during times of high energy use, patterns of consumption can be inferred without need to decrypt or otherwise parse the message.

Finally, once data has been transmitted and received by an external party, a number of protections must be in place. In addition to standard security measures, personal information should be kept in a minimal number of systems from which it may be securely shared, as it is harder to protect information stored in multiple locations. Access to this information should occur on a need-only basis, to provide additional protection. Appropriate language to protect consumers should be built into contracts with third parties allowed to gain access to personal information for legitimate support purposes. As well, there should also be as little persistence of personal information as possible. As such, at the end of the data lifecycle, personal information must be securely destroyed, in accordance with any legal requirements.

6) Smart metering initiatives should be visible and transparent, and should utilize accountable business practices; consumers must be assured that the technology operates according to stated objectives.

Utilities should be able to show that the methods used to incorporate privacy into their smart metering initiatives will meet the privacy requirements of the project. Ensuring such "requirements traceability" between the foundational privacy principles and each stage of a smart metering initiative will ensure that the utility is ready for a third party audit at any time.

Informing consumers of the use(s) to which personal information collected from smart meters will be put, and establishing a clear and accessible complaints process, are key objectives in achieving visibility and transparency.

7) Smart metering initiatives must be designed to respect consumer privacy.

Consumers must be provided with, and educated about, all necessary information, options, and controls to allow them to manage their energy consumption and their privacy. For instance, ERGEG has stated in its Best Practices document that, "it is always the customer that chooses in which way metering data shall be used and by whom [excepting that needed for regulated duties]."[53]

Again, there are multiple ways in which this can be accomplished. Researchers at the Karlsruhe Institute of Technology in Germany have proposed a communications system by which data consumers, such as utilities, send requests to the smart meter, including identity and purpose; the smart meter would respond based on pre-programmed, user-controllable data release policies.[54] As an alternative strategy for the provision of choice, other utilities give consumers options in the smart meter itself. The

53 European Regulators Group for Electricity & Gas (Jun. 10, 2010).

54 Wagner, A., Speiser, S., Harth, A., Raabe, O., and Weis, E. "Basic Privacy Principles for the Smart Grid." Online: http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-20/.

Netherlands, for instance, made the roll-out of smart meters voluntary, and provided consumers the choice of a meter without communications functionality, a meter with communications functionality that had been turned off (allowing for it to be turned on later, at the consumer's discretion), a meter that communicated readings every two months, or a meter that communicated readings every hour.

In the end, though, *Privacy by Design* requires an additional step: to be truly respectful of privacy, utilities must ensure that customers are clear about the meaning, benefits, and consequences of these choices.

Implementing *Privacy by Design* for Smart Meters

The recommendations for *Privacy by Design* given above form a strong foundation for what *should* be done to protect privacy in smart meters. In this section, we build upon this foundation by demonstrating what *can* be done to protect privacy, by considering three case studies: the first, a utility looking to build privacy into their processes; the second, researchers developing protections for the meter itself, and the third is an example of a utility building a culture of privacy to regain the trust of its customers.

Case Study 1: The Vattenfall Smart Meter Deployment

To show that the *PbD* recommendations for smart metering can, and must, be incorporated into a successful deployment, we will describe the work of Vattenfall, a key player in the German and wider European energy market. As is the case with many utilities, Vattenfall is focusing their research and development efforts on developing new smart meter-enabled services, and using digital information in the planning, operation, and maintenance of distribution systems to effect consumer energy savings, cost reductions, and improvements in reliability. They have moved forward with a pilot project that will see the installation of approximately 10,000 smart meters in the Berlin-Maerkisches Viertel area to support an energy efficiency program, and are preparing for future full-scale roll-outs.

The Vattenfall pilot project includes two types of smart meter (see Figure 2), both of which comply with the minimum functionalities required by German law.[55] The first smart meter, the EDL21, does not communicate with the utility. Instead, it provides the consumer with various display options for energy consumption data, including a digital readout on the meter or the remote display of information on a television or mobile device. For remote display, power line communications (PLC) are used to transmit information to a "TV-Box," an interface device that is uniquely coupled to a single smart meter. The second type of smart meter, the EDL40, is equipped to externally communicate with the utility, and is capable of transmitting signed meter readings and enabling time-of-use tariffs. Should consumers consent to the disclosure of their data to a data store, they are provided the additional option of viewing their historical energy consumption data online.

55 EnwG §21b (3a, 3b), §40 (3)

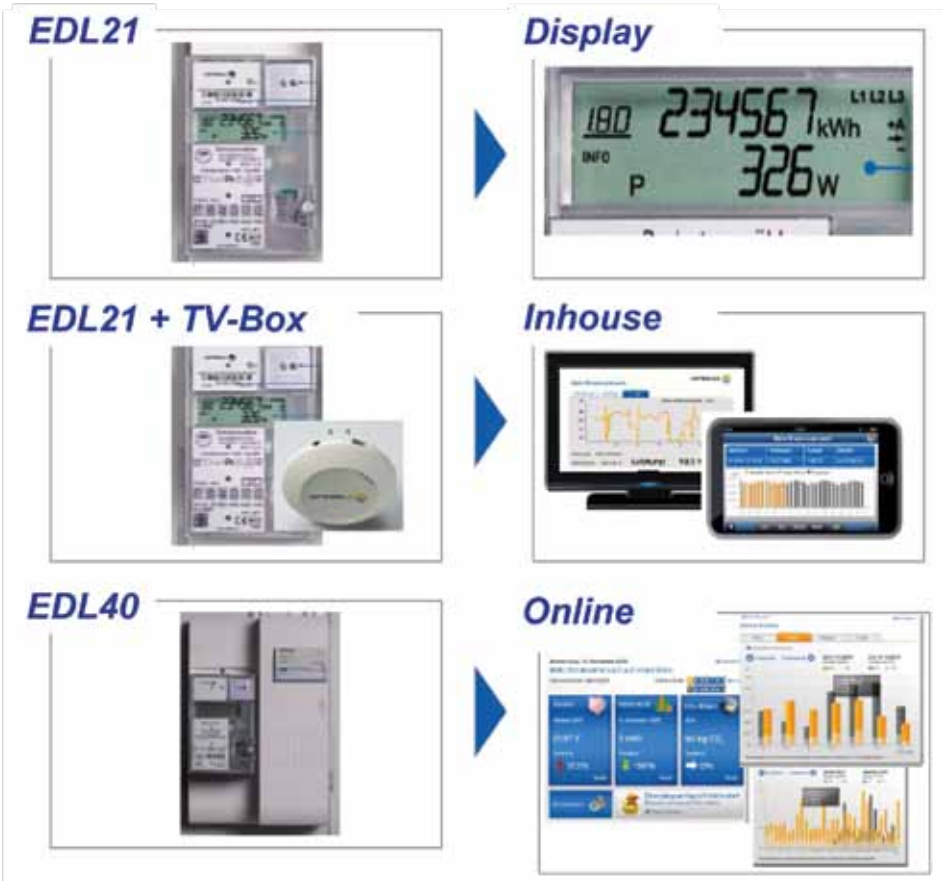

Figure 2 – Different Vattenfall Smart Meter installations[56]
(Source – Vattenfall 2011)

In accordance with German data privacy law, a number of basic principles were adopted in order to ensure that the smart meters protected the privacy of consumers' data. First, consumers are given a choice between the meters described above – and, in particular, whether those meters communicate externally. Second, strong technical guidelines produced by Vattenfall (Vattenfall technical principle guideline TAB 2000) were produced to direct the installation of the meters. Finally, smart meters are not publicly accessible, but instead installed in a specific meter room.

In addition, the following protections were applied to the specific types of smart meter:

EDL21 – On-meter display

A PIN, individual to each smart meter, is provided to each consumer and required to access individual power consumption information (including current power, energy consumption in the past hour/day/week, etc.).

Installation of smart meters is based on technical regulations; depending on the situation, the meter may be installed in a cabinet with glass panels to give the customer visual access to their consumption data, or it may be installed in a locked meter room that must be opened before visual access can be obtained.

56 Coffey, J. (2011, Jan. 21) Smart Meter Pilotprojekt – Märkisches Viertel, Berlin. Online: http://eti-brandenburg.de/fileadmin/eti_upload/downloads2011/Klimakonzepte_Wohnungsbau/7_Jennifer_Coffey.pdf

EDL21 – In-home / mobile display

- The smart meter is uniquely paired to a single TV-box inside the residence, via Power Line Communications; this can also be paired with a WLAN connection in order to access data via a utility-created application on a mobile device.
- Data processing occurs entirely within the house; the data stream is not routed through an external data centre.
- Transmitted data is encrypted with a key known only to the paired smart meter and TV-box.
- The TV-box is returned by the consumer should he or she move, preventing future residents from learning the consumption profiles of previous tenants.

EDL40 – Online display

- Prior to the installation of the meter, the consumer must indicate (by signature) his or her acceptance of remote meter readings and the data protection rules defined by Vattenfall.
- Online access to data visualizations and calculation features is provided via a password-protected, secure Internet portal.
- All data transmitted between the smart meter and the utility is encrypted and sent via SSL.
- Only 2 days of consumption data are stored in the smart meter itself, ensuring there is only a single location (the data centre) at which historical consumption data can be accessed.

In addition to technological considerations, Vattenfall ensured that privacy would be considered in all phases of their pilot project by including their data privacy representative at each step. He served as a key advisor, ensuring the alignment of this project with stringent German data privacy laws and rules, as well as any other applicable regulations. He also served as a valuable source for the elaboration of various approaches to the meeting of data privacy requirements. Overall, with his advice, the following principles have been incorporated into this pilot project:

- Access to data is highly restricted, based on a Vattenfall authorization concept describing which individuals/roles need access to each type of data, as per § 5 BDSG (German data privacy law). All individuals with access to data are legally bound to follow applicable data privacy laws.
- Based on § 5, chapter 1, no. 1, BDSG (German law for data privacy), all data is collected and used exclusively for the purposes specified to the consumer. The collection of any additional data, or use for other purposes of existing data, requires written consent from the data subject (according to § 4 BDSG).

Case Study 2: Aggregated Smart Meter Readings

In addition to building privacy into business processes and the collection of data, *Privacy by Design* can be embedded into the functioning of smart meters themselves. While there have been multiple such technologies developed, we profile here a protocol for the aggregation of smart meter readings

developed by Klaus Kursawe, George Danezis, and Markulf Kohlweiss.[57] These researchers asserted that there was one principle privacy issue surrounding smart metering – the transmission of detailed electrical usage data to the utility (or other third parties). As described previously, frequent meter readings can lead to inferences about an individual's lifestyle. Even an hourly reading of consumption could be used to infer the time at which an individual is both at home and awake – creating initial impressions of the individual's likely lifestyle. This is compounded by the difficulty of taking steps to maintain the privacy of one's electrical consumption behaviour. If an individual wished to increase privacy of their Internet browsing, for instance, he or she could use private browsing modes, use a proxy system, access sites from different computers (Internet cafes, libraries), or adopt one of many other strategies. To prevent profiling based on energy consumption, however, an individual might have to, for instance, change his or her daily patterns, consume energy when he/she is not present (or not consume it when he/she is present), or store energy in a battery system for later consumption – each of which is significant in terms of effort.

To overcome this privacy issue, the researchers concurred with the assertion of multiple groups listed above, that data minimization was a key principle. Specifically, they noted that rather than trying to separate personally identifiable data from the rest, it is best to determine what data is required to perform a task, and ensure that only that data is collected. Extending this line of reasoning, the researchers felt that (except for billing purposes and consumer awareness) the Smart Grid operator does not need to know any individual consumption data – it is sufficient to have aggregate consumption data for a particular area. Thus, they looked to develop a means by which consumption data could be aggregated across a sufficiently large set of customers, subject to a number of constraints. These include:

- The system must be capable of accurately determining individual usage
- The system must be capable of fraud detection / leakage
- Utilities should not lose, and ideally should increase, the functionalities associated with smart metering (must be business positive)
- The system must be robust: failure in one meter cannot break the entire metering system (meters should act independently)
- The system must be capable of functioning within the computational capacity of traditional smart meters
- The system should not greatly increase the number of messages passed by the smart meter

The researchers also chose to work under the assumption (with regard to consumption data) that energy providers may be curious, but unlikely to engage in behaviour that can be shown to deviate from contractual or regulatory obligations.

To further promote data minimization, the researchers noted that there are multiple use cases for the Smart Grid, including demand management, billing, and consumer awareness. The first, the authors note, does not require information from any given meter. Demand management is concerned less

57 Kursawe, K., Danezis, G, and Johlweiss, M. (2011) Privacy-Friendly Aggregation for the Smart-Grid. Fischer-Hübner, S. and Hopper, N (Eds): Proceedings of the 11th Privacy Enhancing Technologies Symposium, Waterloo, ON, July 2011, pp. 175-191. Online: http://research.microsoft.com/pubs/146092/main.pdf

with *who* is consuming electricity as it is with *how* it is being consumed; thus, aggregate information from multiple meters will suffice. Billing, on the other hand, requires information about specific meters, but on a much less granular level (a monthly reading may suffice). Lastly, data for consumer awareness may need to be both individual and granular. Thus, it is suggested, these three data streams should be kept separate, as they require very different forms of the same data. The researchers then turn their attention to two data aggregation protocols that can be used for the first use case – demand management.[58]

The first protocol, called "Diffie-Hellman"-based Private Aggregation (DiPA) is based on a *homomorphic commitment* scheme. A commitment scheme allows for a user (in this case, a smart meter) to "commit" to a secret, and later reveal the secret and prove that this was the value to which it committed.[59] Commitment schemes have two functions:

- **Commit (x, r)**: Given a value *x*, and a random number *r*, Commit outputs the commitment *c*
- **Open (c, x, r)**: Given a commitment *c*, a value *x*, and a random number *r*, Open determines whether *c* is a commitment to *x*.

Commitment schemes have two primary security properties:

- **Secret**: Given *c*, it is hard to compute *x*
- **Binding**: Given *c*, *x*, and *r*, it is hard to compute a different *x'* and *r'* such that *c* is also a commitment for *x'*.

Homomorphic commitments add the special property that computations can be done on the commitments themselves, without having to reveal the secrets.[60] Specifically:

- **Commit (x, r) * Commit (y, s) = Commit (x + y, r + s)**

Thus, for smart meters, DiPA makes it possible to submit a commitment to an aggregate reading from multiple smart meters (the sum total of their energy usage), such that the Smart Grid operator gets the required verifiable demand management data without knowing information about individual household consumption. This protocol also allows for flexible aggregation groups, without meter reconfiguration; thus, a utility could (for instance) aggregate over all smart meters in the area, and then over all consumers that generate electricity.

The second protocol, called Low Overhead Private Aggregation (LOPA), is even simpler than DiPA. For LOPA, each pair of meters in an aggregation group shares a different secret value (that is, for an aggregation group of 10 meters, each meter holds nine shared secrets). When transmitting readings,

58 For a discussion of a privacy-protective means of billing also based on a commitment scheme, see: Jawurek, M., Johns, M., and Kerschbaum, F. (2011) Plug-in privacy for Smart Metering billing, in 11th Privacy Enhancing Technologies Symposium (PETS 2011).

59 The researchers explain this using a Lego-car analogy, in which the original data is a constructed Lego car, the commitment scheme is a rubber hammer to break the blocks apart, and the commitment is the resulting heap of blocks. Knowing only the blocks (the commitment), it is computationally difficult to reconstruct the car (the original data); however, if one knows the car (original data), it can easily be verified to correspond to the heap of blocks (the commitment).

60 Continuing the analogy above, consider three Lego cars and their corresponding heaps of bricks (commitments). In the same way that the three cars can be combined to make a transformer, the three heaps of bricks can be combined to make a larger heap that corresponds to the commitment of that transformer.

one meter in the pair adds the secret value to its actual value, and the other subtracts it (thus, in a group of 10 meters, each submitted reading has had nine secret values added to or subtracted from it). Taking the sum of these submitted readings will generate the actual total reading for the aggregation group, as each secret value is cancelled out (added once, subtracted once). The researchers note that for privacy, these secrets should be changed after readings; this can, however, be accomplished with minimal computational overhead. The major benefit to this approach is the lack of public key cryptography required, which minimizes computation and does not change message size. It is, however, a less flexible protocol, as should one meter not function, the computation on the aggregate group will be inaccurate, and the aggregation group is fixed by the keys stored by the meters.

To show the practicality of these protocols, the researchers have implemented them on production meters from Elster SG. The computation overhead of the masking process was found to be far below one second, which does not create latency issues for even frequent (every 15 minutes, for instance) readings of smart meters.

As a key point, the researchers note that smart meter aggregation is of significant benefit to Smart Grid operators, as well. When readings are aggregated in the manner described, the frequency of readings no longer has an effect on the level of consumer privacy – aggregate minute-by-minute energy readings become no more invasive than day-by-day readings. Thus, the utility is able to collect energy usage data at a higher level of granularity without sacrificing consumer privacy. The utility could also make the readings themselves richer – collecting, for instance, energy usage by air conditioners, refrigerators, laundry systems, etc., individually. Again, aggregation here allows for this richness of data without revealing information about an individual user. The work of these researchers is, then, a defining example of the "positive-sum paradigm" – in which user privacy is *enhanced* at the same time that Smart Grid operators *gain* functionality (via increased collection of unidentifiable data).

Case Study 3: Alliander's Data Privacy and Security Certification Project

As a complementary measure to incorporating *PbD*, Alliander obtained a Data Privacy and Security certification in February 2011 after a two-year process. Alliander is the first distribution grid operator to obtain this kind of certification in Europe. In 2009, there was public concern over privacy and smart meters which led the Dutch Minister of Economic Affairs to suspend smart meter deployment. Since then, smart meters have only been introduced for those clients who request it. The certification process involved a €2 million investment in which Alliander worked with PriceWaterhouseCoopers, an auditing company, and Accenture, an IT services provider. Over 300 criteria were identified for completion as part of the certification process spanning four control areas: technology, procedures, organization, and policy.

Technology controls were applied to: M-bus devices, smart meters, data concentrators, communication networks, and central systems. These controls included wireless encryption, device pairing, detection of tampering, activity logs, firewalls, etc. Procedural controls were applied to: technology, contract management, the roll-out of smart meters, and the operation of smart meters. Procedural controls

included: registration for the permission to collect data, key encryption updating, processes for incident management, information management system reports, and access and correction of consumer data. Organizational controls were applied to the role of the data privacy owner, the privacy officer, and the information security manager. In addition, roles and responsibilities were outlined for employees. Policy controls were created, such as privacy and security guidelines, which were approved by management.

An audit performed in 2010 highlighted a few outstanding items before Alliander could receive its certification. The first related to notification and communication to customers about the collection of data from smart meters. As a result, Alliander sent 46,000 letters over a two-week period and placed 327 phone calls to customers. In reply, only two clients refused to have smart meters installed. The second issue related to security intrusion tests which revealed that a subset of smart meters were more vulnerable than others. As a result, Alliander disabled their communication function and planned to replace those meters.

Following the wrap-up of these final outstanding items, and after a final auditing and assessment of privacy readiness, Alliander was awarded its certification. Although Alliander has achieved this designation, it must continually manage its privacy and security processes. As such, Alliander has created an Information Security & Privacy Management System (ISPMS) which tracks tasks, due dates, mitigations, monitoring, reporting requirements, follow-ups, etc.

Conclusion

The importance of maintaining consumer trust and confidence with respect to privacy concerns is exemplified in the Netherlands' experience with smart metering. In 2006, a bill proposing the mandatory roll-out of smart meters was introduced in the Dutch Parliament. Although the bill was adopted in the lower chamber, privacy concerns raised by Consumentenbond (a Dutch Consumers' Organization) contributed to its rejection in the upper chamber. A report commissioned by Consumentenbond concluded that there were several privacy issues with the bill, and suggested that the bill might have violated Article 8, respect for one's private and family life, of the European Convention on Human Rights.61 Paul van Engelen, senior manager at PriceWaterhouseCoopers noted that in the Netherlands:

"[T]he privacy discussion had a major impact on the smart meter rollout. Currently there are around 300,000 meters in pilot programs in the field but we could have had a million or more in place by now if privacy had not been an issue. Since the privacy concerns became apparent Dutch grid companies have taken initiatives to develop data privacy and protection policies, a code of conduct and have started open discussions with different stakeholders. If these initiatives had taken place from the inception of the law back in 2005, there would have been a good chance of avoiding the legislative setbacks."[62]

61 Cuijpers, C., Koops, B.-J., Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 EVRM, Online: http://www.consumentenbond.nl/morello-bestanden/209547/onderzoek_UvT_slimme_energi1.pdf. See also Cuijpers, C., "No to mandatory smart metering does not equal privacy!" Online: http://vortex.uvt.nl/TILTblog/?p=54

62 PriceWaterhouseCoopers, "Smart from the start: Managing smart grid programmes," http://download.pwc.com/ie/pubs/smart_from_start.pdf

Smart meters, and the Smart Grid, are an excellent case study for the application of *Privacy by* Design to a networked technology. They are at a nascent stage, allowing privacy to be built into new technologies, but are being integrated into a legacy system that may require an appeal to *Privacy by ReDesign*. This network has a wide variety of players, spanning multiple industries and jurisdictions. As such, regulation and technical measures associated with this system cannot be defined or enacted by any single provider or jurisdiction – a collaborative effort is required. There are clear privacy implications for individuals, who may have sensitive lifestyle information divulged or inferred without their knowledge. Finally, there is also a very clear need for, and benefits associated with, this advance, providing a strong driving force for deployment that can, as has been seen, be derailed by improper, or lacking, considerations for individual privacy. "Getting it right" will thus be important not just to ensure the future success of the Smart Grid, but also to provide a strong template for the ever-increasingly networked world in which we live.

APPENDIX A – Overview of European Smart Grid Strategy and Framework Initiatives

In the past decade, there have been numerous Smart Grid strategy and framework initiatives developed by a broad range of groups in Europe. Here we describe the genesis and outcomes of a number of initiatives intended to be applicable across Europe.

During the first International Conference on the Integration of Renewable Energy Sources and Distributed Energy Sources in December 2004, industrial stakeholders and the research community suggested the creation of a **European Technology Platform for the Electrical Networks of the Future** (ETP SmartGrids). The concept, initially developed by the **European Commission Directorate General for Research**, aimed to formulate and promote a vision for the development of European electricity networks in 2020 and beyond. The ETP SmartGrids group published a **Strategic Research Agenda for Europe's Electricity Networks of the Future** in 2007, and the **Strategic Deployment Document for Europe's Electricity** in April 2010.

Directive 2006/32/EC on energy end-use efficiency and energy services established targets, incentives, and the financial and legal frameworks needed to eliminate market barriers to the efficient end-use of energy. It also created the conditions for the development and promotion of a market for the delivery of energy saving programs. Specifically, member states were required to adopt and achieve an indicative energy saving target of nine per cent by 2016 in the framework of a National Energy Efficiency Action Plan (NEEAP).

A key move forward for smart metering in the EU occurred in August 2009, when the European Union published **Directive 2009/72/EC (of the Third Legislative Package),** which provides that in order to promote energy efficiency, Member States will ensure the implementation of "intelligent metering systems" to assist active consumer participation in the electricity supply market. In this directive, Member States are required to undertake an economic assessment of smart metering by September 3, 2012 and, subject to its results, ensure that at least 80 per cent of consumers are equipped with intelligent metering systems by 2020.

On March 12, 2009, the **European Commission** issued **Standardization Mandate M/441,** in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability for smart meters and Advanced Metering Infrastructure.

The **European Regulators Group for Electricity and Gas** (ERGEG) was established in 2003 by the European Commission to act as an advisory group on internal energy market issues, and comprises the energy regulatory authorities of the EU. They have also been active in considering the regulatory aspects of the Smart Grid, beginning with a **Status Review on Regulatory Aspects of Smart Metering** in 2009, continuing with public consultation on a **Position Paper on Smart Grids** published in December 2009, and a public consultation resulting in a final set of **Guidelines of Good Practice on Regulatory Aspects of Smart Metering.** Recommendations and guidelines developed by this group are directed at Member States, national regulatory authorities and industry. The work of ERGEG will support and complement the work of a new EU **Agency for the Cooperation of Energy Regulators**

(ACER), which became operational in March 2011, and whose mission is to assist, and where required coordinate, national regulatory agencies in exercising their tasks in EU Member States.

Also in 2009, the European Commission set up a **Smart Grids Task Force**. Similar to some others, the goal of this task force was to "identify and produce a set of regulatory recommendations to ensure EU-wide consistent, cost-effective, efficient and fair implementation of Smart Grids, while achieving the expected Smart Grids' services and benefits for the network users." This Task Force was divided into three **Expert Groups** (EGs), to jointly develop a common vision on Smart Grids: EG1, focussed on the functionality of the Smart Grid and smart meters; EG2, focussed on privacy, security, and data safety; and EG3, focussed on the roles and responsibilities of the various actors. Importantly for this paper, EG2 released its **Regulatory Recommendations for Data Safety, Data Handling and Data Protection** on Feb. 16, 2011.

In May 2010, the European Network of Transmission System Operators for Electricity (ENTSO-E), the European Distribution System Operators for Smart Grids (EDSO-SG), ERGEG and the European Commission, among other stakeholders, released the **European Electricity Grid Initiative (EEGI) Roadmap 2010-18 and Implementation Plan 2010-12.** This research, development, and demonstration program focuses on system innovation, rather than on technological innovation, addressing the challenge of integrating new technologies under real-life working conditions.

Smart Grid standards work in Europe remains ongoing: in April 2011, the **European Commission** released a Communication for the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, titled "**Smart Grids: from innovation to deployment.**" In it, five challenges for the deployment of the Smart Grid were identified, along with suggested actions. Also that month, the **Article 29 Data Protection Working Party** released its "**Opinion 12/2011 on smart metering**," which provides interpretations of how smart metering information will relate to European data protection laws.

Finally, at its 50th meeting (September 12-13, 2011, in Berlin, Germany), the **International Working Group on Data Protection in Telecommunications** (IWGDPT) adopted a working paper titled "*Privacy by Design* and Smart Metering: Minimize Personal Information to Maintain Privacy." This paper, which is expanded upon in the current paper, laid out a set of recommendations for ensuring that privacy was built into both the technologies and regulatory frameworks associated with the Smart Grid.

APPENDIX B – The Electrical System in Germany

According to an Internal Market Fact Sheet (Jan 2007) German electricity and gas markets were fully opened to competition in 1998. Germany's market may be characterized as being dominated by a few large companies and is the biggest in continental Europe on the basis of generation capacity, with an annual power consumption about 550 TWh and generation capacity of 125 GW, half of which is coal fired, 17 per cent nuclear, and 18 per cent gas fired (Analyticalq – Anne Ku March 2001). There is no independent system operator or regulator – rather there are six transmission system operators and several hundred distribution network operators acting in the spirit of cooperation and self-regulation. Germany is also considered the largest electricity market in continental Europe by number of players and generation capacity (Anne Ku, March 2001).

The Federal Network Agency (or *Bundesnetzagentur*) and provincial authorities (or *Landesregulierungsbehörden*) are responsible for regulating electricity and gas utilities in Germany. The Federal Network Agency's central purpose is to establish fair and effective competition in the supply of electricity and gas, and include ensuring non-discriminatory third-party access to networks and monitoring the use-of-system charges levied by market players. Provincial regulators have jurisdiction over power supply companies with fewer than 100,000 customers connected to their electricity or gas networks whose grids do not extend beyond a federal state's borders, and are responsible for monitoring consumer energy pricing.

According to a recent report entitled European Smart Metering Landscape Report (Vienna Feb 2011) that classified Member States into five groups (dynamic movers, market drivers, ambiguous movers, the waverers and lastly, the laggards), Germany was classified under "market drivers." This category is labeled as such because there is no legal requirement for a roll-out of smart meters. Generally speaking, Distribution Service Operators (DSOs) are going ahead because of customer demand or internal synergetic effects. (Vattenfall is a Swedish company operating in Germany – Sweden is considered a dynamic mover where smart meter roll-out is mandatory or pilots are already underway.)

In April, 2010 the DKE put out a roadmap for Germany's e-energy technology program and Smart Grid initiatives, which was promoted by the Federal Ministry of Economics and Technology in cooperation with the Federal Ministry of the Environment, Nature Conservation and Nuclear Safety. The purpose of the initiative was to draft a strategic technically-oriented road map of the standardization requirements for Germany's Smart Grid vision (DKE report). Besides identifying key areas for standards work, the roadmap also signifies the importance of security and privacy (SG-SD-1 Importance of privacy and data protection) for the implementation of the Smart Grid concepts and for acceptance by users, the protective objectives of availability, reliability, integrity and confidentiality are to be taken into account in the technical concepts and operation. The contacts for these issues are the privacy and data protection representatives of the federal states, the BSI and national and international standardization organizations (IEC, DKE, DIN) with active assistance from the relevant associations (BITKOM, VDE/ITG). In this connection, conceivable conflicts between objectives of data protection with the demand for data thrift on the one hand, and the Smart Grid approach with extended network management and the involvement of consumers by means of incentive-oriented load management systems on the other hand, are to be resolved.

Marek Jawurek and Martin Johns have also detailed the security challenges associated with the German Smart Grid deployment.[63] They identify five areas which can give rise to such challenges: more communication relationships with heterogeneous partners; interfaces where no interfaces existed before; new communications paradigms; high amounts of privacy-related data; and, an overarching architecture. They conclude, similar to this paper, that "now is the time to ensure a secure and private future of energy supply."

63 Jawurek, M., and Johns, M. (2010) Security Challenges of a Changing Energy Landscape. In Securing Electronic Business Processes, Pohlmann, N., Reimer, H., and Schneider, W. (eds). Online: http://www.e-ikt.de/binary.ashx/~default.download/430/security-challenges-of-a-changing-energy-landscape.pdf

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

April 2012

http://www.privacybydesign.ca