

NIST Smart Grid High Level Consumer-to-Utility Privacy Impact Assessment

**Prepared by Rebecca Herold, Christophe Veltsos & Ward Pyles
For use by the NIST CSWG Smart Group Privacy Group**

September 10, 2009

Table of Contents

High-Level Smart Grid Consumer-to-Utility PIA Report3
A. Summary of PIA Findings 3
B. Purpose of a High-Level PIA 3
C. NIST Smart Grid Description..... 5
D. GAPP Alignment..... 9
E. Regulatory and Legal Compliance.....16

High-Level Smart Grid Consumer-to-Utility PIA Report

NIST enlisted the input of a wide range of industry, information security and privacy experts to review the plans for the Smart Grid systems. With the extremely limited time and resources available to this group the assessment was not able to perform deep review of all possible information exchanges. However, even with limited resources, this high-level assessment revealed many significant privacy concerns and issues.

This PIA examines the privacy implications and related information security safeguards within the planned U.S. Smart Grid system, in particular the issues involved with the consumer-to-utility data items collected and how they are used. This analysis was performed in accordance with numerous U.S. federal data protection requirements, and the OECD privacy principles as outlined within the AICPA Generally Accepted Privacy Principles (GAPP), U.S. Federal Trade Commission Fair Information Practices (FIPs), in addition to incorporating the safeguard concepts from ISO/IEC 27002.

The scope of this PIA included review of available documentation and information obtained from a variety of utilities industry contacts and experts.

A. Summary of PIA Findings

The results of a high-level privacy impact assessment (PIA) of the consumer-to-utility metering data sharing portion of the Smart Grid reveal that there are significant areas of concern that must be addressed within each localized section of the Smart Grid.

While some states have examined the privacy implications of the Smart Grid, most states do not have any documentation available that demonstrates this analysis. Research revealed there are currently no formal privacy policies or standards that have been implemented by each state utility commission. None of the individual utilities contacted have documented or implemented any privacy policies, standards or procedures for the data collected throughout the Smart Grid. A comprehensive and consistent definition of “personally identifiable information” (PII) does not exist at any of the state utility commissions, at FERC, or within the utility industry.

Lack of consistent and comprehensive privacy policies, standards and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a very significant privacy risk that must be addressed.

B. Purpose of a High-Level PIA

This document summarizes the results of a high-level PIA, performed during August of 2009, of the consumer-to-utilities component of the planned Smart Grid systems. The PIA goals were to determine if the risks to personally identifiable information (PII) and associated privacy issues are mitigated appropriately and that PII data is not inaccurate

or out-of-date, excessive or used in unacceptable or unexpected ways beyond the control of data subjects.

The documentation for the consumer-to-utilities smart meter technology and data gathering and use practices were reviewed against the following international generally accepted privacy principles (GAPP), which form the basis of most international, national and local data protection laws, along with consideration of safeguards as found in the international information security standard ISO/IEC 27001, also widely used for data protection regulatory compliance:

1. **Management & Accountability:** An organization must formally appoint someone to ensure that information security and privacy policies and practices exist and are followed. Documented requirements for regular training and ongoing awareness activities must exist and be followed. Audit functions must be present to monitor all data accesses and modifications.
2. **Notice & Purpose:** There must be a clearly specified notice describing the purpose for the collection, use, retention, and sharing of PII. Data subjects should be told this information at or before the time of collection.
3. **Choice & Consent:** The organization must describe the choices available to individuals and obtain explicit consent if possible, or implied consent when this is not feasible, with respect to the collection, use and disclosure of their PII.
4. **Collection & Scope:** Only PII that is required to fulfill the stated purpose should be collected from individuals. Treatment of the information must conform to fair information processing practices. Information must be collected directly from each individual person unless there are very good reasons why this is not possible.
5. **Use & Retention:** Information should only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorized to receive it. PII should be aggregated or anonymized wherever possible to limit the potential for computer matching of records. PII should only be kept as long as is necessary to fulfill the purposes for which it was collected.
6. **Individual Access:** Organizations should provide a process for PII data subjects to allow them to ask to see their corresponding PII and to request the correction of perceived inaccuracies. PII data subjects must also be informed about parties with whom PII has been shared.
7. **Disclosure & Limiting Use:** PII should be used only for the purposes for which it was collected. PII should not be disclosed to any other parties except for those identified in the notice, or with the explicit consent of the individual.
8. **Security and Safeguards:** PII, in all forms, must be protected from loss, theft and must prevent unauthorized access, disclosure, copying, use or modification.
9. **Accuracy & Quality:** Every effort must be made to ensure that the PII is accurate, complete and relevant for the purposes identified in the notice, and remains accurate throughout the life of the PII within the control of the organization.
10. **Openness, Monitoring & Challenging Compliance:** Privacy policies must be made available to PII data subjects. PII data subjects must be given the ability and

process to challenge an organization's compliance with their state privacy policies as well as their actual privacy practices.

C. NIST Smart Grid Description

Some of the goals of the planned U.S. smart grid will use digital technology to improve reliability, security, and efficiency of the nationwide electricity system from large generation power transmission, distribution, and management, through the delivery systems to electricity consumers and increasing numbers of distributed-generation and storage resources. As described in the July 2009 "Smart Grid System Report" from the U.S. Department of Energy¹:

"Areas of the electric system that cover the scope of a smart grid include the following:

- *the delivery infrastructure (e.g., transmission and distribution lines, transformers, switches),*
- *the end-use systems and related distributed-energy resources (e.g., building and factory loads, distributed generation, storage, electric vehicles),*
- *management of the generation and delivery infrastructure at the various levels of system coordination (e.g., transmission and distribution control centers, regional reliability coordination centers, national emergency response centers),*
- *the information networks themselves (e.g., remote measurement and control communications networks, inter- and intra-enterprise communications, public Internet), and*
- *the financial and regulatory environment that fuels investment and motivates decision makers to procure, implement, and maintain all aspects of the system (e.g., stock and bond markets, government incentives, regulated or non-regulated rate-of-return on investment)."*

As work progresses on the Smart Grid, privacy concerns continue to be raised as a result of discussions and speculation about how the data automatically collected from the smart meters, and distributed throughout the entire Smart Grid system, will be used.

The scope of this high-level PIA is the consumer meter to local utility (consumer-to-utility) data flow and associated privacy issues. However, before looking specifically at the consumer-to-utility issues, first consider the wide breadth, with associated significant depth, of information flow throughout the entire Smart Grid network. As Figure C.1 shows, the expanse is huge.

¹ Retrieved 08.27.09 from page iv at http://www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf

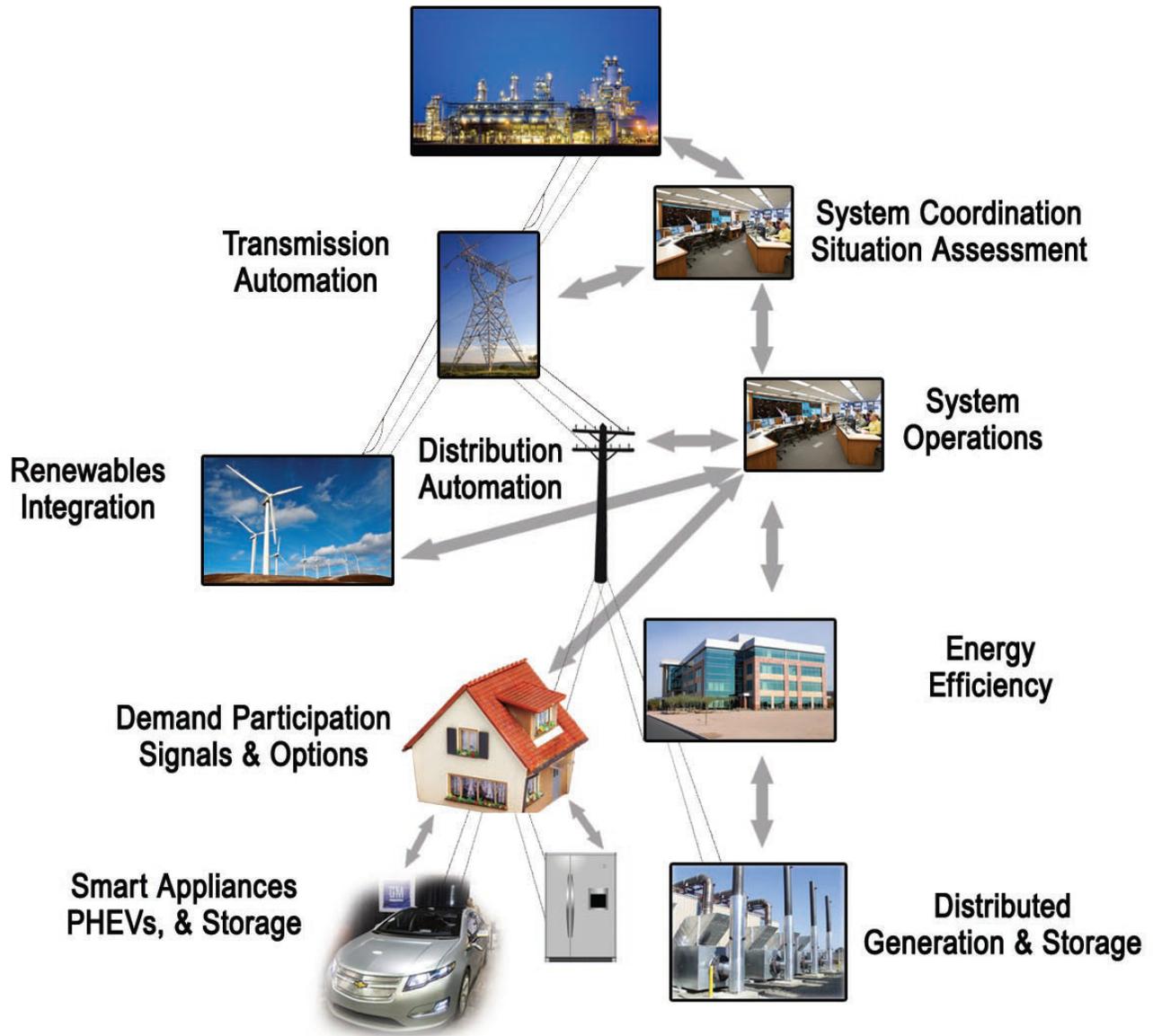


Figure C.1 The key information sharing components of the Smart Grid²

Data is, and will be, flowing between all these many components within the Smart Grid. Now let's drill down and consider types of data flows between utilities and home meters. The flow of data back and forth between utilities and residential meters will now be similar to the types of data flows between commercial meters and utilities. While the data flows are similar, as the diagram in Figure C.2 indicates, the specific data items involved, and the associated privacy issues, are very different. The data items collected from the Distributed Energy Resources (DERs) and smart meters will reveal much different types of information about residential consumers and activities within the house

² Retrieved 8/27/09 from page 2 at http://www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf.

than the information collected from commercial DERs and smart meters. The differences in potential impacts to individuals are significant.

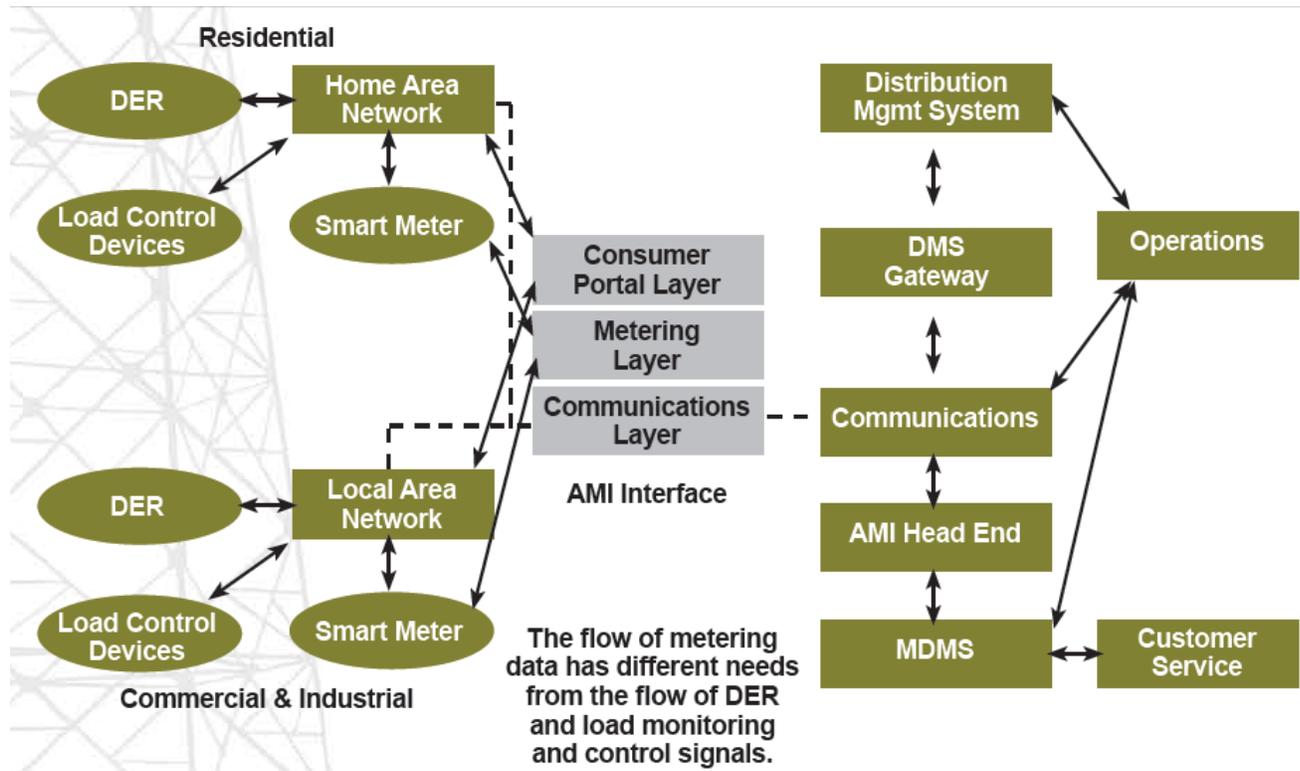


Figure C.2 – Data Flows of Residential and Commercial Meter Data³

Consumers will consider much of the information obtained from the home meters as personally identifiable information (PII). Many of the data items that are not individually considered as PII will form PII when grouped with one or more other data items. For example, Figure C.3 shows the power use within a home during specific times of the day. Just viewing the grid data alone within a centralized server would not directly reveal a specific individual or household. However, if this usage data were viewed or connected to a name, address or meter identifier, it would reveal the activities of a household; a significant privacy concern. As another example, the HAN devices could disclose specific device usage that would reveal information about a specific household.

The ability for smart grid devices to “roam” to other utility systems – for example, driving an electric vehicle (PEV) over to visit family and recharging it while there – implies that there will likely be additional flows of PII or derived PII data between the roaming devices and their “host” utility (such as the PEV id). In this example, the “host” utility would bill the PEV’s “home” utility for the PEV’s recharge.

^{3 3} Retrieved 8/27/09 from page 14 at http://www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf.

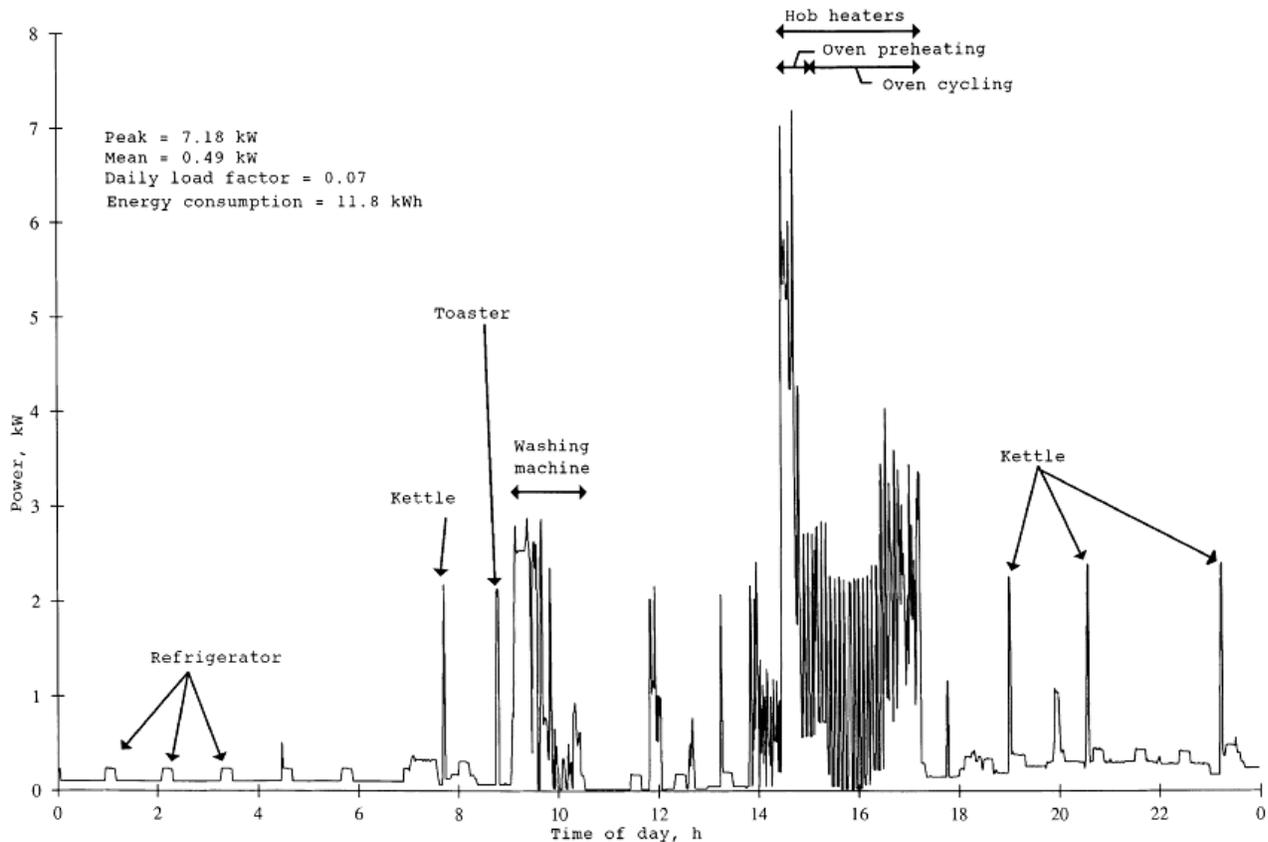


Figure C.3 – How power use can reveal personal activities⁴

From this point forward these grouped data items that can reveal insights into personal lives and activities are referenced as “derived PII.” How the data items are used, grouped, shared and maintained are key privacy concerns. Figure C.4 lists the types of data items that will be collected and shared between the home meters and the utility company. Specific types of PII data items are highlighted in green. Data items that can be combined with other data items to form derived PII are highlighted in yellow.

Data Item	Data Item Description
1. Resident Name	Primary resident name
2. Address	Address for residence
3. Meter Location	Number identifying specific residence location
4. Billing Number	Account number for the residence as assigned by the utility
5. Meter ID	Number identifying specific metering device
6. Electricity Profile	Electricity profile
7. Electricity Load	Smart meter data collected from a number of meters and collated

⁴ Elias Leake Quinn, *A Report for the Colorado Public Utilities Commission, Spring 2009*, pg. 3. (citing M. Newborough & P. 3Augood, *Demand-side Management Opportunities for the UK Domestic Sector*, IEEE Proceedings of Generation Transmission and Distribution 146 (3) (1999) 283–293).

Signal	into single electricity load signal for a specific geographic area.
8. Electricity Usage Preferences	Entered by the resident to automate such things as thermostat response to changing electricity prices, etc.
9. Smart Plug Technology	Usually a voltmeter that represents the usage of electric devices connected to it. But, this may have ability to control load through peak disconnect commands. Amounts of energy used by such plugs; e.g., can see who is using an electric or hybrid car, etc.
10. Timestamp	Specific times when automatic meter reads occurred.
11. Outage	Outage data
12. Voltage	Voltage data
13. Smart Appliance Data	Smart appliance data

Figure C.4 – Data Items within Smart Grid Home-to-Utility Processing

The remainder of this PIA will focus on the related issues of the specific and derived PII as they map to the internationally-recognized Generally Accepted Privacy Principles, which were built around the OECD privacy principles, the basis of most world-wide data protection laws and regulations.

D. GAPP Alignment

1. Management, Accountability & Training

From the brief amount of time available to do research, no formally documented privacy responsibilities exist for Smart Grid management positions, and no one position or person has been assigned responsibility for privacy oversight for the Smart Grid as a whole.

There should be regulations at best, and standards at least, that require a formal creation of a position dedicated to privacy protections throughout the Smart Grid. Such a position is necessary to privacy and associated information security policies and practices exist. Standards are defined to ensure the appropriate use of and access to PII and derived PII.

Documented requirements for regular privacy training and ongoing awareness activities for all utilities, vendors and other entities with management responsibilities throughout the Smart Grid should be created, implemented and compliance enforced. Audit functions must be present to monitor all data accesses and modifications.

Recommendations:

- 1.1 Establish an overall Smart Grid privacy policy that defines and articulates consumer privacy rights, PII definitions and derived PII definitions, privacy standards and suggested protection practices.
- 1.2 Formally establish a position with privacy oversight and standards enforcement authority for the Smart Grid.

- 1.3 Establish standards and policies to ensure all entities involved with implementing, maintaining and accessing consumer Smart Grid and meter data have regular training and ongoing awareness communications for information security and privacy responsibilities and related issues.
- 1.4 Establish energy industry standards that require each utility to perform at least annual PIAs, and PIAs when significant operations changes occur, for their area of responsibility on the Smart Grid and to show the data flows and related privacy vulnerabilities and threats for consumer meter and power collection points.

2. Notice & Purpose for PII Use

For currently-used non-smart meters there are no clear notices for how the information read from the meters or provided in the billing process is used. Consumers have generally long assumed the information was only used for billing purposes. The new smart meters and accompanying potential and actual uses creates the need for utilities to be more transparent and clearly give notice documenting the types of information items collected through the smart meters, and the purposes for collecting the meter data.

Within the Smart Grid there must be a clearly specified notice describing the purpose for the collection, use, retention, and sharing of PII. Data subjects should be told this information at or before the time of collection.

Recommendations:

- 2.1 Establish policies and standards for the types of privacy notices and content that utilities must provide to consumers.
- 2.2 Establish publicly available locations, such as on utility websites, where consumers can find more information about the types and purpose of PII collected and used within the Smart Grid.

3. Choice & Consent to use PII

For currently-used non-smart meters the data taken from the meters is basic data usage readings. Locations of extreme energy use, energy use related to time, and other types of information that can reveal the activities of the residents is not collected. The new smart meters and accompanying potential and actual uses creates the need for utilities to give residents a choice about the types of data collected, especially if energy use is not dependent upon specific types of data. Utilities should also obtain consent from residents for using the collected data for any other purposes, and as a requirement before data can be shared with other entities.

Within the Smart Grid there must be a clearly documented policy and standard for utilities to follow to give residents choice for PII use, and to obtain consent before sharing residential PII.

Recommendations:

- 3.1 Establish policies and standards for the types of choices that utilities must give to residents.
- 3.2 Establish policies and standards for utilities to follow to obtain consent before sharing residential PII with other entities.

4. Collection of PII

For currently-used non-smart meters the data taken from the meters is basic data usage readings that is required to create the bills. The new smart meters will not only collect many more types of data, but any extraneous data collected could be PII, or combined with other data items and used as derived PII. Because of the associated privacy risks, only the minimum amount of data items necessary for the utility companies to use for energy management and billing should be collected. However, the amount of information collected may vary, depending on whether or not power generation occurs on the premises. Home generation services will likely increase the amount of information created and shared.

Only PII that is required to fulfill the stated purpose should be collected from individuals. Information use must conform to fair information processing practices.

Recommendations:

- 4.1 Establish policies and standards to specify the types of data items that can be collected through the smart meters.
- 4.2 Establish policies and standards directing utilities not to collect any more data items than specified.

5. Use and Retention of PII

For currently-used non-smart meters the data taken from the meters is used to create the residents bills, determine energy use trends, and let customers control their energy usage both onsite and remotely. The new smart meters, and the Smart Grid network, will have the capability to use the collected data in an unlimited number of ways. Many of these ways could create the privacy situations described in section 7 below.

Information should only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorized to receive it. PII should be aggregated or anonymized wherever possible to limit the potential for computer matching of records. PII should only be kept as long as is necessary to fulfill the purposes for which it was collected.

Recommendations:

- 5.1 Establish policies and standards that outline the appropriate and acceptable uses for data items collected through all the possible types of Smart Grid devices.

5.2 Establish policies and standards that specify how long each type of meter data should be retained.

5.3 Establish policies and standards that specify how to effectively and irreversibly remove meter data from Smart Grid devices, and from the home meters, when it is no longer needed for Smart Grid energy management purposes.

6. Individual access

For currently-used non-smart meters the data taken from the meters is easily obtainable by consumers from their own homes. The data collected from the new smart meters, and the associated data collected and derived, will potentially be stored in multiple locations throughout the Smart Grid. Currently no standardized process or mechanism has been identified that will allow residents to get access to their own corresponding PII that is stored throughout the Smart Grid. However, there are multiple companies, such as Google, Microsoft and 4Home, that are proposing solutions for consumers to have all the same information that the utilities are collecting from the residence.

Currently customers are provided the ability to access their account information through their monthly bill, utility websites, and yearly T&C statements. The utilities that comprise the Smart Grid, and any third party company that customers have provided consent for data sharing, should establish and provide to all customers a process to allow them to ask to see their corresponding PII and to request the correction of perceived inaccuracies. PII data subjects must also be informed about parties with whom PII has been shared.

Recommendations:

6.1 Establish policies and standards to provide individuals access to their corresponding PII data items that are stored within all the Smart Grid systems.

6.2 Require any third party company that is storing customer Smart Grid data to establish and follow policies and procedures to provide individuals access to their corresponding PII data items.

6.3 Establish policies and standards, from companies managing parts of the Smart Grid and third parties storing customer PII, to notify residents whenever their PII is shared with another entity.

7. Disclosure and Limiting Use of PII

Significant privacy concerns and risks exist when PII and derived PII is inappropriately shared without the knowledge and consent of the individuals about whom the PII applies. PII should be used only for the purposes for which it was collected. PII should

not be disclosed to any other parties except for those identified in the notice, or with the explicit consent of the individual.

Data collected through the smart meters should be used only for the specific purposes for which it was collected. If utilities want to use the data for other purposes, or share with other entities, they should notify consumers, clearly communicate their plans, and obtain consent to use and share the data as described. However, based upon the documents reviewed, there does not appear to be any policies

Figure D.7.1 provides a summary of the privacy concerns related to PII and derived PII use when disclosed to other entities and used for purposes beyond the PII collection purposes.

Privacy Concern	Discussion
1. Identity Theft	Specific combinations of PII may be used to impersonate a utility consumer, resulting in potentially severe impacts, such as negative credit reports, fraudulent utility use and other damaging consumer actions.
2. Determine Personal Behavior Patterns	Access to data use profiles that can reveal specific times and locations of electricity use in specific areas of the home can also indicate the types of activities and/or appliances used. The information revealed is a type of surveillance. The data could be (mis)used by other entities to do target marketing, by governments to try and tax specific activities and uses, and by persons with malicious intent..
3. Determine Specific Appliances Used	Smart meter data will have the ability to track the use of specific smart appliances that are programmed to communicate with the smart meters. Appliance manufacturers may want to get this information to know who, how and why individuals used their products in certain ways. Such information could impact appliance warranties. Insurance companies may want to use this information to approve or decline claims. And there is an unlimited number of other possible uses as yet not imagined that this data could provide.
4. Perform Real-Time Surveillance	Access to live energy use data can reveal if people are in the residence, what they are doing, where they are in the residence, and so on. This not only presents a safety risk, with burglars and vandals using it to their destruction, but it could also be used to do target marketing based upon home energy use behaviors.
5. Reveal Activities Through Residual Data	Several articles have been published warning that if the data on the metering devices is not effectively or completely removed, the residual data can reveal to the new meter user, or entity that possess the meter, the activities of the former owner. If true, not only does this present similar concerns to those listed in the first three concern topics, it could also be

	used by activists or others who have agendas to reveal what they view as a lack of social responsibility. However, to prevent any tampering of historical data and to satisfy the size constraints for the new meters — providing more functionality in the same physical meter box — the data is not likely to be stored within the smart meter itself. But, the possibility of storing data within home meters should be considered in any meter functionality plans so that if it does become possible to store PII in smart meters the privacy issues will be appropriately addressed.
6. Target Home Invasions	Malicious use of meter data for specific consumers could lead to a wide number of problems, such as physical invasions to the home because crooks could tell when residents were away, whether or not they have an alarm system, and so on.
7. Provide Accidental Invasions	Combinations of meter data, analyzed for one purpose, could reveal unexpected information about the residents that is then used to the detriment of the residents.
8. Activity Censorship	The meter data could reveal resident activities or uses that utility companies may then subsequently decide are inappropriate or should not be allowed. Without restrictions, if this information could then shared with local government, law enforcement, or public media outlets the residents could suffer embarrassment, harassment, loss of vital appliances, or any number of other damaging actions.
9. Decisions and Actions Based Upon Inaccurate Data	With meter data being stored in potentially many locations, accessed by so many different individuals and entities, and used for a very wide variety of purposes, it is a significant risk that the PII data will become inappropriately modified. Automated Smart Grid decisions made for home energy use could not only be detrimental for residents (e.g., restricted power, thermostats turned to dangerous levels, and so on) but decisions about Smart Grid power use and activities could be based upon inaccurate information.
10. Reveal Activities When Used With Data From Other Utilities	Even more personal activities and derived PII could be revealed if the power meter PII was combined with the PII from other utilities and utility meters, such as those for gas, water, and so on.

Figure D.7.1 – Privacy impacts for PII disclosure and misuse

Recommendations:

7.1 Establish policies and standards that clearly define how PII, and derived PII, within all areas of the Smart Grid can, and cannot, be used.

8. Security and Safeguards

For currently-used non-smart meters, physical security is the primary means of protecting the usage information that is on the readout viewable on the meter. The data collected from the new smart meters, and the associated data collected and derived, will potentially be transmitted to and stored in multiple locations throughout the Smart Grid. Establishing strong security safeguards will be necessary to protect the PII. PII, in all forms, must be protected from loss, theft and must prevent unauthorized access, disclosure, copying, use or modification.

Recommendations:

8.1 Establish policies, standards and definitions for what constitutes a privacy breach of PII within the Smart Grid system.

8.2 Establish policies and standards the utilities and all other Smart Grid entities must follow for responding to privacy breaches, including breach notification requirements.

9. Accuracy & Quality of PII

For currently-used non-smart meters, accuracy of the information physically collected from the meters is dependant upon the care given to collecting the meter reading by the person collecting the meter reading. The data collected from the new smart meters, and the associated data collected and derived, will potentially be stored in multiple locations throughout the Smart Grid. There could be a variety of ways in which the meter data is automatically collected. The ability to inappropriately modify the data could be significant in utilities where access controls are not appropriately set. Establishing strong security safeguards will be necessary to protect the PII. With meter data being stored in potentially many locations, accessed by so many different individuals and entities, and used for a very wide variety of purposes, it is a significant risk that the PII data will become inappropriately modified. Automated Smart Grid decisions made for home energy use could not only be detrimental for residents (e.g., restricted power, thermostats turned to dangerous levels, and so on) but decisions about Smart Grid power use and activities could be based upon inaccurate information.

Every effort must be made to ensure that PII collected at all points throughout the Smart Grid, and at all points where it is stored, is accurate, complete and relevant for the purposes identified in the notice, and remains accurate throughout the life of the PII within the control of the entire Smart Grid system.

Recommendations:

- 9.1 Establish policies and standards for all utilities to follow, and all areas of the Smart Grid with PII storage repositories and accessibility, to ensure integrity and accuracy.
- 9.2 Establish policies and standards for all third parties, who have obtained access to Smart Grid PII, to follow to ensure integrity and accuracy.

10. Openness, Monitoring & Challenging Compliance

For currently-used non-smart meters, utilities throughout the United States follow a very wide variety of methods and policies for communicating to residents how PII will be used. Some utilities do not provide any types of privacy notices to residents. The data collected from the new smart meters, and the associated data collected and derived, will potentially be stored in multiple locations throughout the Smart Grid, possibly within multiple states. Privacy protections must be applied consistently and at the same level for all PII throughout the entire Smart Grid system to be effective.

The Smart Grid must establish comprehensive and consistent privacy policies throughout the entire network, applicable to all states. Smart Grid consumers must be given the ability and process to challenge a utility's compliance with the published Smart Grid privacy policies as well as a specific utility's actual privacy practices.

Recommendations:

- 10.1 Establish a comprehensive privacy policy that applies to all parts of the Smart Grid.
- 10.2 Establish policies and standards specifying how consumers can submit complaints and challenges regarding privacy policy compliance by specific utilities.
- 10.3 Establish a Smart Grid agency responsible, or assign responsibility to an existing utilities agency, for oversight and enforcement of the Smart Grid privacy policy.

E. Regulatory and Legal Compliance

As mentioned in the AMI-SEC System Security Requirements, one of the standards approved by NIST for the Smart Grid,

*The organization shall conduct a privacy impact assessment on the information system in accordance with regulatory and the organization's policy.*⁵

⁵ Retrieved from page 50 at: http://www.controlsroadmap.net/pdfs/AMI_System_Security_Requirements-v1_01-1.pdf

In the absence of federal or state regulatory requirements, state utility commissions and customer advocacy groups (working through their respective state attorney general or public counsel) should strongly encourage Smart Grid entities to perform a Privacy Impact Assessment and provide appropriate choice and notice to consumers.

In many respects, the push to address privacy issues created by the Smart Grid has already begun. NARUC has adopted the *"Resolution Urging the Adoption of General Privacy Principles For State Commission Use in Considering the Privacy implications of the Use of Utility Customer Information."* (available at http://www.naruc.org/Resolutions/privacy_principles.pdf)