**PRIVACY™ PROFESSOR**

## Smart Grid Privacy Concerns

### October 2009

### Rebecca Herold

After doing some more thinking, researching, digging and having some great discussion with the folks participating in the NIST smart grid privacy group, I added five more smart grid privacy concerns to the list from September. Table 1 shows an updated 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) I sent to the NIST smart grid privacy group in October for them to consider and for us to discuss.

***NOTE: These represent my viewpoints and not necessarily those of NIST! I am making them public so that I can engage in meaningful discussion about these issues, and any others not identified within the table. Let me know your thoughts!***

| 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. |
| 11. **Profiling** | Profiling may be possible in ways that were previously not possible, or not as easily possible. What can you tell about what you can see from energy consumption?  For example, if the consumers are straight or gay?  Terrorist profiles? Affairs?  Illegal activities?  Will access to do data mining for investigations put people on terrorist watch lists, etc.?  Will politicians want to use for potential activity taxation?  Performing a gap analysis could point out scenarios and associated risks. |

| | |
|---|---|
| **12.Unwanted Publicity and Embarrassment** | Embarrassment and other negative impacts resulting from unauthorized disclosure and/or publication of household or electric vehicle use. |
| **13.Tracking Behavior Of Renters/Leasers** | When a different individual owns and pays the utilities other than the resident, such as in the case of a rental unit, room subletting, leasing, and so on, the landlord or property owner could have access to the smart meter data and potentially track the residents' activities.  Rent decisions could be made base on past power usage history.  Power usage profiling could following individuals and impact a wide range of decisions. |
| **14.Behavior Tracking** | Will there be any items within the smart meters that can act in ways similar to browser/document cookies or web bugs?  If so, these items could be (mis)used in ways similar to how cookies and web bugs are currently (mis)used.  Perhaps RFID tags can be used in some ways?  Perhaps GPS types of technologies? |
| **15.Public Aggregated Searches Revealing Individual Behaviors** | What kind of smart grid search engines will there be?  What discussions or plans have occurred around this possibility?  What information would be involved?  What control would consumers have to not have their data included in such searches?  The privacy issues would be similar to the privacy concerns that currently exist with Internet search engines, only the implications could be more wide-reaching because the data would be based upon individuals' actual daily living activities, and not upon what they consciously chose to put onto the Internet. |

*Figure 1- Privacy impacts for Smart Grid information disclosure and misuse*