

## Rebecca Herold Notes

Information sent to Lillie Coney at EPIC to discuss prior to our Wednesday, 11/11/09 meeting

(NOTE: Will likely change prior to 11/11! This is an FYI for the group)

### **DRAFT proposed privacy standards for organizations that are part of the smart grid (and beyond):**

The following is based upon long-established privacy principles (from the OECD and then subsequently another draft from AICPA/CICA), as well as existing data protection laws and regulations as I've documented within the NIST smart grid privacy group working spreadsheet.

1. **Consent & Choice**: 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 personal information.
2. **Notice & Purpose Specification**: The organizations must provide a clearly worded notice, at or before the time of collection, describing the purpose for the collection, use, retention, and sharing of personal information, along with listing the items that are collected.
3. **Individual Participation & Access**: Organizations must provide a process for individuals and households to allow them to ask to see their corresponding personal information. Organizations must also provide a process to allow individuals and households to request the correction of perceived inaccuracies within the corresponding personal information provided by each organization. Individuals and households must also be informed about all the other parties with whom their corresponding personal information has been shared.
4. **Data Quality/Integrity/ Accuracy**: Organizations must make every effort, using documented policies, procedures, standards and ongoing training and awareness communications, to ensure that personal information and other data collected from smart meters is accurate, complete and relevant for the purposes identified in the notice, and remains accurate throughout the life of the information within the control of the organization. Policies and procedures must be in place to notify all other entities when corrections to personal information is made so that they can appropriate correct the corresponding information for which they are the custodians.
5. **Use Limitation**: Information within the smart grid networks and systems 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. Personal information should be aggregated or anonymized wherever possible to limit the potential for computer matching and data mining the records.
6. **Retention & Disposal Policies/Practices**: Smart meter information and corresponding personal information should only be kept as long as is necessary to fulfill the purposes for which it was collected. When it is no longer needed for the stated purposes for which it was collected, it should be irreversibly be deleted/destroyed using disposal method which, at a minimum, meets NIST disposal standards.
7. **Transparency & Openness**: Documented privacy policies must be made available to individuals and households that are part of the smart grid systems and networks. Individuals and households must be given the ability and process to challenge an organization's compliance with their stated privacy policies as well as their actual privacy practices.
8. **Collection Limitation**: Only information that is required to fulfill the stated purpose(s) should be collected from individuals from from households. Organizations collecting information must follow fair information processing practices. Personal information must

be collected directly from each individual or household, their corresponding smart meter, or an approved mobile smart meter data collection device, unless there are approved and documented reasons why this is not possible.

9. **Security/Safeguards:** Organizations that are part of the smart meter network must protect personal information, in all forms, from loss, theft and must prevent unauthorized access, disclosure, copying, use or modification.
10. **Accountability & Management:** Each organization must formally appoint a position, team, department or individual 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 consistently followed.
11. **Disclosure and Limiting Sharing:** Personal information must be used only for the purposes for which it was collected. Personal information must not be disclosed to any other parties except for those identified in the notice, or with the explicit consent of the corresponding individual or appropriate household representative.
12. **Monitoring & Enforcement:** Each organization that is part of the smart grid network and systems must monitor compliance with its privacy policies and procedures and have procedures to address privacy-related inquiries and disputes. Audit functions must be present to monitor all smart grid data and personal information uses, sharing and modifications.

### **Proposed certification recommendations:**

1. **Organization privacy self-certification** (for smart grid, but could be a way to "certify" any organization in any industry; follows along the concept of the EU Safe Harbor program):

We strongly recommend the energy industry follow the lead of the U.S. government agencies who perform annual privacy impact assessments (PIAs) and require each organization that participates in the smart grid network and systems, as well as each organization that performs activities for such organizations, to:

- 1) perform an annual PIA, provide it to each state's energy commissioner office to review, and
- 2) perform a PIA on each new system, network, or smart grid application and provide it to each state's energy commissioner office to review.

The state energy commissioner office will:

- 1) either acknowledge the PIA is appropriate and send approval to the organization, after which the organization will post it on their website, or
- 2) notify the organization and communicate the privacy deficiencies identified within the PIA and ask them to correct them. While the correction is being made, a notice containing an executive summary of the PIA findings must be posted on the organization's website, along with a high-level description of the corrective actions being performed and corresponding target dates for completion.

2. **Smart Meter device privacy certification:**

We strongly recommend that the energy industry require each smart grid meter be reviewed by *<appropriate group or agency>* prior to its use and implementation, and be certified as appropriately providing privacy choices and having proper privacy protections. ***<Much needs to be expanded upon here.>***

## **Questions and notes about the above sections:**

- Should "household" be replaced with a different term, such as "dwelling," or "location," or "facility," or something else to broaden the scope from just places where people live?
- I believe self-certification would be a very good thing. However, the details I've provided are VERY rough and need a lot of fine-tuning and rewriting. However, I wanted to provide them to get the conversation started.
- I believe requiring the smart meter devices to be certified as being "privacy friendly" is a good idea, but the details need to be worked out, in addition to determining how the certification would occur, and the entities qualified to do such certifications.
- What is the best term to use in place of "state energy commissioner office"?
- What is the best term to use in place of "energy industry"?
- We need to create some definitions for the above referenced terms when we have identified what will be used.
- The wording needs to be tweaked considerably to fit with NIST expectations and requirements.

## **Proposed definitions (need to add more):**

- **Personal information:** Information that reveals information, either explicitly or implicitly, about a specific individual, or household dwelling (note, I'm expanding this beyond the normal "individual" component because I believe there are just as serious of privacy impacts for all individuals living in one dwelling as are there the typically considered impact to a specific individual. This can include items that, on their own, may not point to one specific individual or dwelling, such as energy use patterns. I believe the pattern can become unique to a household just as a fingerprint or DNA is unique to an individual; but simply looking at it will not reveal to the naked eye who the individual is, or where the dwelling or associated individuals are at.
- **Personally identifiable information (PII):** An information item that can point to a specific individual, such as Social Security number, Credit Card number, birthdate (under certain conditions), address, and so on.
- **Multi-part personally identifiable information (Multi-part PII):** Non-PII items that, when combined with certain other non-PII items, can actually become PII. In other words, aggregating non-PII to form PII. A collection of data items that, when each individually is not considered, could become PII and reveal insights into personal lives and activities.