

classifieds: autos homes jobs pets ads

Home Delivery
About Us
Customer Service
Email newsletters
Join The Sun Club

Your home. Your local news.
Naperville Sun
NaperSun.com Member of Sun-Times Media

21°F
Clear
Weather

Search »

 Site All Papers
 Web Search by
YAHOO!

BECOME A MEMBER!
What's this?

Become a member of our community!

[Home](#) | [News](#) | [Sports](#) | [Business](#) | [Entertainment](#) | [Classifieds](#) | [Lifestyles](#) | [Ebert](#) | [Search](#) | [Archives](#) | [Obituaries](#) | [Video](#) | [Blogs](#) | [RSS](#)



PHOTOS: ARREST MUGS»
More Naperville police news



VIRTUAL COOKIE EXCHANGE»
Search, then share your favorites



PHOTOS: SANTA SNAPSHOTS»
Share your pictures



PHOTOS: HOLIDAY PETS»
Share your pictures

our towns
Twitter
football scores
Twitter
facebook

News Alerts
[E-mail](#)
[Text message](#)
[RSS](#)
Blogs
[Potluck](#)
News
[Local](#)
[Region](#)
[Nation](#)
[World](#)
[Blagojevich](#)
[Obama](#)
[Education](#)
[Elections](#)
[Health](#)
[Politics](#)
[Religion](#)
Local News
[Main Page](#)
[Police Blotter](#)
[Schools](#)
[Neighborhoods](#)
[Obituaries](#)
[Elections](#)
[Opinions](#)
[Weather](#)
Columnists
[David Dial](#)
[The Fixer](#)
[Cy Frank](#)
[Potluck Digest](#)
[Bill Mego](#)
[Readers' Editor](#)
[A. George Pradel](#)
[The Pulse](#)
[Naperville Talk](#)
[Tim West](#)



NAPERVILLESUN ::

The views expressed in these blog posts are those of the author and not of the Sun-Times News Group.



Information-Security-Resources.com
Helping industry stakeholders, government regulators, and the public better understand and address the mounting information security threats inherent in the cyber age.

Smart Grid Privacy Standards Proposed

Tuesday, December 01, 2009

By *Rebecca Herold (The Privacy Professor) CIPP, CISSP, CISM, CISA, FLMI*

Sorry to be so tardy in getting a blog post out. As many of you know I've been working with the NIST Smart Grid Privacy Subgroup since late June.



The work done for this group is through time volunteered by all involved.

As a quick recap, I led the privacy impact assessment (PIA) for the consumer-to-utility portion of the planned smart grid during the late June to late August/early September time frame.

On Friday, 11/20, I provided an update on our NIST groups activities during the Gridwise Alliance phone conference; perhaps some of you were on that call?

Here are some links showing information about our NIST Smart Grid privacy group's work:

- You can see the documents showing our group's work on the [NIST Smart Grid twiki](http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy) at: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy>
- The draft PIA I referenced earlier is located at: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGPrivacy/NIST_High_Level_PIA_Report_-_Herold_09_09_09_w-edits.doc
- See some of my blog posts about Smart Grid privacy at:

SEND A NEWS TIP

Share news and photos with us

If you have a news tip or photo of a newsworthy event, let us know by using our online [submission form](#), calling us at (877) 681-NEWS (6397) or e-mailing us at news@scn1.com.



Visit zip2save.com for all your favorite circulars & coupons!

[Circulars](#) | [Coupons](#) | [Deals](#)

Video

- [Cupcake wine show Ta...](#)
- [The Dancing Horses](#)
- [A Tour of Rich](#)

TOP STORIES ::

NEWS
[Naperville officers sued over TV show](#)

BUSINESS
[Expectant moms turn to baby planners](#)

SPORTS
[Are the answers in Florida?](#)

ENTERTAINMENT
[Oak Ridge Boys changing with the times](#)

LIFESTYLES
[Chocolate's health benefits keep expanding](#)

INSIDE ::

[SearchChicago - Autos](#)

b. Attributing personal mobile electricity use, such as through PEVs, to another individual or household

Discussion: Specific combinations of smart grid data, collected from PEVs or other types of mobile electricity usage equipment, 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.

Mitigating controls (privacy standards): 8, 9, 10, 11, 15, 16, 17, 18

2. Personal Surveillance**a. Perform real-time personal surveillance of dwelling inhabitants based on energy use**

Discussion: Access to live energy use data can reveal if people are in the dwelling, what they are doing, where they are in the dwelling, 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 dwelling energy use behaviors.

Mitigating controls (privacy standards): 1, 3, 4, 5, 6, 8, 9, 10, 11, 14, 16, 17, 18, 19

b. Determine personal behaviors and activities of dwelling inhabitants and tracking over time

Discussion: Access to data use profiles that can reveal specific times and locations of electricity use in specific areas of the dwelling can also indicate the types of activities and/or appliances used as well as various types of activities within the dwelling over a period of time.

The information revealed is a type of surveillance.

The data could be used, and misused, by other entities to do target marketing, by governments to try and tax specific activities and uses, by employers who want to know where and when employees were and what they may have been doing during certain dates, by insurance investigators as part of their claims investigations, and by persons with malicious intent.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19

c. Determine personal behavior patterns of dwelling inhabitants

Discussion: Access to data use profiles that can reveal specific times and locations of electricity use in specific areas of the dwelling can also indicate the habits of the dwelling inhabitants.

By knowing habits of inhabitants, assumptions can be made about what what types of activities they will do, or when they will likely, or likely not, be within the dwelling.

Such assumptions about habits can potentially lead to inappropriate or erroneous decisions by not only utilities companies, but also by appliance makers, vendors using the smart grid, government agencies, law enforcement, employers, insurance companies, criminals and others.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19

d. Reveal activities through smart meter and/or smart grid residual data

Discussion: If the data on the metering devices is not effectively or completely removed, the possibility exists that the residual data can reveal to the new meter user, or entity that possess the meter, the activities of the former owner.

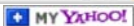
If true, not only does this present similar concerns to those listed in the first three concern topics, it could also be used by activists or others who have agendas to reveal what they view as a lack of social responsibility.

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.

Mitigating controls (privacy standards): 8, 11, 15, 17, 18, 19

e. Tracking personal behavior of renters/leasers



© Copyright 2009 Sun-Times Media, LLC
 Terms of Use • Privacy Policy •
 Submission Guidelines • About Our Ads

Discussion: When a different individual owns and pays for 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 based on past power useage history. Power useage profiling could following individuals nad impact a wide range of decisions.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 6, 7, 8, 15, 17, 18, 19

f. Profiling

Discussion: 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.

Mitigating controls (privacy standards): 6, 7, 9, 10, 11, 14, 15, 16, 17, 19

g. Data Mining

Discussion: Combinations of meter data and other data within the smart grid network, analyzed for one purpose, could unexpectedly reveal information about the dwelling inhabitants that is then used to the detriment in one of many ways, as listed in this matrix, of the residents.

Mitigating controls (privacy standards): 6, 7, 9, 10, 11, 14, 15, 16, 17, 19

3. Energy Use Surveillance

a. Determine specific appliances used (when, where, how long, etc.)

Discussion: 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.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

b. Perform real-time energy use surveillance

Discussion: Smart meter data will have the ability to track the real-time 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.

Access to live energy use data can reveal if people are in the dwelling, what they are doing, where they are in the dwelling, 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.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

c. Reveal activities that have occurred when used with data from smart meters, smart appliances, etc.

Discussion: Data from smart appliances when compared to and used with data from smart meters may be able to reveal activities that occurring within dwellings at specific times and on specific dates.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 15,

16, 17, 18, 19

d. Tracking energy use behavior of renters/leasers

Discussion: When a different individual owns and pays the utilities other than the dwelling occupant, 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 useage history. Power usage profiling could following individuals and impact a wide range of decisions.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 6, 7, 8, 14, 15, 16, 17, 18, 19

e. Determining energy use when combining data with the data from other utilities or other entities (e.g., Google and Microsoft applications)

Discussion: Even more personal activities and information could be revealed if smart meter data and/or smart grid data was combined with data from other utilities and utility meters, such as those for gas, water, and so on, or with other smart grid vendors or organizations that have collected smart grid data in any way.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,11, 15, 17, 19

f. Energy consumption and related activity censorship or limitation

Discussion: Combinations of meter data, analyzed for one purpose, could unexpectedly reveal information about the residents that is then used to the detriment of the residents.

E.g., making financing decisions, investigations, insurance rates, and so on.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,11, 15, 17, 19

g. Energy consumption and related activity taxation

Discussion: Smart meter and smart grid data could be used to determine energy use activities in ways that government entities may wish to tax or otherwise find uses for that could penalize the dwelling occupant in some way because of their assumed (from the grid data) lifestyles.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,11, 15, 17, 19

4. Physical Harm

a. Stalking and domestic abuse

Discussion: Malicious use of smart meter, or any smart grid, data for specific consumers could lead to a wide number of problems, such as physical invasions to the home from stalkers or ex-spouses or ex-partners who want to do harm to the residents, or want to enter the premises when residents were away.

Meter data could allow such malicious individuals to tell whether or not the residents have an alarm system, where they are located at any point in time in the dwelling, and so on.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19

b. Targeted home invasions

Discussion: 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.

The meter data could also allow crooks to determine the types of appliances are within the dwelling based upon usage data, giving them information used to make decisions about which dwellings to rob or terrorize.

Mitigating controls (privacy standards): 1, 2, 3, 4, 5, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19

c. Negative health impacts based upon automated or breached smart grid or smart meter actions/activities

Discussion: Smart meter thermostats can theoretically be programmed to make decisions about the house's heating and air conditioning levels.

The thermostat can be set to adjust automatically to use less energy. Smart appliances can also conceptually be programmed to run during times when electricity is less expensive, such as adjusting the thermostat at night or to start the dishwasher automatically at night when no other appliances are running.

If someone determines when inhabitants are in the dwelling and gets access to make changes to the meter settings they could make the dwelling colder or hotter with physical detriment to the inhabitants, especially those inhabitants who are not physically able to change the meter settings themselves.

Mitigating controls (privacy standards): 15, 16, 17, 18, 19

5. Decisions and Actions Based Upon Inaccurate Data

a. Reveal household or individuals activities through residual data from smart grid components

Discussion: If the data on the metering devices, or other smart grid components, is not effectively or completely removed, the residual data can reveal to the new meter user, or entity that possesses the meter or other smart grid component, 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 personal information in smart meters the privacy issues will be appropriately addressed.

Mitigating controls (privacy standards): 8, 14, 15, 16, 17, 18, 19

b. Decisions made based upon data mining inaccurate smart grid data

Discussion: 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 smart meter and smart grid data for specific consumers could become inappropriately or accidentally modified.

Even when security controls work correctly, data can be inappropriately and accidentally 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 for specific dwelling inhabitant activities could be based upon inaccurate information.

Mitigating controls (privacy standards): 13, 14, 15, 16, 17, 18, 19

c. Decisions made based upon data profiling using smart grid data

Discussion: 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 smart meter and smart grid data for specific consumers could become inappropriately or accidentally modified.

Data profiling is increasingly being used to determine the activities and characteristics of specific individuals, and then subsequently used in investigations, research, credit monitoring, insurance decisions, and an unlimited number of other activities.

Using data profiling applications to make decisions about Smart Grid power use for specific dwelling inhabitant activities could be based upon inaccurate information, and could subsequently result in actions that negatively impact dwelling inhabitants in their home, work or travel activities.

Mitigating controls (privacy standards): 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19

6. Reputation Harm

a. Unwanted publicity and embarrassment based upon smart grid or smart meter reports or associated data

Discussion: Embarrassment and other negative impacts could result from unauthorized disclosure and/or publication of household, electric

vehicle or other types of smart meter/appliance/vehicle use.

Mitigating controls (privacy standards): 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 19

b. Public aggregated searches of smart grid data revealing individual behaviors

Discussion: What kind of smart grid network 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.

Mitigating controls (privacy standards): 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 19

c. Provide unintended publicized privacy invasions as a result of data aggregation and mining activities

Discussion: Even more personal activities and personal information could be revealed if the smart meter data was combined with the data from other utilities and utility meters, such as those for gas, water, and so on.

What types of reports will utilities, smart appliance and meter vendors, and other entities involved with the smart grid be publishing?

Will they publish reports that will reveal activities or information about specific dwellings or PEVs? 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?

Mitigating controls (privacy standards): 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 19

Establishing and implementing a comprehensive set of privacy standards will be effective for providing a significant set of baseline mitigating controls.

Of course there will likely need to be other specific types of controls added within specific sections of the smart grid as well, but using a set of proposed privacy standards are a good solid basis to start from.

Plus, establishing multiple privacy controls (resulting from implementation of the standards) will create the layers of protections necessary to truly have a positive impact for effectively protecting privacy.

As we've long known with information security, layers of controls are necessary to provide effective protection; doing single actions in isolated areas helps, but does not effectively provide protection throughout the network in the long run.

The same concept is true for protecting privacy; we need layers of privacy protections throughout the entire smart grid to effectively address privacy concerns and prevent privacy invasions and breaches.

So, I spent time creating the proposed smart grid privacy standards below, and indicated within the matrix, the ones that best map to each of the privacy impacts (these are indicated by the numbered mitigating controls above).

Again, I realize there are other mitigating controls that are likely to be necessary, but these can provide a solid starting point.

Plus, it highlights the power (pardon the pun) that good privacy standards can have when built into the smart grid from the very beginning, and also when used and followed by all entities involved with the smart grid.

1. **Limiting the collection** of data by the smart meter to only that necessary for the purposes of improving energy use and efficiency for the specific dwelling.
2. **Limiting the collection** of data by the utilities from the persons paying the utilities account at the dwelling to only that necessary to manage the account and to improve energy efficiency.
3. **Notify** the dwelling inhabitants (which may be different from the individuals paying the utilities bill for the dwelling) and persons paying the utilities bills of the data being collected, why it is necessary to collect the data, along with the specific uses for the data, the purpose for the collection, and the use, retention, and sharing of the data. Data subjects should be told this information before the time of

collection.

4. **Notify** the dwelling inhabitants whenever the utility, or a smart grid entity, wants to start using existing collected data for different purposes.

5. **Notify** the dwelling inhabitants whenever the utility, or a smart grid entity, wants to start collecting additional data beyond that already being collected, along with provided a clear explanation for why the additional data is necessary.

6. Each utility and any other entity collecting energy usage data from or about dwellings must **provide** a clearly worded description to the dwelling inhabitants notifying them of 1) any **choices available** to individuals and, 2) **explain why specified data items must be collected and used** in specified ways without obtaining consent from the individual.

7. Each utility and any other entity collecting energy usage data from or about dwellings must describe the **choices available** to dwelling residents with regard to the use of their data and obtain explicit **consent** if possible, or implied consent when this is not feasible (such as for providing basic service), with respect to the collection, use and disclosure of the data collected from the specific dwelling.

8. Data, and subsequent created information that reveal personal information or activities, from and about specific dwellings should be **retained only for as long as necessary** to perform the purposes that have been communicated to the inhabitants. When no long necessary the data and information, in all forms, should be irreversibly destroyed.

9. Data and created information from and about specific dwellings should only be **used or disclosed for the specified purposes** for which it was collected and should only be divulged to or shared with those parties authorized to receive it, and whom the organizations have told the dwelling inhabitants it would shared.

10. Data and created information from and about specific dwellings should **not be disclosed to or shared** with any other parties except for those identified in the notices that have been provided to the dwelling inhabitants, or with the explicit consent of the individual.

11. Data collected from dwellings should be **aggregated and anonymized** by removing personally identifiable information elements wherever possible to ensure usage for data of individual dwellings are limited appropriately.

12. Each utility and any other entity collecting energy usage data from or about dwellings should **provide a process** to allow dwelling inhabitants to ask **to see and be given access** to the corresponding data from their specific dwelling, generated through their energy use and on their utilities account, and to request the correction of perceived inaccuracies.

13. Each utility and any other entity collecting energy usage data from or about dwellings must establish documented policies and procedures to ensure that the data collected from, and subsequently created about, dwelling inhabitants is **accurate, complete and relevant** for the purposes identified in the notice, and remains accurate throughout the life of the dwelling data within the control of the organization participating in the smart grid.

14. Each utility and any other entity collecting energy usage data from or about dwellings **must make privacy policies available** to dwelling inhabitants. Organizations participating in the smart grid must establish a procedures that allows dwelling inhabitants to the organization's compliance with their published privacy policies as well as their actual privacy practices.

15. Each utility and any other entity collecting energy usage data from or about dwellings must formally **assign responsibility** to a position or person to ensure that information security and privacy policies and practices exist and are followed. As part of their responsibilities, documented requirements for regular training and ongoing awareness activities must exist and be followed. Audit functions must also be present to monitor all data accesses and modifications.

16. Each utility and any other entity collecting energy usage data from or about dwellings must ensure that information in all forms, collected from, and subsequently created about, dwelling inhabitants, is **appropriately protected from loss, theft and must prevent unauthorized access, disclosure, copying, use or modification**.

17. Each utility and any other entity collecting energy usage data from or about dwellings must **perform annual privacy impact assessments** (PIAs) and provide it to each state's energy commissioner office to review. They must also perform a PIA on each new system, network, or smart grid application and provide it to each state's energy commissioner office to review.

18. Each utility and any other entity collecting energy usage data from or about dwellings must establish policies and procedures to **identify breaches and misuse** of smart grid data, along with establishing procedures and plans for notifying dwelling inhabitants in a timely manner with appropriate details about the breach.

19. Each utility and any other entity collecting energy usage data from or about dwellings must obtain and **maintain a current organizational privacy certification** from an authorized third party certification organization to validate processes, policies and controls are in place that supports each of the previously listed applicable privacy standards. The organization should post an approved certification seal on their website to allow easy validation of their privacy certification.

I want to know what you think so I can take your feedback to the group, and also consider and discuss with you. What are your thoughts about these privacy impact categories?

My proposed privacy standards?

I'll put PDFs of the matrix and the list of proposed standards [on my website](#) soon for easier reference, and also they'll look alot better than my blog editor can allow!

* * *

Stay Informed With ISR News Feeds and Email Alerts Here:

Enter your email address: Delivered by

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, is an information privacy, security and compliance consultant, author and instructor with her own company, Rebecca Herold & Associates, LLC, who has provided assistance, advice, services, tools and products to organizations in a wide range of industries throughout the world for over two decades.



The
Privacy
Professor,
aka
Rebecca
Herold &



Associates, LLC, has been a trusted source for effective information security, privacy and compliance tools, education and consulting since 2004. The Privacy Professor is located in Des Moines, Iowa within easy driving distance to Minneapolis/St. Paul, Chicago, Omaha, Kansas City and St. Louis, and easy flights to the east and west coasts. The Privacy Professor brings over two decades of expertise to organizations of all sizes, in all industries throughout the world. You can reach her at rebeccaherold@rebeccaerold.com or www.theprivacyprofessor.com.

The Publisher gives permission to link, post, distribute, or reference this article for any lawful purpose, provided attribution is made to the author and to Information-Security-Resources.com

These icons link to social bookmarking sites where readers can share and discover new web pages.



[Read more from this blogger](#)

The views expressed in these blog posts are those of the author and not of the Sun-Times News Group.