Smart metering, smart grid and privacy by design

Project E-Cube

Marco Berliri, Partner, Hogan Lovells (Rome)
Winston Maxwell, Partner, Hogan Lovells (Paris)

September 21, 2010

Hosted by Telecom Italia
Smart Meters, Grids and Privacy by Design ("PbD")

- Smart meters and grids
- Privacy by Design
  - Proactive not Reactive; Preventative not Remedial
  - Privacy as the Default
  - Privacy Embedded into Design
  - Full Functionality: Positive-Sum, not Zero-Sum
  - End-to-End Lifecycle Protection
  - Visibility and Transparency
  - Respect for User Privacy
Smart Meters, Grids and Privacy by Design ("PbD")

- Conclusions of European Expert Group 2 (June 22, 2010):
  - "from the beginning, legislation on privacy and data protection must be taken into account as important requirements in the design of smart metering systems"
  - "ESOs...should mandate that smart grid products and solutions should be designed from the start with appropriate levels of data privacy and security at their core."
  - "Security is a path, not a destination!"
  - "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."
Smart Grids and Privacy in France

- **Article 18 of the law n°2009-967** to the implementation of the Grenelle Environment Project dated August 3, 2009

- **Deliberation of the French Data Protection Authority**, the CNIL dated August 5, 2010

- Creation of a **task force** composed of the CNIL, and the Commission de Régulation de l'Energie (the CRE). A recommandation is supposed to be provided to the French Government by 2011/2012
Smart Grids and Privacy in Italy

➢ Legislative and regulatory initiatives

- Law Decree No. 73 of 2007
  - Art. 1: immediate and non discriminatory access to customers consumption data to "make commercial offers and manage the contract"

- Deliberation of July 25 2007 of the Italian DPA
  - specific guidelines concerning processing of data subjects' personal data in the energy and gas market
  - Need for personal consent for marketing initiatives
  - Privacy policy (also through the internet)
Smart Grids in Italy: practical examples

➤ Practical Examples

– Diffusion of advanced metering systems
  • ENEL Telegestore Project: over 30 million devices installed

– Smart Grid projects
  • Milano Wi Power Project
  • Google Power Meter
  • E-Cube
SMART GRIDS: EU Initiatives

- **Key Findings of EC Smart Grid Task Force EG2**
  - Mission: "the key deliverable is to identify the appropriate regulatory scenario and recommendations for data handling, safety and consumer protection"
  - Benchmark using other industry experience (banking, telecom, road pricing)
  - Address security & privacy at design stage
  - Consider security features developed out of identified threats in Telecom
  - Data aggregation and anonymization will be essential

- Dutch framework, and "Payment Card Industry Data Security Standard" (PCI-DSS) as possible examples to follow
SMART GRIDS: EU Initiatives

- Key Findings of EC Smart Grid Task Force EG2
  - Differentiate between "technical data" and "personal data":
    - "consumer data is considered as specific data and can be traced back to the individual consumer whereas technical data is aggregated and anonymous and does not contain explicit references to persons or individual metering points"

- Organisational safeguards
  - "To ensure data safety and security within an intelligent network a clear division of roles and responsibilities regarding ownership, possession and access to data, read and change rights, etc. has to be defined"
SMART GRIDS: EU Initiatives

- Key Findings of EC Smart Grid Task Force EG2
SMART GRIDS: EU Initiatives

 Key Findings of EC Smart Grid Task Force EG2

The smooth operation of an intelligent network requires a clear division of roles and responsibilities - the central question to assess the risk especially for private consumer data is: Which data is used by whom and for what purpose?
Definition of personal data within the meaning of the 95/46/EC Directive
- 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;

Possibility to aggregate or anonymize data in order to avoid the personal data regulation

e-Privacy directive (2002/58/EC) applies to "traffic data" and "location data"

2006 data retention directive (2006/24/EC - for law enforcement) may also apply
Personal Data Regulation (and implementation laws such as Italian Law 196 of 2003 and French law 78-17 of 1978)

➤ Data protection general principles:

• Collection of relevant and proportionate data only
• Clear and complete information of data subjects
• Notification/Authorization of the data processing with the local DPA
• Right of access/modification/removal of data
• Consent of data subjects prior to any disclosure of their personal data to any third party
• Term of storage of data
Remainder of key European principles (cont'd)

➤ Collection of Relevant and Proportionate Data Only:

- Specifically, personal data undergoing processing needs to be relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed;

- As a consequence, data subjects' need to grant specific consent in advance to allow for their data to be used for other processing activities not falling within the above description (and in particular processing for marketing purposes).
Reminder of key European principles (cont'd)

➢ **Clear and Complete Information of Data Subjects:**
  
  • **Privacy information notice to data subject:** as a general rule, each person to whom the data collected and processed relate to must be provided in advance with a specific privacy information notice through which, among others, he/she is informed about the following:
    
    – Nature of the data collected;
    – Purposes of the processing;
    – Categories of persons who have accessed the data and the persons/entities to which the data will be communicated;
    – The rights to access, update and oppose to the processing.
Italian notification requirements

➢ Notification/Authorization of the Data Processing with the DPA:

• **Notification to the Italian DPA:** According to the Privacy Code, the notification to the Italian DPA is required only in certain cases specified in article 37. Among these cases, the notification is mandatory when the "data [are] processed with the help of electronic means aimed at profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users".

• **It is necessary to determine whether the data processing activities performed:**
  – allow the data controller to analyse and monitor the consumption patterns of consumers in order to profile them (even only for statistic purposes) for purposes different from the execution of the service provided; or
  – is only aimed at executing the service.
Key European data protection principles (cont'd)

- **Data Subjects' right of Access/Modification/Removal of Data:**
  - Data subjects are entitled to exercise the above rights by making a request to the data controller or processor without formalities, also by the agency of a person in charge of the processing.
  - A suitable response shall be provided to said request without delay, and without unreasonable cost.
Reminder of key European principles (cont'd)

- **Consent of data subjects prior to any disclosure of their personal data to any third party:**
  - Data controllers need not obtain the consent of data users with regard to data usage necessary for the fulfilment of ordinary contractual obligations and regular business activity.
  
  Therefore, data subjects need to grant specific consent in advance to allow for their data to be used for other processing activities not falling within the data controller's ordinary obligations (which generally excludes data processing for marketing purposes) vis-à-vis the data users.

- **Term of Storage of Data:**
  - Kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.
Preliminary considerations

1. The difficulty of assessing who the data controller is:

   - Definition of the 95/46/EC Directive: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (…)
   - Privacy issues arising from the question of the legal ownership of the data being collected → with ownership comes both control and rights with regard to data usage.
   - In the case at hand, the utility or the energy providers?

2. The difficulty of assessing who the recipient of the data should be:

   - Who should be an authorized recipient:
     - The utility companies?
     - The energy providers?
     - Competitors?
     - Insurance companies?
   - Unauthorized recipients who might try to access the data:
     - lawyers in divorce cases
     - burglars
Specific privacy issues in connection with Project E-Cube

➢ Security of Data:
  • the Privacy Code sets out certain minimum security measures which data controller must implement in order to avoid any unauthorized access to the data, loss or deletion (even accidental) of it, utilization of the data for different unlawful purposes.
  • Main measures requested:
    – one or more authentication processes for electronic database such as an ID code associated with a secret password that must only be known by the person in charge of the processing;
    – antivirus aimed at protecting the system annually updated (every six months in case of sensitive data processing);
    – specific instructions in writing to the persons in charge of the data processing.

➢ Transfer of Personal Data Outside the EU:
  • data transfer (temporary or permanent, in any form and by any means) of personal data to non-EU countries which do not guarantee an adequate level of data protection (i.e. the US), is allowed only upon granting of a specific consent by data subjects or when certain exceptions occur, such as when the transfer is necessary for the performance of contractual obligations or for the fulfillment of legal duties.
Key developments in the U.S. relating to privacy and smart grids
Structure of the Smart Grid US legislation

- Federal laws: Energy Independence and Security Act (EISA) 2007
  - American Recovery and Reinvestment Act (ARRA) 2009

- Federal regulators: FCC, FERC, FTC, NIST

- State laws: e.g. California law: SB17, October 11, 2009

- State PUCs: e.g. Cal CPUC, December 29, 2009

- Tension between allowing access by third party service providers ("innovation at the edge") and ensuring end-to-end security and privacy
1. Secure wireless communications for Smart Grid –
   3 options:
   • Using existing network, e.g. wifi, mobile.
   • Dedicating spectrum to Smart Grid (e.g. 700MHz public safety)
   • Limiting use of wireless / public internet to mitigate privacy and security risks

2. Sharing of information with third parties
   • Heavy emphasis on promoting third party innovation "at the edges"
   • States must develop reasonable policies over the next 18 months; otherwise, Congress should consider national legislation to cover consumer privacy and the accessibility of energy data
The NIST: Guidelines of Smart Grid Cyber Security - August 2010

• 3 volumes:
  – Smart Grid Cyber Security Strategy, Architecture and High Level requirements
  – Privacy and Smart Grid
  – Supportive analysis and references

• The 4 dimensions of privacy:
  – Privacy of personal information: "any information relating to an individual, who can be identified directly or indirectly by that information"
  – Privacy of the person: "the right to control the integrity of one's own body"
  – Privacy of personal behavior: "right of any individuals to keep any knowledge of their activities, and their choices, from being shared with others"
  – Privacy of personal communications: "right to communicate without undue surveillance, monitoring, or censorship"
Generally, most data protection laws and regulations apply only to data covered by the first and fourth dimensions (privacy laws, and rules on electronic communications).

However, the two other dimensions are important privacy considerations too, and should be considered by Smart Grid entities, e.g.

- The Nonintrusive Appliance Load Monitoring (NALM) techniques
- The NALM results identified in the graph below reflect intimate details of people's lives and their habits and preferences inside their homes.

  The Supreme Court highlights the issue that new technologies allow government to see into suspects' home without actually entering into the premises. The use of these technologies constitutes a "search" and is "presumptively unreasonable without a warrant"
Power Usage to Personal Activity Mapping
(extract from NIST 7628 "Guidelines for Smart Grid Cyber Security" v.1.0 - Vol.2 – August 2010)

Peak = 7.18 kW
Mean = 0.49 kW
Daily load factor = 0.07
Energy consumption = 11.8 kWh
PII v. Personal Data?

- The concept of Personally Identifiable Information (PII), commonly used in the US, is narrower than the European concept of "Personal Data"
- However, there is recognition in the US that PII is too narrow.
  - "The energy use pattern could be considered unique to a household or premises similar to how a fingerprint or DNA is unique to an individual"
  - Convergence between EU and US approach (cf. EG2 conclusions)
- Convergence as well regarding the limits of consent
The Consumer-to-utility privacy impact assessment (PIA)

- The NIST has implemented a comprehensive process for determining the privacy, confidentiality, and security risks associated with the collection, use and disclosure of personal information in order to mitigate, or if possible erase, the identified risks.
- This PIA identifies several domains as specific privacy related topics which are mostly based on OECD and EU existing principles.
PIA for consumer to utility communications: NIST Recommendations:

1. **Conduct a initial PIA** before making the decision to deploy and/or participate in the Smart Grid to identify risks to the personal information and establish a baseline privacy posture measurement.

2. **Conduct subsequent PIAs** when (i) major changes occur within the organization, systems, or applications, (ii) new laws and regulations are put into effect, and (iii) at any other time an event occurs that impacts how the Smart Grid entity does business.

3. **Draft and implement a clear and complete set of privacy policies** recalling the following principles:
   - Management and Accountability
   - Notice and Purpose
   - Choice and Consent
   - Collection and Scope
   - Use and Retention
   - Individual Access
   - Disclosure and Limiting Use
   - Security and Safeguards
4. **Develop a comprehensive set of privacy use cases** that will help utilities and third-party Smart Grid providers to rigorously track data flows and the privacy implications of collecting and using data, and help the organization to address and mitigate the associated privacy risks within common technical design and business practices.

5. **Educate the public** about the privacy risks within the Smart Grid and what they as consumers can do to mitigate them

6. **Share information concerning solutions** to common privacy-related problems with other Smart Grid market participants

7. Manufacture and sell smart meters, smart appliances, and other types of smart devices **which collect only the energy and personal data necessary for the purposes of the smart device operations**
NIST "privacy use cases"

- landlord and tenant scenario
- PEV (plug-in vehicle) general registration and enrollment process

• What is the difference between a PIA and a privacy use case?
Case study: comparison between ZigBee and Open ADR (case study prepared by CDT, Dec. 1, 2009)

• The ZigBee/HomePlug Smart Energy Profile:

  – A ZigBee Smart Energy network consists of (i) an Energy Service portal (ESP), (ii) Metering Device, (iii) Programmable Communicating Thermostat (PCT), and (iv) Smart Appliance Device
  – The ESP communicates with customers' devices via encrypted wireless communication
  – The system permits the utility company to communicate directly with household devices (eg. utility company instructs the water heater to reduce load by 10%)

• End-to-end security is engineered into the system, but utility company collects granular use information
OPEN ADR case study

• Under Open ADR, the communication between the utility and the consumer goes through the Demand Response Automation Server (DRAS).
  – This DRAS may be a standalone third-party service, or integrated with the utility, or with the consumer's information system. The DRAS "client" may be located on the consumer's premises. The DRAS client acts as a shield between the utility and detailed usage data. There is no direct interaction between customers' HAN devices and utilities.

• All public communication interfaces are subject to confidentiality, authentication, and non-repudiation requirements

• Utility will send general instructions ("reduce load by 10%") and DRAS client will manage how that instruction is carried out by devices within the house
  – Far less information about customers' devices are collected by the utility under Open ADR than under ZigBee Smart Energy Profile

• Open ADR also offers an opt-out functionality if offered to customers who want to opt-out of a demand response program
The California Public Utilities Commission (CPUC)

- **December 29, 2009**: CPUC's decision re sharing of usage data
  - by end 2010: customers and authorized third parties should have access to electricity pricing information and to usage data collected by utilities via backhaul
  - by end 2011: customers and authorized third parties should have access to usage data on a near real time basis
- **June 24, 2010**: CPUC requires major utilities to submit smart grid deployment plans that incorporate:
  - baseline privacy assessment: how information is treated now
  - forward-looking privacy assessment, responding to nine questions regarding how information will be treated in future smart grid deployment
- **Before end 2010**: CPUC will issue privacy rules before utilities are required to share information with third parties
  - Problem of regulatory jurisdiction over other players (eg. Microsoft, Google)
Conclusions

- Privacy by design is an opportunity for smart grids rather than a threat
- Customers' perception of privacy is quickly changing: the statutory provisions could not be enough
  - Competitive advantage for who offers more privacy protection
- Need to implement a preventive, not remedial approach
- Role of utilities manufacturers: Privacy *Embedded* into Design
- Visibility and Transparency
  - Provision of privacy policy and collection of consent
  - Internet
- Role of the Service Provider
Thank you

Marco Berliri
marco.berliri@hoganlovells.com
+39 06 675 82 31

Winston Maxwell
winston.maxwell@hoganlovells.com
+33 1 53 67 48 47
**Hogan Lovells has offices in:**

<table>
<thead>
<tr>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abu Dhabi</td>
<td>Caracas</td>
<td>Hong Kong</td>
<td>Munich</td>
<td>Shanghai</td>
<td>Silicon Valley</td>
<td></td>
</tr>
<tr>
<td>Alicante</td>
<td>Colorado Springs</td>
<td>Houston</td>
<td>New York</td>
<td>Singapore</td>
<td>Tokyo</td>
<td></td>
</tr>
<tr>
<td>Amsterdam</td>
<td>Denver</td>
<td>Jeddah*</td>
<td>Northern Virginia</td>
<td>Riyadh*</td>
<td>Tokyo</td>
<td></td>
</tr>
<tr>
<td>Baltimore</td>
<td>Dubai</td>
<td>London</td>
<td>Paris</td>
<td>Ulaanbaatar*</td>
<td>Warsaw</td>
<td></td>
</tr>
<tr>
<td>Beijing</td>
<td>Dusseldorf</td>
<td>Los Angeles</td>
<td>Philadelphia</td>
<td>Washington DC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Berlin</td>
<td>Frankfurt</td>
<td>Madrid</td>
<td>Prague</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boulder</td>
<td>Hamburg</td>
<td>Miami</td>
<td>Riyadh*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brussels</td>
<td>Hanoi</td>
<td>Milan</td>
<td>Rome</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Budapest*</td>
<td>Ho Chi Minh City</td>
<td>Moscow</td>
<td>San Francisco</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Zagreb*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Hogan Lovells* or the "firm" refers to the international legal practice comprising Hogan Lovells International LLP, Hogan Lovells US LLP, Hogan Lovells Worldwide Group (a Swiss Verein), and their affiliated businesses, each of which is a separate legal entity. Hogan Lovells International LLP is a limited liability partnership registered in England and Wales with registered number OC323639. Registered office and principal place of business: Atlantic House, Holborn Viaduct, London EC1A 2FG. Hogan Lovells US LLP is a limited liability partnership registered in the District of Columbia.

The word "partner" is used to refer to a member of Hogan Lovells International LLP or a partner of Hogan Lovells US LLP, or an employee or consultant with equivalent standing and qualifications, and to a partner, member, employee or consultant in any of their affiliated businesses who has equivalent standing. Rankings and quotes from legal directories and other sources may refer to the former firms of Hogan & Hartson LLP and Lovells LLP. Where case studies are included, results achieved do not guarantee similar outcomes for other clients. New York State Notice: Attorney Advertising.

© Hogan Lovells 2010. All rights reserved.

* Associated offices