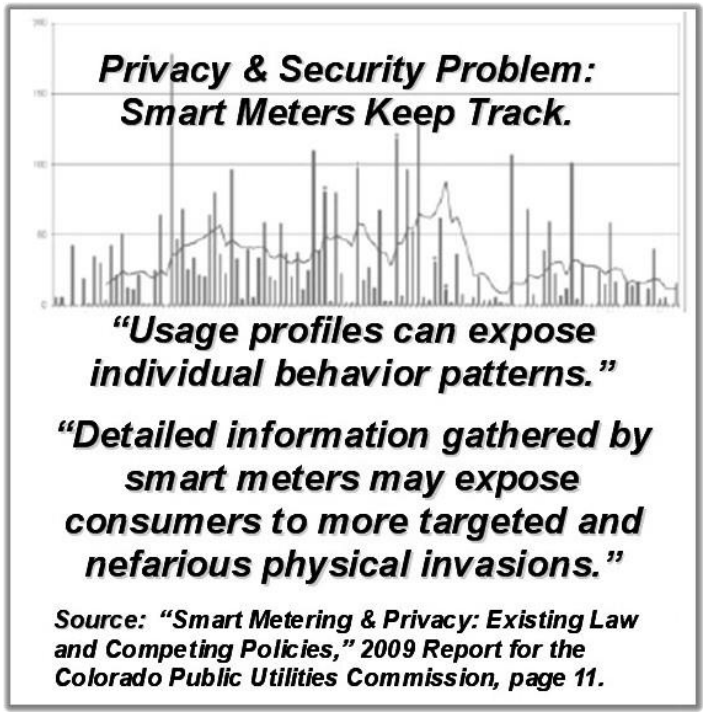
A PERSPECTIVE
ON HOW SMART METERS
INVADE INDIVIDUAL PRIVACY

by

K. T. Weaver

March 2, 2014
Updated August 22, 2014



SkyVision Solutions

Naperville, Illinois

http://skyvisionsolutions.org

Table of Contents

Section or Topic Description	Page
Introduction	3
What Are Smart Meters?	9
Smart Meter Data Collection Guidelines	11
What Data Do Smart Meters *Currently* Collect?	13
Are Smart Meters Even Necessary?	15
What Data *Should* Smart Meters Collect (if Utilized)?	17
An Example on How Consumer Privacy Interests Have *Not* Been Considered	20
Why Is Collected Smart Meter Data an Infringement on Privacy?	23
Specific Examples on How Smart Meters Reveal Household Activities	30
Peer Reviewed Literature on Cyber and Data Security Threats	35
Smart Meter Data Retention	41
Misrepresentations of Risks Associated with Smart Grid Technologies	42
Additional Substantiation of the Privacy and Security Issues	48
How Specifically Are Privacy Interests Being Compromised?	50
Legal Criteria for Determining Whether Privacy Rights Have Been Violated	52
Case Law for Privacy Infringements	53
Demonstrated Expectation for Privacy	58
Expectation for Privacy is “Reasonable”	58
Conclusions and Recommended Actions	61
Addendum: Additional Supporting Information	66
Attachment A, Smart Meter Privacy Invasions by “State Actors”	67
Attachment B, The White House Report on Big Data and Privacy	70

A Perspective on How Smart Meters Invade Individual Privacy

by K. T. Weaver [1]

Introduction

This document outlines a perspective that demonstrates that installation and use digital smart meters by a Utility represents an unprecedented invasion of privacy and, under certain circumstances, can be considered an unreasonable search in violation of the Fourth Amendment of the United States Constitution.

Although countless people claim that smart meters invade their privacy, it is unclear as to whether a compelling argument has yet been fully made that properly articulates an invasion of privacy assertion in a way that is understandable or convincing enough to persuade a sufficient number of legislators, governmental officials, court judges, or public utility commission hearing officers. To some extent, concerned consumers and activists have devoted a disproportionate amount of time and energy toward addressing potential health issues related to wireless smart meter RF emissions and have left the privacy arguments somewhat underdeveloped. In other instances, consumers are simply unaware of the significant privacy (and related cybersecurity) risks that exist with smart grid technologies. It is the purpose of this document to help formulate a clear and comprehensive message on how digital smart meters unreasonably invade consumer privacy.

---

[1] K. T. Weaver (hereafter referred to as the "Author") operates a website under the name of SkyVision Solutions at http://skyvisionsolutions.org or http://smartgridawareness.org/ dedicated to raising public awareness about the benefits, costs, and risks associated with smart grid systems as well as the potential hazards related to radiofrequency (RF) radiation emissions from all wireless devices, including smart meters.

Many consumers claim that smart meters violate their constitutional right to privacy based upon the language in the Fourth Amendment to the U.S. Constitution where it states, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches, shall not be violated …” In fact, many state constitutions are even more explicit. For example, Section 6 of Article 1 of the Illinois Constitution states: “The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications…”

Certainly in spirit, the Author believes that people are justified in claiming that their constitutional rights are being violated by smart meters being attached to their homes without their consent. In a legal sense, however, court rulings have generally limited constitutionally guaranteed privacy protection rights to situations that have involved overt government intrusion. If the Utility installing smart meters is also a government entity, then a Fourth Amendment allegation can be made. For a private “investor-owned” Utility, Fourth Amendment protections may not apply.

What is frustrating is that government-related public utility commissions for various states are allowing or even mandating that privacy invading smart meters be installed by utilities without consumer consent. In addition, in many areas of the United States, Department of Energy grant awards have been used to help fund the deployment of smart meters. This can certainly be considered as a form of *de facto* government intrusion.

Consequently, if a private utility company is ordered by a state public utility commission to install privacy invading smart meters as part of a mandate or otherwise ordered to charge a penalty fee for those refusing smart meters, then the private utility arguably becomes an “instrument or agent of the state” and

must abide by Fourth Amendment provisions. Refer to Attachment A, "Smart Meter Privacy Invasions by 'State Actors,'" for more information on this topic.

Setting aside that potential legal argument for now, the facts of record support an assertion that smart meter technologies have not been deployed for the overall benefit of the consumer. Instead, smart meters have debatably been deployed in favor of corporate financial interests, political agendas, and justified on the basis of somewhat hypothetical and dubious societal interests.

Based upon the information presented in this document, it will be demonstrated that through the use of "smart meters," utilities expose consumers to unnecessary risks by collecting massive amounts of data not necessary for billing purposes simply because "they can" and do so without regard to consumer privacy and security interests. Smart meter data, consisting of granular, fine-grained, high-frequency type of energy usage measurements, can be used by others either maliciously or inadvertently using existing or developing technology to infer types of activities or occupancies of a home for specific periods of time. In a general sense, analysis of granular smart meter energy data results in or may result in:

- Invasion of privacy and intrusion of solitude;
- Near real-time surveillance;
- Behavior profiling;
- Endangering the physical security of life, family, and property;
- Unwanted publicity and embarrassment (e.g., public disclosure of private facts or the publication of facts which place a person in a false light).

More specifically, analysis of smart meter data or manipulation of smart meter data/firmware can be used for the following purposes:

- Determine how many people are home and at what times;

- Determine your sleeping routines;
- Determine your eating routines;
- Determine what appliances you use when, e.g., washer, dryer, toaster, furnace, A/C, microwave, medical devices … the list is almost endless;
- Determine when a home is vacant (for planning a burglary), who has high-priced appliances, and who has a security system;
- Law enforcement can obtain information to identify suspicious or illegal behavior or later determine whether you were home on the night of the alleged crime;
- Landlords can spy on tenants through an online utility account portal;
- For consumers with plug-in electric vehicles, charging data can be used to identify travel routines and history;
- Utilities can promote targeted energy management services and products;
- Marketers could obtain information for targeted advertising;
- Hackers could wirelessly update smart meter firmware and remotely disconnect users. This could also allow attackers to corrupt the smart meters of individual homes, running up bogus charges or cause an electrical system to malfunction, shut down, or surge (frying all of your outlets and anything connected to them). Cyber assaults could involve hackers causing networked thermostats and appliances to malfunction possibly causing physical harm, especially to vulnerable populations. [Reference: "The Future of Crime" article, dated May 14, 2014];
- In combination with smart water meter data, exact times for taking a shower or bath can be determined and, with even greater accuracy, when is a home vacant and susceptible to undetected burglary.

With regard to informing consumers of smart grid risk-related information, utilities and manufacturers have *no* incentive to inform consumers of these risks since such action would create an even greater consumer backlash against the deployment of the smart grid technologies. ***Risk-related information is being deliberately suppressed by the smart grid industry, and the public is being provided misinformation which would indicate that there are no additional privacy or security risks related to smart meters as compared to the old analog meters.***

Part of the purpose of this document is to raise broad awareness of the type of full argument that needs to be made in order to have better success in convincing legislators, government officials, and others that smart meters *unreasonably* invade privacy. An argument that relies narrowly on the language contained in the Fourth Amendment may not be persuasive enough to effect changes in smart meter installation policies, except possibly for instances where the installing Utility is also a governmental entity (or a "state actor").

The principal arguments made in this document can be made in any setting (or nearly any country). A person has a legitimate expectation for privacy in their own home that is being compromised by smart meter technology, and a person can list a number of reasons why society should view those expectations as reasonable. Let's hope there are still conscientious government officials, legislators, and even utility executives who will listen to rational and thoughtful arguments. The reasoning outlined in this document can be adapted for use in both Federal and civil lawsuits, as applicable, but parties need to be prepared for possible costly and lengthy legal proceedings.

Originating within the City of Naperville, Illinois, there has been an ongoing Federal lawsuit (referred to hereafter as the Naperville Federal Lawsuit) that has sought relief for Naperville residents from alleged Constitutional infringements related to the mandatory installation of smart meters within that city. Among the assertions made within a Complaint to the Court is that smart meters infringe upon individual privacy rights granted under the Fourth Amendment of the U.S. Constitution. This Court proceeding is being held under the jurisdiction of the United States District Court for the Northern District of Illinois, Eastern Division. The Case Number is 11-CV-09299.

There will be occasion to reference specific documents from that Court proceeding during the course of documenting this perspective on how smart meters invade individual privacy. Some of the more recent Court documents can be viewed at the website link of http://skyvisionsolutions.org/lawsuits/federal-lawsuit-against-the-city-of-naperville-il/.

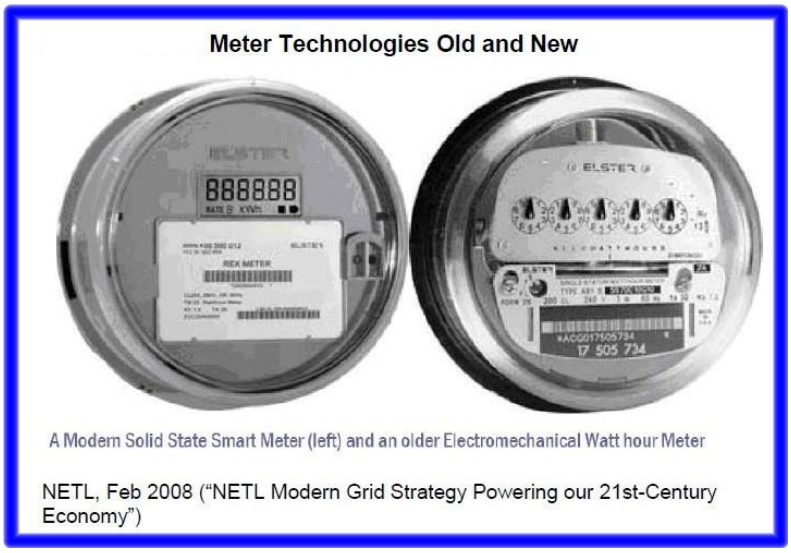
As somewhat of a disclaimer, the Author of this document will acknowledge upfront that he is not an attorney. The Author's professional career would primarily qualify him as a technical and regulatory expert. During the course of his career, the Author has had occasion to frequently work with attorneys on legal issues and has accumulated considerable experience in reviewing and analyzing legal documents. To the extent possible, the Author has applied that prior experience and analytical ability in researching the area of privacy implications of smart meters being imposed upon consumers without their consent. Additionally, a certain level of technical expertise is required to fully appreciate the capabilities of smart grid technology, and to that extent, the Author's technical background provides more insight than might be possible from any number of attorneys who would not have such background. Once this document is linked to the website at http://skyvisionsolutions.org/, then attorneys, concerned citizens, and others, are free to review it, criticize it, and make use of it in any way that may be helpful to them. If the Author is provided constructive criticisms or suggestions, the document could be adjusted or revised as appropriate.

To fully develop the invasion of privacy argument, we will go through a number of stages to reach the final conclusion. Think of this as a journey in search of the "truth," presented in what will hopefully be a rational and objective manner.

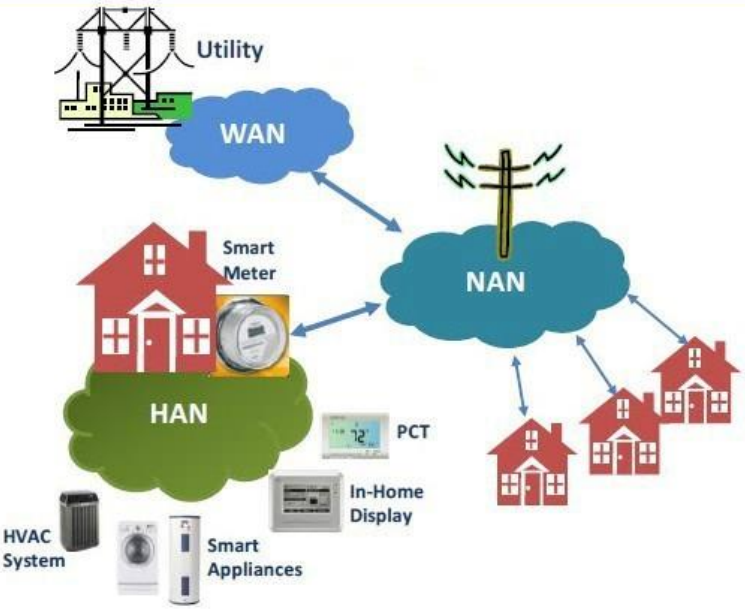
What Are Smart Meters?

Just to be thorough, let us first begin by defining smart meters. According to a description provided by the Edison Electric Institute (EEI)*:

> "Smart Meters are electronic measurement devices used by utilities to remotely communicate information for billing customers and operating their electric systems."
>
> "The combination of the electronic meters with two-way communications technology for information, monitor and control is commonly referred to as Advanced Metering Infrastructure (AMI). Previous systems which utilized one way communication and were referred to as AMR (Automated Meter Reading) Systems. AMI has developed over time, from its roots as a meter reading substitute (AMR) to today's two-way communication and data system."
>
> "Smart Meters collect [granular energy-related] data locally and [generally] transmit via a [Neighborhood Area Network (NAN)] to a data collector. … The collector retrieves the data and may process it or simply pass it on for processing upstream. Data is transmitted via a Wide Area Network (WAN) to the utility central collection point for processing and use by business applications. Since the communications path is two way, signals or commands can be sent directly to the meters, customer premise or distribution device."
>
> [* Reference: "A Discussion of Smart Meters and RF Exposure Issues," An EEI-AEIC-UTC White Paper, March 2011]



Most new wireless smart meters being installed in the United States and Canada contain two separate transmitters. One transmitter functions within the Neighborhood Area Network (NAN), communicating with the Utility and with other smart meters in the area. The second transmitter exists to function within a Home Area Network (HAN), communicating with "smart" appliances within an individual residence and with an in-home display unit.



Advanced Metering Infrastructure with Home Area Networking

The use of an in-home display unit with communication with other home devices for the HAN is *voluntary* on the part of the consumer for all instances known to the Author. The HAN is thus considered outside the scope of this document as we will focus on the technology that is often mandated on an involuntary basis for the collection, transmission, and retention of granular energy-related data by digital smart meters through the use of NAN and WAN communications.

However, one significant concern is that the HAN transmitter contained within a wireless smart meter might somehow become activated inadvertently or without the customer's consent, thereby transmitting real-time and extremely detailed

granular appliance-related data to anyone able to access and interpret the data transmission.

Within the context of this document, reference to "smart meters" generally refers to the measurement of consumer electrical usage data, but the same general principles can be applied for measurement of natural gas or water usage as well.

Smart Meter Data Collection Guidelines

First, it is important to establish a framework for what energy-related data should reasonably be collected by the smart meters located on customer property. As outlined in NIST Document NISTIR 7628, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid", August 2010, page 20:

> "In the current operation of the electric utilities, data taken from traditional meters consists of basic data usage readings required to create bills. Under the Smart Grid implementation, smart meters will be able to collect other types of data. … Some of this additional data may constitute personal information or may be used to determine personal activities. Because of the associated privacy risks, only the minimum amount of data necessary for services, provisioning, and billing should be collected." [emphasis added]

Additionally, in December 2012, a document was published entitled, "A Model Privacy Policy for Smart Grid Data." This document was prepared by the Vermont Law School and supported by a Department of Energy Award # DE-OE0000446. On page 1, it states:

> "It shall be the policy of the Utility to preserve the privacy of Customer personal identifying information (PII), … to the maximum extent possible. The Utility shall use all reasonable means [so that] only that PII which is reasonably necessary for the Utility to provide services to Customers is collected and retained."

On page 3, the document states:

> "Before collecting any new Confidential Information from Customers or implementing any programs or systems that automatically collect Confidential Information, the Utility shall determine what Confidential Information is reasonably necessary [emphasis added] to effectively implement Smart Grid Technology."

On page 1 of the Vermont Law School document, Confidential Information is described to ***include*** anonymous personal usage information where:

> "Anonymous personal usage data is any information that is collected, received, and/or stored by the Utility regarding the electrical demand and/or usage habits of individual Customers or small groups of Customers that, either explicitly or implicitly, reveals details, patterns, or other insights into the personal lives, characteristics, or activities of individual Customers or members of the group but which does not reveal the identity of the consumer or group from whom the information was collected. Such information shall not be considered anonymous if it contains PII or any other information from which a third party could reasonably deduce the identity of the Customer or Customers for who such data is collected."

So given the above information, it is clear that in order to acknowledge the privacy interests of the consumer, ***the bare minimum*** of information should be collected by the Utility.

It is asserted that most Utilities have *not* followed the basic common sense guidelines given above in deciding what private and/or confidential data may reasonably be collected from the customer without consent. In fact, it would appear that many Utilities are collecting as much information as smart meter technology currently can be afforded from a cost perspective with *no* regard to the consumer.

Let us progress to the next step to determine what type of information is actually being collected by smart meters and whether that information is indeed the bare minimum necessary to conduct business with the customer and for implementation of the Smart Grid. Is the Utility collecting more information than might be considered reasonably necessary?

What Data Do Smart Meters *Currently* Collect?

We must understand in more detail what types of information that a smart meter collects and how frequent it is collected. This aspect of data collection may differ somewhat from utility to utility, depending on the type of meters purchased and how they are programmed. The primary example used in this document will be for the City of Naperville, Illinois, where the Author is an electric consumer.

The basic data collection scheme for smart meters being installed in Naperville, Illinois, was explained to the Author in an e-mail message from one Naperville City Council member, dated January 12, 2012. The explanation may be somewhat simplistic, but the information shown below is considered a reasonable and revealing characterization of what actual data each Naperville smart meter monitors and *records every 15 minutes*.

From: [mailto:[City Council Member]@naperville.il.us]
Sent: Thursday, January 12, 2012 12:29 PM

Subject: Re: Smart Meter Information

The four data points are;

1 Energy delivered, measured in kWh. This is what we have historically used to bill with and will continue to do so.

2. Energy received , measured in kWh. This is the net metering side. If anyone wants to sell energy back to the grid this is how it would be measured.

3. Voltage. Knowing this we will be able to know not only when the power goes out but are we delivering to much or too little. This will be a major way for us on the utility side to better manage our system resulting in cost savings for all of us as we will minimize line-losses in distribution.

4. Volt-Amps reactive measured kW/KVA. This is basically how we measure total load on the system and will know if we need more power sent due to an increasing load. Conversely we will also use this to determine when we can shed load due to decreasing demand. This will also help us manage our transformers and extend their useful life.

... we will be measuring [these variables] in 15 minute blocks.

Data point 1 is the “energy delivered” in kWh and is described as what is used to bill the customer. Clearly for this energy delivery information, only one data point is needed per month for billing purposes, unless a customer voluntarily requests to participate in an energy control program which might include time-of-use rates, etc. Data point 2 is only applicable in cases where a customer elects to “sell energy back to the grid.”

Data points 3 and 4 are those points that the Utility desires to collect on a frequent and incremental basis in order to help manage the electrical grid system more effectively. Although these parameters do not directly relate to the data point measured for the energy consumed by the consumer for billing purposes, at least one of the data parameters affects consumer privacy as will be explained later in this document.

As an example of what type of information is collected by a smart meter, what is shown below is a small sample data stream from one Naperville smart meter for just the one parameter of “energy delivered” in kWh in 15-minute time increments. The meter identification number has been blurred for privacy reasons.

Sample Data Stream from Naperville Smart Meter
by Meter Number and Indicating Real Power Usage in 15-Minute Time Increments

METER_ID	CHANNEL_ID	READ_DTM	READ_DTM_DST	READ_VERSION	READ_VALUE	UOM
[illegible]	1	4/26/2013 0:15	4/26/2013 1:15	1	0.0522	KWH
[illegible]	1	4/26/2013 0:30	4/26/2013 1:30	1	0.0522	KWH
[illegible]	1	4/26/2013 0:45	4/26/2013 1:45	1	0.078	KWH
[illegible]	1	4/26/2013 1:00	4/26/2013 2:00	1	0.0768	KWH
[illegible]	1	4/26/2013 1:15	4/26/2013 2:15	1	0.0522	KWH
[illegible]	1	4/26/2013 1:30	4/26/2013 2:30	1	0.0522	KWH
[illegible]	1	4/26/2013 1:45	4/26/2013 2:45	1	0.0522	KWH
[illegible]	1	4/26/2013 2:00	4/26/2013 3:00	1	0.0576	KWH

All smart meters collect, record, and transmit time-stamped data similar to shown above whether it be in hourly, 15-minute, or sub-15-minute intervals. Many advanced smart meters also record and transmit other time-stamped information such as Voltage and Volt-Amps Reactive as described earlier in this section.

Are Smart Meters Even Necessary?

Before proceeding, the Author would like to challenge the straw man argument that smart meters are even a necessary part of modernizing the electrical grid, particularly with regard to collecting incremental measurements of “energy delivered” data in kWh from the consumer and whether such information has any unique value to be considered essential for Utility operation and maintenance purposes.

As documented in the Federal lawsuit of *Naperville Smart Meter Awareness vs. City of Naperville*, Document # 51-2 of Case # 11-CV-09299, page 5, the City states:

> ***"Smart meters enable real-time communication between the consumer and the utility."***

In the same Court document on page 6, the City says:

> “***Smart meters collect energy in killowatt-hours (kWh) used by customers during 15 minute intervals and transmit the data to [the Electric Department] 4-6 times per day."***

The above statements are revealing in many ways as to whether smart meters and the smart grid can ever live up to their advertised expectations. Although wireless smart meters continuously chatter with other smart grid components throughout the day, the actual data transmission of individual customer account information is stated to occur only once every 4 to 6 hours. ***This is not real-time, either for the consumer or the Utility***. Furthermore, at least for the consumer, there is typically an additional delay of several more hours before smart meter-related data would become available through an online portal.

We thus have a clear inconsistency in the statements presented in Court documents by the City of Naperville. Although smart meters collect energy-related data on an incremental basis providing both an extensive short-term and long-term record of consumer energy usage patterns, the information is not truly available on a “real-time” basis to meet advertised expectations for the Utility or consumer. This delayed availability of data by several hours significantly limits the Utility’s ability to precisely

measure energy consumption on a daily basis in 15-minute increments to meet the advertised objective of buying power more accurately in the marketplace, e.g., as stated in Court Document # 51-2 of Case # 11-CV-09299, page 7, where it states:

> ***"… we are going to now be able to more precisely measure our energy consumption on a daily basis in every 15 minutes. And we can buy our power more accurately in the marketplace."***

The above facts support the Author's assertion that incremental measurements by smart meters of energy usage in kWh (delivered) are not essential for operation and maintenance of the Utility. In fact, it can be stated that other Utility sensing networks already provide more timely, efficient, and cost-effective methods for assessing electrical grid distribution loads and conditions. It is likely impractical and overly cumbersome to envision Utilities deriving timely distribution load information by aggregating thousands (or millions) of smart meter data transmissions that occur at a frequency of once every 4 to 6 hours.

The above perspective is consistent with information contained in "Getting Smarter About the Smart Grid," a document released in 2012 where it states,

> ***"SCADA networks already provide utilities with the aggregate transformer or substation load data needed to assess distribution loads and conditions. … SCADA (System Control and Data Acquisition) is an array of communication protocols that have been employed by the utility industry for decades, primarily for substation monitoring and distribution automation purposes. … A premises meter is not needed."***

Moreover, a major U.S. Utility, Northeast Utilities (NU), recently filed a document with the Massachusetts Department of Public Utilities where NU was highly critical of a proposed plan that would require utilization of "advanced metering" or smart meters within the state of Massachusetts as part of an electrical grid modernization plan. Relevant content of the NU submittal which is in agreement with the "Getting Smarter About the Smart Grid" statements quoted above is as follows:

- *"An Advance[d] Metering System is not a 'basic technology platform' for grid modernization and is not needed to realize 'all of the benefits of grid modernization.'"*

- "In fact, there are non-metering technologies that the Companies have implemented, or can implement in the future within a grid-modernization plan, that would tangibly advance the grid-modernization objectives … For example, utilizing SCADA-enabled smart switches will both reduce outages and mitigate the effects that outages have on customers. Substation monitoring, remote controls and microprocessor relays can mitigate the impact of widespread outages; manage load constraints; and help to optimize the use of assets in ***real time***. … Therefore, it is clear that the Companies would be able to identify and implement a suite of non-meter technologies and processes, in addition to those already implemented, in order to advance the Department's grid-modernization objectives *without* the implementation of an advanced metering system." [emphasis added]

- For a more complete summary of the Northeast Utilities submittal, refer to a SkyVision Solutions article entitled, "Major U.S. Utility Says "No Rational Basis" for Mandating Smart Meters."

Based upon the information presented in this section, it is concluded that if a Utility installs smart meters to collect incremental energy usage data from consumers, then the Utility has no legitimate basis to claim that such information is essential to Utility operations and maintenance.

What Data *Should* Smart Meters Collect (if Utilized)?

In accordance with the guidelines of NIST Document NISTIR 7628 (and emphasized earlier): "Because of the associated privacy risks, only the minimum amount of data necessary for services, provisioning, and billing should be collected." It is thus the assertion of the Author that an appropriate energy-related data collection requirement as applicable to the customer would be as follows:

> One data point measured per month of energy usage in kWh (delivered) for customers with a fixed rate pricing program, for the limited business purpose of calculating a monthly bill.

To collect the specific data parameter of energy usage in kWh (delivered) more frequently than monthly is not reasonable since it not necessary for billing purposes or account management, and it is not essential for operation and maintenance of the Utility.

Any additional incremental measurements are unnecessary and constitute an invasion of privacy unless the customer consents to additional metering and voluntary energy control programs. This assertion is consistent with *In re Restraint of Maxfield*, 133 Wn.2d 332, 341 (Wash. 1997):

> "Electricity, even more than telephone service, is a 'necessary component' of modern life, pervading every aspect of an individual's business and personal life: it heats our homes, powers our appliances, and lights our nights. A requirement of receiving this service is the disclosure to the power company (and in this case an agent of the state) of one's identity and the amount of electricity being used. The nature of electrical service requires the disclosure of this information, but that disclosure is only for the limited business purpose of obtaining the service." [emphasis added]

It is acknowledged for those customers who voluntarily participate in "net metering," the Utility needs to collect readings for energy usage in kWh (received).

It is further acknowledged that most Utilities today desire to collect incremental measurements for Voltage and Volt-Amps Reactive* with the advertised goal of operations and maintenance of a smart grid and to realize the full benefits of smart grid technology.

[* *Technical Note*: *Volt-Amps Reactive, or var, is a unit used to measure "reactive power" in an AC electrical power system. Reactive power is present in an AC circuit when the voltage and current are not in phase*.]

Incremental measurements of Voltage and Volt-Amps Reactive have technical implications that are somewhat beyond the scope of this document to fully address at this time. For example, customers may not have a conceptual objection to the Utility collecting Voltage information at 15 minute (or sub-15-minute) intervals since

that data parameter by itself would not unduly affect the privacy interests of customers as long as energy usage information is ***not*** also measured and recorded at that same frequency. Energy (delivered) usage information need only be collected monthly unless otherwise agreed to by the customer.

The measurement of Volt-Amps Reactive information at 15-minute (or sub-15-minute) intervals becomes more problematic. One issue is whether currently deployed smart meters could be re-programmed to monitor for and record Volt-Amps Reactive information without also recording the associated energy usage information in kWh. As will be further explained in a later section, it is the combination of recording both the energy usage information in kWh and Volt-Amps Reactive information that can create a substantial threat to privacy. In addition, it is the Author's conclusion (based upon a review of available technical information) that the frequent collection of Volt-Amps Reactive data alone can also provide at least limited information on the frequency and types of appliance usage within a residence. However, in this area, if Utilities were willing, and if technical barriers could be overcome, there is likely a manner in which the privacy interests of consumers could be protected while still allowing the Utility to modernize its electric grid by monitoring the data parameters of Voltage and Volt-Amps Reactive.

At present, for the example in Naperville, Illinois, smart meters measure and record all four parameters mentioned above at 15-miute intervals, because, well, that is just how the meter is programmed to function. *This programming could and should be changed to more reasonably reflect the data that the Utility either needs or reasonably desires to collect*.

An Example on How Consumer Privacy Interests Have *Not* Been Considered

The widespread deployment of smart meters has resulted in serious concerns that such devices unreasonably invade the privacy of consumers. Many of the principal privacy concerns have been summarized in published literature and several of these concerns are listed in the figure provided below.

Summary of Privacy Concerns Related to Smart Meters

Application Group	Example Concern	References
Illegal Uses	Burglars finding out when homes are unoccupied. Stalkers tracking the movements of their victims.	(Lisovich et al., 2010; Quinn, 2009; Cavoukian et al., 2010; McDaniel, 2009; Lerner and Mulligan, 2008; Subrahmanyam, 2005)
Commercial Uses	Targeted advertising: use of individual or aggregated household smart meter data to target advertising at a specific household or individual. *Note*: Use of aggregated or 'anonymous' data may be more acceptable than use of individual household data. Insurance adjusting e.g. do you tend to leave your appliances on when away from home?	(Lisovich et al., 2010; Quinn, 2009; Cavoukian et al., 2010; McDaniel, 2009; Anderson and Fuloria, 2010; Bohli et al., 2010)
Uses by law enforcement agencies	Detection of illegal activities e.g. sweatshops, unlicensed commercial activities, and drug production. Verifying defendant's claims e.g. that they were 'at home all evening'.	(Lisovich et al., 2010)
Uses by other parties for legal purposes	In a custody battle: do you leave your child home alone? In a landlord–tenant dispute: is the property over-occupied?	(Quinn, 2009)
Use by family members and other co-inhabitants	One householder 'spying' on another e.g. parents checking if their children are sleeping or staying up late playing video games. Partners investigating each other's behavior.	(Hargreaves et al., 2010)

Source: Table 1 of "Smart Meter Data: Balancing Consumer Privacy Concerns with Legitimate Applications," McKenna, et. al., *Energy Policy*, 41 (2012) pp 807-814.

As a general rule, the ability to discern occupancy and specific activities from smart meters depends on the time resolution of the energy consumption data collected. Daily readings would generally enable one to determine dwelling occupancy over

time. As the data collection intervals are further reduced, a load profile is revealed that allows determination of general movement and activities within a dwelling on an hour by hour basis. With further increased granularity of the data, usage of individual appliances within a dwelling can be identified. For example, as indicated on page 14 of NIST Document NISTIR 7628, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid," research shows that analyzing 15-minute interval household energy consumption data can by itself pinpoint the use of most major home appliances.

As has already been established, it is essential that the amount of data collected by smart meters be limited to the ***bare minimum*** necessary to accomplish Utility objectives.

Based upon the above information, it evident that the privacy interests of the consumer must be properly considered *before* a Utility can move forward with its goal to enhance its electrical grid operations. This consideration would require that a *privacy impact assessment* be performed where a Utility would consciously, thoughtfully, and methodically ensure that the data collection capabilities of a smart meter did not unreasonably infringe on the privacy expectations of the consumer. Was such a *privacy impact assessment* performed for the City of Naperville's implementation of its smart grid initiative? Evidently not based upon the paragraphs that follow.

As documented in the Naperville Federal lawsuit, (Document # 51-2 of Case # 11-CV-09299 pp 21, 22), please review the following verbal exchange regarding smart meter data collection frequencies:

> COURT: "Is there a reason why the 15-minute unit time was chosen as opposed to daily or — … weekly?"

> CITY: "Yes. … we chose the 15-minute interval because of our overall program and our — our need to be able to determine our energy usage on a more accurate basis for purposes of buying our power out in the marketplace. And so that when we buy our power, we buy it more accurately."
>
> COURT: "Okay. With regard to — let's put it this way: Is there magic as to 15 minutes as opposed to an hour, as opposed to 30 minutes, as opposed to five minutes?"
>
> CITY: "Your Honor, we chose 15 minutes as – it was a balance between the meters' memory capacity, cost of the meters, and the resolution that we would have liked to obtain information where we could lower demand and provide cost savings." [emphasis added]
>
> COURT: "In other words, you could have bought meters that sent off information every five minutes, but they would have been more expensive?"
>
> CITY: "That's correct, your Honor. More expensive, or we could retain less than the amount of information that we needed inside the meter."

As you can see from the Court proceedings, there is ***no*** indication that the privacy interests of the individual were even *remotely* considered in determining the data collection capabilities of the smart meter. In fact, if it were not for cost considerations, there is an implication that the City may have purchased meters configured to collect electrical usage data even more frequently than the current 15-minute interval … resulting in even greater privacy invasions for consumers.

So rather than considering the privacy interests of consumers prior to moving ahead with the City's goal to enhance its electrical grid operations, the City formally stated in a Court of law that the current 15-minute smart meter data collection interval was a "balance" between such factors as memory capacity and cost. There was no mention of customer privacy as a consideration. As such, the City has failed to follow the basic common sense guidelines presented at the

beginning of this document in deciding what private and/or confidential data may reasonably be collected from the customer without consent.

To summarize for this "real-life" example, the City of Naperville and its municipally owned utility have failed to properly consider the privacy interests of its customers.

Why Is Collected Smart Meter Data an Infringement on Privacy?

Now that the nature of data collected by Utility smart meters has been clarified, and it has become clear that the privacy interests of consumers have not been properly considered, additional evidence will be presented on how granular and incremental energy-related information represents an unreasonable invasion of privacy. All of this information is from credible sources.

As summarized by the Congressional Research Service (CRS) report entitled, "Smart Meter Data; Privacy and Cybersecurity," Feb. 2012, page 3, the principal privacy and security concerns surrounding the installation of residential smart meters are:

> "(1) privacy concerns that smart meters will reveal the activities of people inside of a home by measuring their electricity usage frequently over time [(i.e.,] Data that offers a high degree of detail is said to be 'granular[,"] and
>
> (2) fears that inadequate cybersecurity measures surrounding the digital transmission of smart meter data will expose it to misuse by authorized and unauthorized users of the data."

Also, as stated in NIST Document NISTIR 7628, p 9,

> "Energy consumption patterns have historically not risen to the level of public concern given to financial or health data because (1) electrical meters had to be physically accessed to obtain usage data directly from buildings, (2) the data showed energy usage over a longer time span such as a month and did not show usage by specific appliance, and (3) the utilities were not sharing this data in the ways that will now be possible with the Smart Grid.

> Public concerns for the related privacy impacts will likely change with implementation of the Smart Grid, because energy consumption data can reveal personal activities and the use of specific energy using or generating appliances, and because the data may be used or shared in ways that will impact privacy." [emphasis added]

Furthermore, as stated in NIST Document NISTIR 7628, page 11:

> "[T]he Smart Grid significantly expands the amount of data available in more granular form as related to the nature and frequency of energy consumption and creation, thereby opening up more opportunities for general invasion of privacy. Suddenly a much more detailed picture can be obtained about activities within a given dwelling, building, or other property, and the time patterns associated with those activities make it possible to detect the presence of specific types of energy consumption or generation equipment. Granular energy data may even indicate the number of individuals in a dwelling unit, which could also reveal when the dwelling is empty or is occupied by more people than usual." [emphasis added]

As stated in NIST Document NISTIR 7628, pages 13 and 14:

> "… Because smart meters collect energy data at much shorter time intervals than in the past (in 15-minute or sub-15-minute intervals rather than once a month), the information can reveal much more detailed information about the activities within a dwelling or other premises than was available in the past. This is because smart meter data provides information about the usage patterns for individual appliances—which in turn can reveal detailed information about activities within a premise through the use of nonintrusive appliance load monitoring (NALM) techniques…. For example, research shows that analyzing 15-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances. … NALM techniques have many beneficial uses, including pinpointing loads for purposes of load balancing or increasing energy efficiency. However, such detailed information about appliance use can also reveal whether a building is occupied or vacant, show residency patterns over time, and reflect intimate details of people's lives and their habits and preferences inside their homes." [emphasis added]

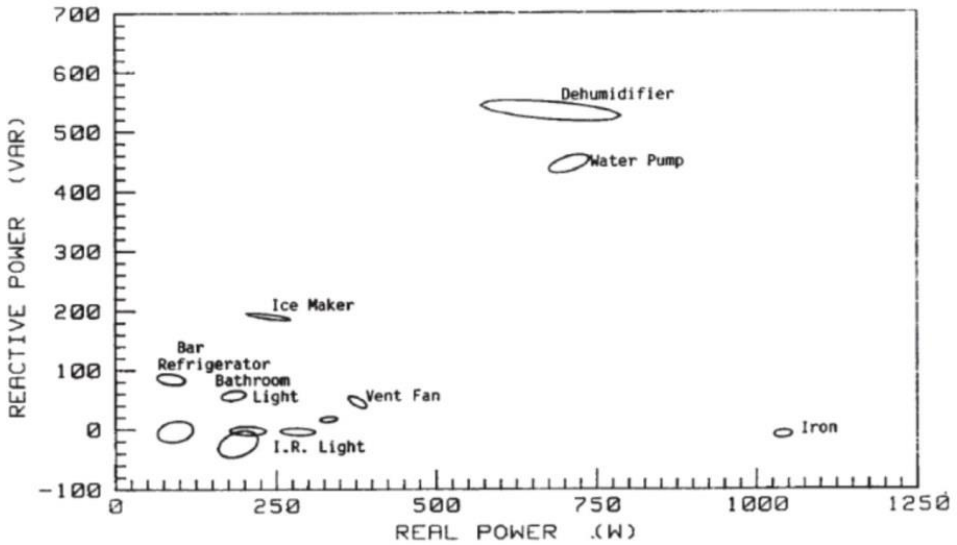
To further explain the nature of what is meant by non-intrusive appliance load monitoring (NALM), selected quotes will be provided from an article entitled,

"Compressive Sampling for Non-Intrusive Appliance Load Monitoring (NALM) Using Current Waveforms," dated June 2012, and published by ACTA Press:

> "The non-intrusive appliance load monitoring (NALM) is a convenient approach to determine the energy consumption of individual appliances. The NALM employs only a single point of measurement, e.g., at the main electrical service entry point of the home, which does not require installing meters on each individual appliance. The NALM monitors the voltage and current of the total load and derives the activity of the individual appliances which constitute the load. Each appliance has electrical features that can be used as a unique 'signature' to recognize its contribution in the overall consumption. **The most well developed NALM technique utilizes the signature given by the real and reactive power of the appliance** during its steadystate operation." [emphasis added]

Thus, collection of smart meter data for the parameters of both real and reactive power in combination with a backend computer analysis can reveal individual appliance signatures. Refer to the figure below for a somewhat simplistic and conceptual illustration of how appliances have "signatures."

Illustration on How a Combination of Real Power and Reactive Power Readings Can Reveal Appliance Signatures

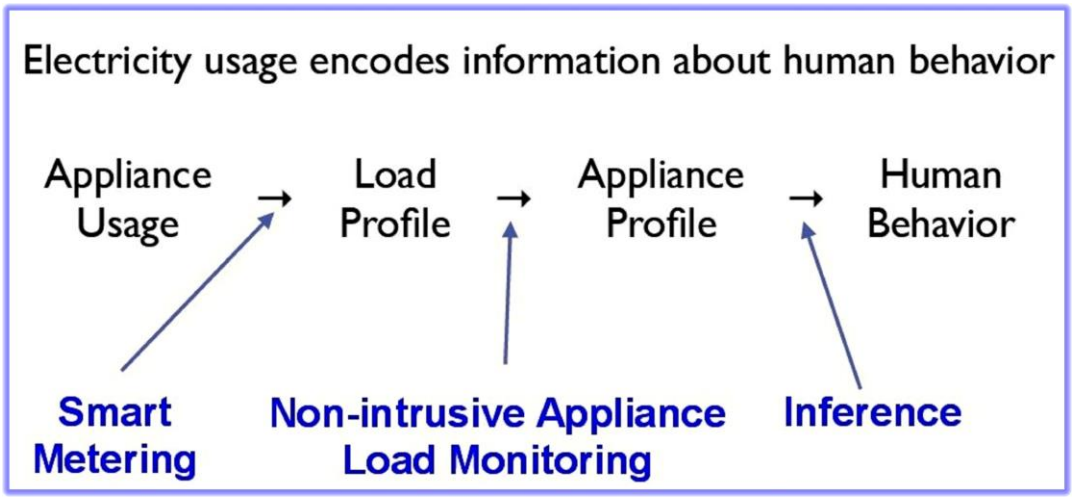


Source: "Non-intrusive Appliance Load Monitorng (NIALM): Promise and Practice, Zeifman & Roth, Fraunhofer USA, March 2012

So this is where we arrive at a situation where we can clearly disprove Utility simplistic claims that smart meters "only record total energy usage for the home, just like current analog meters." In fact, smart meters record much more granular information than analog meters, and furthermore, many new smart meters record information beyond the real power usage required to calculate monthly bills. Specifically, many new smart meters like those in Naperville, Illinois, also record granular data for what is referred to as "reactive power." As stated in the above referenced article, specific appliance use can be identified based upon unique signatures created by a combination of monitoring and analyzing a home's energy-related data that contains both the **real** and **reactive power** parameters.

In fact, the Author of this document when discussing smart meters, to be more precise, generally refers to smart meters as collecting, recording, and transmitting **energy-related data**, not just **energy *usage* data**.

In the Naperville, Illinois, and elsewhere, most new smart meters collect energy-related data in hourly, 15-minute increments, or even more frequently. Based upon the information presented above, it is clear that "behavioral privacy*" is at risk due to the use of smart meters. This can be figuratively shown as follows:



* As defined by NIST Document NISTIR 7628, page 6, behavioral privacy is "the right of individuals to keep any knowledge of their activities, and their choices, from being shared with others."

Referencing another document, according to a 2009 report prepared for the Colorado Public Utilities Commission, entitled, "Smart Metering & Privacy: Existing Law and Competing Policies," page v, it was stated that "insufficient oversight of this [smart metering] could also lead to unprecedented invasions of consumer privacy. Many intricate details of household life can be gleaned from information obtained via advanced metering infrastructure." [emphasis added]

Additional select quotations from the above referenced document are as follows:

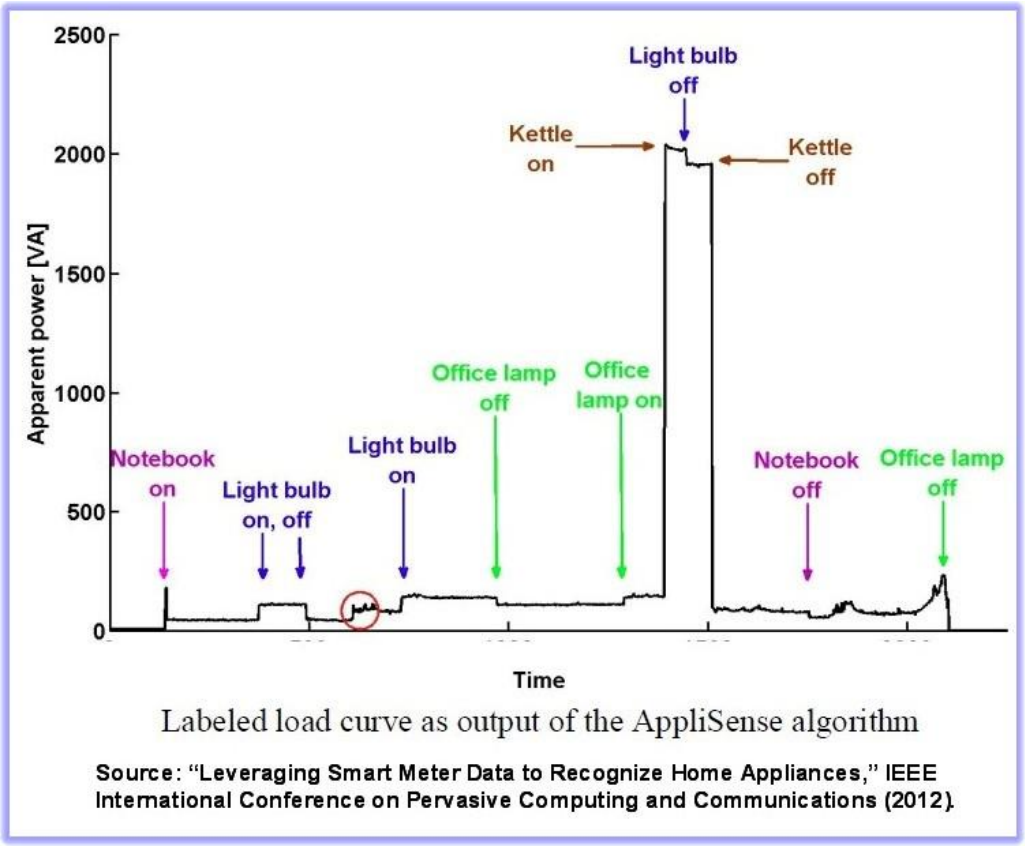
> From page 3: "An Italian study published in 2002 used fifteen-minute interval data -- the same resolution collected by most smart meters today -- to identify heavy-load appliance uses within an electricity usage profile. Researchers there were able … to pinpoint the use [of] washing machines, dishwashers, and water heaters with accuracy rates of over 90 percent from within the noise of the aggregated load information."
>
> From page 9: "[T]he massive deployment of smart meters across the country and the trend toward finer and finer interval data means that more and more information will be discernable about more and more people. While the raw information about when an appliance event occurred in a given home may not seem to be sensitive information, it could be used to construct a detailed picture of residential life."
>
> From page A-5: "A remarkable number of electric appliances can be identified by their load signatures, and with impressive accuracy. Researchers have all but mastered identification of the larger common household appliances such as water heaters, well pumps, furnace blowers, refrigerators, and air conditioners, with recognition accuracies approaching perfection. Ongoing work focuses now on the myriad smaller electric devices around the home such as personal computers, laser printers, and differentiating [types of] light bulbs."
>
> From page A-9: "What's more, the sheer volume of the research and development in this area helps understand the field as a vector, one that points directly at more and more-detailed information collected concerning the activities of millions of people. While the motivations for this aggregation of data may be noble, the potential for serious privacy invasion is only growing, and so the need for care."

The identification of devices utilized in the home is becoming a for-profit business industry. Many Utility customers do not want to risk participation in such behavioral profiling activities, even inadvertently, in order to preserve behavioral privacy. To

provide an example of load profiling, a recent published article, entitled, "Leveraging Smart Meter Data to Recognize Home Appliances," was presented at the IEEE International Conference on Pervasive Computing and Communications in 2012. Excerpts from the article state the following:

> "The worldwide adoption of smart meters that measure and communicate residential electricity consumption gives rise to the development of new energy efficiency services. Several particularly promising applications involve the disaggregation of individual appliances within a particular household in terms of their energy demand. … We generated 144 device-switching events in our test scenario. 16 of these came from devices with a consumption so small that the filter canceled out the corresponding edges. When subtracting these events, the algorithm identified 125 out of the remaining 128 events correctly, which results in an overall recognition rate of about 90%. … we are considering methods to derive occupancy state from electricity and appliance use data, [emphasis added] in order to use this information in a smart heating control strategy."

One of the figures included with the article is shown below:



Labeled load curve as output of the AppliSense algorithm

Source: "Leveraging Smart Meter Data to Recognize Home Appliances," IEEE International Conference on Pervasive Computing and Communications (2012).

The above figure represents power versus time, showing step changes due to individual appliance events. This is an example of the type of information that can be gleaned from non-intrusive appliance load monitoring (NALM). The display of the type of load profile information in the above figure was *not possible* with month to month utility readings.

Even *without* the somewhat sophisticated approach of using non-intrusive appliance load monitoring (NALM) techniques, another report published in 2010 shows that analyzing just household real power readings *alone* is sufficient to reveal a range of information, such as when people are at home, sleeping routines, eating routines, etc. The report is entitled "Private Memoirs of a Smart Meter," was prepared by members of the Department of Computer Science, University of Massachusetts Amherst, Here are some selected quotations from the report:

> "In this paper, we argue that the widespread deployment of smart meters has serious privacy implications since they inadvertently leak detailed information about household activities. The information leaks directly correlate with the time granularity that a meter measures power consumption. Unlike traditional dumb meters that record aggregate monthly usage for a utility, today's smart meters allow [a] utility, or a malicious party, to glean detailed information about household activity in real-time from fine-grained usage measurements. Further, research on non-intrusive load monitoring (NILM) has shown that it is possible to disambiguate individual appliance usage from an aggregate smart meter power trace by using prior knowledge of an appliance's power signature. Such techniques reduce or eliminate the need for outlet- or appliance-level meters, since they are able to extract detailed usage information for individual appliances from an aggregate household power trace. We show that even ***without*** detailed knowledge of appliance signatures a priori or prior training, it is possible to extract complex usage patterns from smart meter data using off-the-shelf statistical methods. [emphasis added] Our methods are able to label specific types of activity in the home over time based on a number of characteristics, including the level of power consumption, its intermittency, and its duration. … [W]ith our limited data, we argue that it is possible to infer detailed information about household activity -- questions such as how many people are in a home at a given time and whether a resident went out for dinner on a particular evening, for example." [emphasis added]

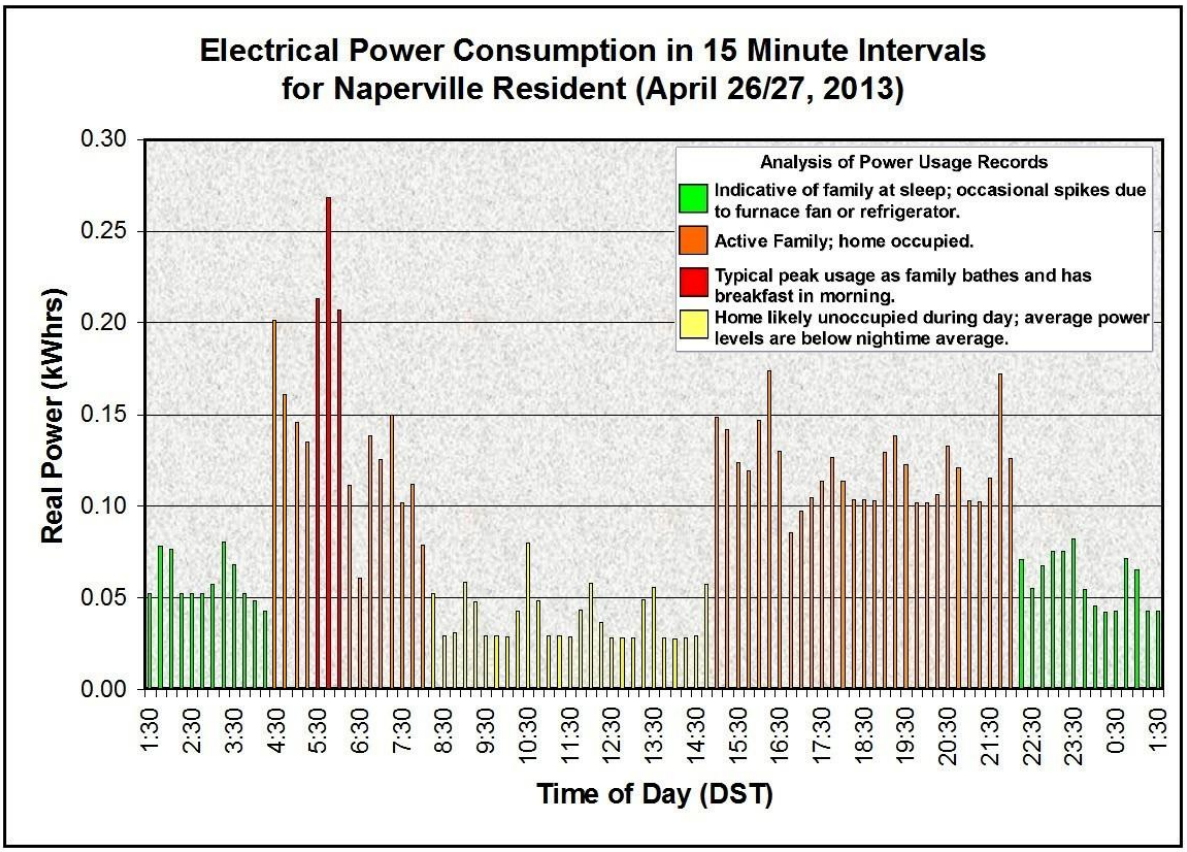
Thus, even *without* specific appliance use identification made possible through using non-intrusive appliance load monitoring (NALM) techniques, considerable information on human behavior or home occupancy can be gleaned by simply reviewing a graph of power usage versus time over the course of any given day.

In the next section, the Author will present specific "real-life" examples on how human behavior or home occupancy can be determined by reviewing consumer load profile information *without* the use of any special software algorithms or analysis techniques.

Specific Examples on How Smart Meters Reveal Household Activities

Over the past year, the City of Naperville and its municipally owned utility have installed smart meters for nearly all residents. In an attempt to resolve some concerns related to the City no longer documenting "current" and "previous" electrical usage meter readings on monthly bills, one resident sent the City of Naperville a Freedom of Information Act (FOIA) request in an attempt to obtain this information for her account. What she received back was a month's worth of 15-minute interval usage amounts in kWh.

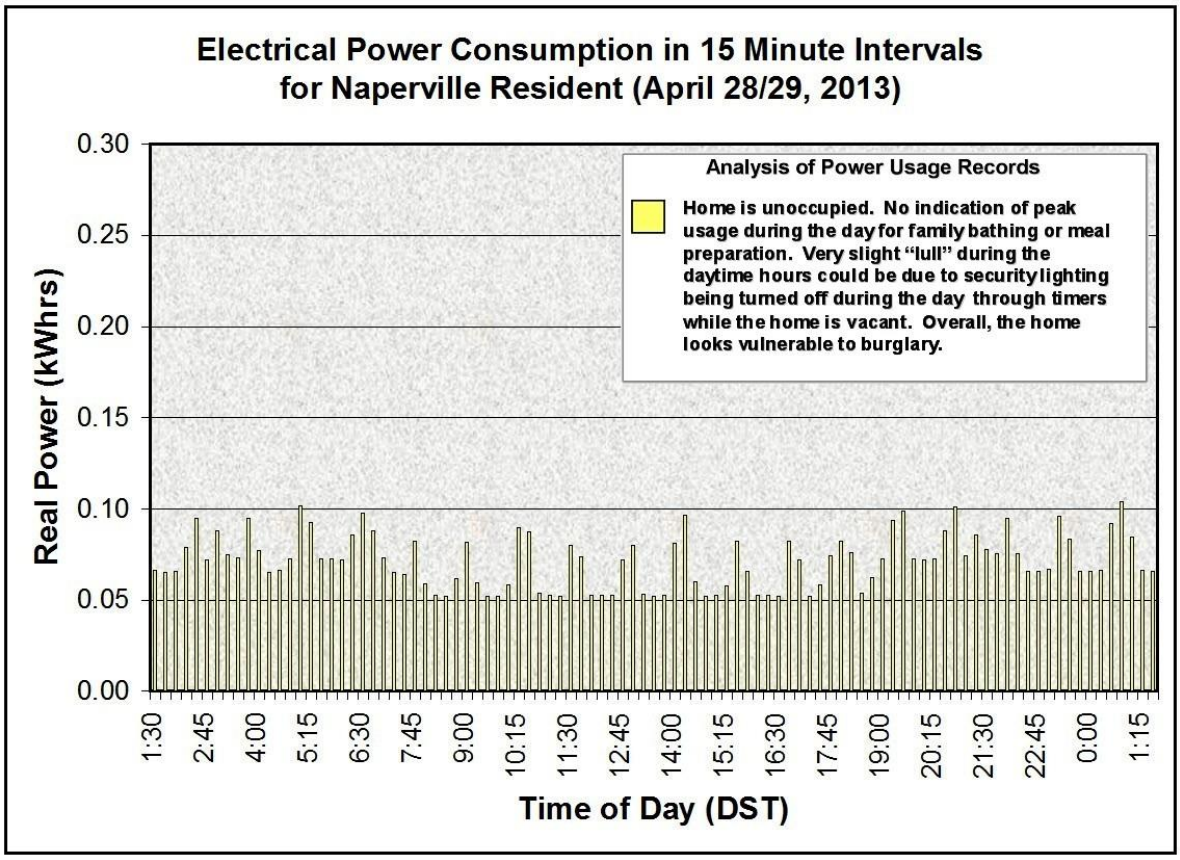
As an example of load profile information, the 15-minute interval usage numbers for April 26, 2013, were graphed as shown in the figure below (next page). Without any special software or analysis, it is quite easy to infer human behavior from the graph. It is clear that people in the family arose at 4:30 am and started their day with the typical activities of bathing and meal or coffee preparation. From this graph one cannot determine exactly what appliance is being used when, but the graph clearly reveals discrete human activity. It is also clear that there is little or no human activity from about 8:30 am until 3:00 pm. You can also see how the usage readings abruptly drop off at 10:15 pm indicating that the family is retiring for the evening.



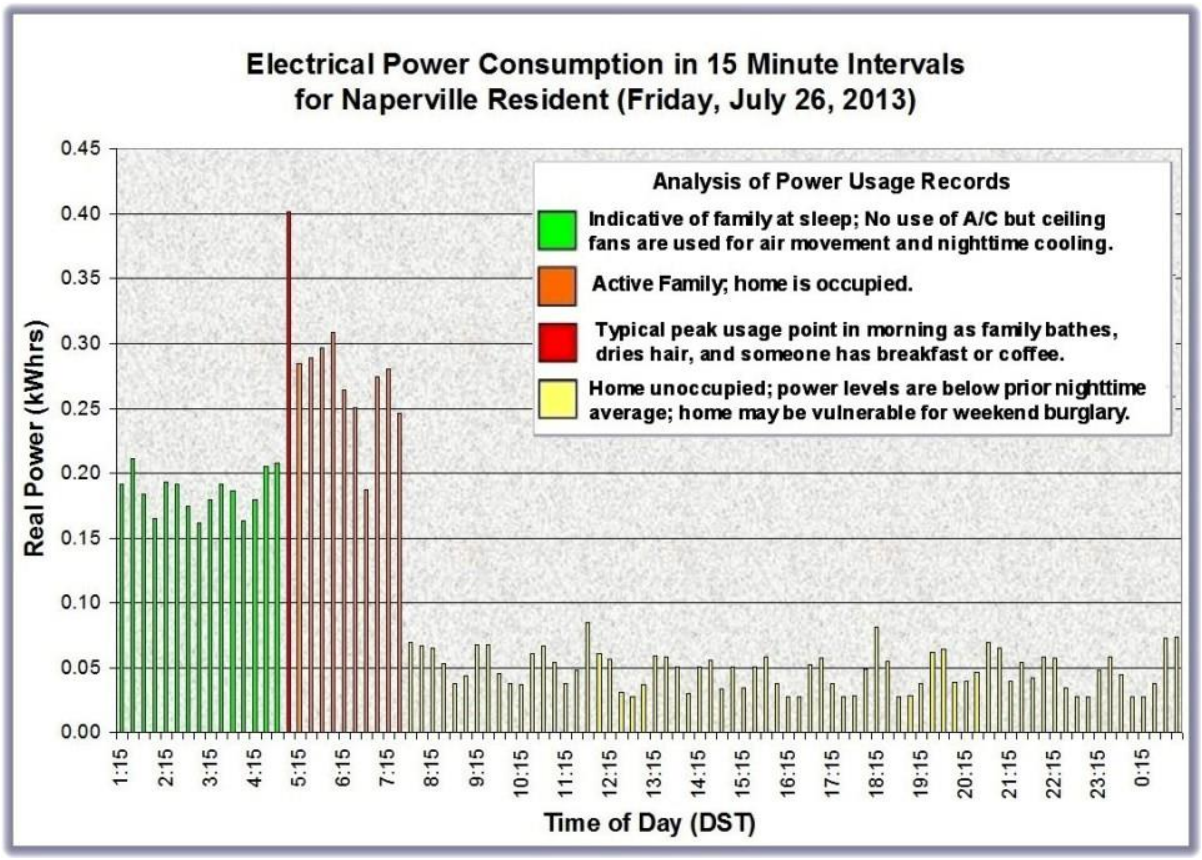
For many informed consumers, the type of information (as shown above) is exactly what they do *not* want other people to have in their possession. They don't want other people to be able to discern when they get up in the morning or when they go to bed. When people go on vacation, they don't want the ability for other people, no matter *who* they are, to be able to tell when (or confirm when) the house is either occupied or unoccupied. The *unnecessary* collection of the above information and data is considered by many as a clear invasion of privacy and a threat to both personal security and the security for the home and property.

Let's select a different day of April 28, 2013, for the same Naperville resident. Refer to the figure on the next page. See the difference? The home is unoccupied. There are no characteristic peak energy usage readings. What you see is a levelized load with intermittent peaks associated with a refrigerator and probably one

other appliance. It doesn't take a rocket scientist to discern that the home is now unoccupied and is more vulnerable to having an undetected burglary take place.



Let us look at one more example. The graph presented on the next page shows actual smart meter data for Friday, July 26, 2013, for a residence in Naperville, Illinois. This "real life" example of an electrical usage profile is fairly basic and should allow anyone to properly surmise the activities and occupancy status for this home. The family was asleep during the early morning hours of July 26 until about 4:45 am when there is then a spike in energy usage. The family was not using air conditioning due to the reasonably cool summer weather being experienced during this time period. Ceiling fans were used for night-time air movement and cooling. The family members arose to go through a morning routine of bathing and getting dressed, etc., and were out of the house by 7:30 am. ***Family members did not return home for the remainder of the day or evening***.



What is the significance of the information displayed in the above graph? *The above information in the hands of the "wrong" people could be used for purposes of surveillance in terms of when to best plan a robbery, targeted home invasion, or burglary*. There is a good chance the homeowners have gone on a weekend trip and won't be back for a couple of days. The smart meter data essentially advertises the fact that the home is now vulnerable for a successful weekend burglary. The utility counter-argument for the above concern would likely be that your records are safe with them and you don't need to worry. How comforting is that with the type of threat information presented in this document? The main point at this juncture is, "***Why take the unnecessary risk***"? There is no justifiable reason for a Utility to collect thousands of data points for incremental energy usage in order to bill each customer for monthly service.

Keep in mind that the behavioral inferences and home occupancy in Naperville, Illinois were determined with no special software algorithms or consideration of the "reactive power" energy-related parameter also measured by Naperville smart meters every 15 minutes. With backend computer analysis and data reviewed over a longer time period, additional behavioral determinations could be made.

Based upon the evidence presented in the previous paragraphs from credible information sources and "real-life" example situations, it has been established that collection of the granular and incremental energy usage information exposes the customer to unnecessary risks for invasion of privacy. The risks are unnecessary in large part due to the fact that such data collection is not required for billing purposes and is not essential for utility operations and maintenance. Informed consumers can have an informed debate on how significant the above risks are in terms of privacy and data security, etc. To some extent, it is unknown. However, there can be no doubt that at least some risks exist and that the risks could actually be quite significant. An invasion of privacy with possible infringement of Constitutional rights occurs when the residential electric customers are prohibited from providing informed consent for the unnecessary additional risks to be incurred.

Another even simpler invasion of privacy mechanism may involve smart meters installed on multiple building units or apartments. Landlords may be able to access another resident's smart meter data in cases where the resident is a "consumer" but not a Utility "customer." For example, a landlord could directly access a tenant's smart meter information through an online portal website and use it to observe tenant electrical usage patterns and behavior. Hypothetically, a landlord and possibly other "management" personnel could use information obtained from smart meter data to determine whether the tenant has broken a lease provision or for other more malicious purposes. A form of cyber stalking could thus occur without anybody actually needing to "hack" into Utility accounts. The Utility would likely claim that it

has no concern or control over such activities, yet the Utility is installing the technology that allows this avenue of privacy invasion to occur.

Peer Reviewed Literature on Cyber and Data Security Threats

When faced with questions dealing with the security of smart meter data, Utilities typically respond with statements like: "The data recorded by your smart meter is encrypted and transmitted to the Utility via a secure wireless network." Despite these all encompassing reassurances, a review of peer reviewed literature reveals a different story, one which fully substantiates consumer concerns. What follows are selected statements from the peer-reviewed journal "*International Journal of Renewable Energy and Smart Grid (IJRESG)*." Last year, the Author received permission from the publisher to publicly display *selected quotations* from smart grid-related articles contained in the journal provided that said Works are each identified by title and as articles published by ETP, Engineering and Technology Publishing. Articles in this instance were from the *IJRESG* journal, Vol. 1, No. 1, from September 2012. What follows are selected quotations from three (3) published articles demonstrating that cyber and data security threats to the consumer and to the smart grid are very real and not easily remedied. In fact, according to the Berkshire-Litchfield Environmental Council (BLEC): "The smart grid/metering creates security vulnerabilities that never existed with the old hardened utility grid in large part due to new IT connectivity. The problems are inherent to its very wireless design in a way that better encryption alone cannot fix. The smart grid as currently designed cannot be made safe from cyberattack, according to many experts."

[Reference: See article at http://wp.me/p3nav9-RL related to the BLEC.]

Quotations from Article #1: "Smart Grid Security: Threats, Vulnerabilities and Solutions"

"Smart grid network … vulnerabilities might allow attackers to access the network, break the confidentiality and integrity of the transmitted data, and make the service unavailable. … the following vulnerabilities are the most serious in smart grids:

1) *Customer security*: ***Smart meters autonomously collect massive amounts of data and transport it to the utility company, consumer,***

and service providers. This data includes private consumer information that might be used to infer consumer's activities, devices being used, and times when the home is vacant. [emphasis added]

2) *Greater number of intelligent devices*: A smart grid has several intelligent devices that are involved in managing both the electricity supply and network demand. These intelligent devices may act as attack entry points into the network. Moreover, the massiveness of the smart grid network (100 to 1000 times larger than the internet) makes network monitoring and management extremely difficult.

3) *Physical security*: Unlike the traditional power system, smart grid network includes many components and most of them are out of the utility's premises. This fact increases the number of insecure physical locations and makes them vulnerable to physical access.

4) *The lifetime of power systems*: Since power systems coexist with the relatively short lived IT systems, it is inevitable that outdated equipments are still in service. This equipment might act as weak security points and might very well be incompatible with the current power system devices.

5) *Implicit trust between traditional power devices*: Device-to-device communication in control systems is vulnerable to data spoofing where the state of one device affects the actions of another. For instance, a device sending a false state makes other devices behave in an unwanted way.

6) *Different Team's backgrounds*: Inefficient and unorganized communication between teams might cause a lot of bad decisions leading to much vulnerability.

7) *Using Internet Protocol (IP) and commercial off-the- shelf hardware and software*: Using IP standards in smart grids offer a big advantage as it provides compatibility between the various components. However, devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service, and others.

8) *More stakeholders*: Having many stakeholders might give raise to a very dangerous kind of attack: insider attacks."

"The just mentioned vulnerabilities can be exploited by attackers with different motives and expertise and could cause different levels of damage to the

network. Attackers could be script kiddies, elite hackers, terrorists, employees, competitors, or customers. [Attackers can be grouped as]:

1) Non-malicious attackers who view the security and operation of the system as a puzzle to be cracked. Those attackers are normally driven by intellectual challenge and curiosity.

2) Consumers driven by vengeance and vindictiveness towards other consumers making them figure out ways to shut down their home's power.

3) Terrorists who view the smart grid as an attractive target as it affects millions of people making the terrorists' cause more visible.

4) Employees disgruntled on the utility/customers or ill-trained employees causing unintentional errors.

5) Competitors attacking each other for the sake of financial gain."

"***The massiveness of the smart grid and the increased communication capabilities make it more prone to cyber attacks***. [emphasis added] Since the smart grid is considered a critical infrastructure, all vulnerabilities should be identified and sufficient solutions must be implemented to reduce the risks to an acceptable secure level."

For more information on the above article, refer to the following link:

http://smartgridawareness.org/privacy-and-data-security/smart-grid-vulnerabilities-a-more-detailed-review/smart-grid-security-threats-vulnerabilities-and-solutions/.

Quotations from Article #2: "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures"

"In this paper, we structure the analysis on threats and vulnerabilities in three tiers:

- **Tier 1:** deals with threats to electric appliances, smart meters and their uplink to concentrator nodes. This part is often referred to as the 'last mile' and is considered as most vulnerable to attacks due to the physical accessibility of devices.

- **Tier 2:** deals with vulnerabilities of the uplink from smart meters over concentrator nodes to data centers and interfaces to Web-based applications.

- **Tier 3:** deals with Web-based applications and value-added services that use gathered meter data."

"*Integrity* of reported energy consumption data is of paramount importance since this information is used for accounting and billing. Numerous possible frauds need to be prevented, such as a customer sends tampered meter data in order to pay less; or make someone else to pay more. Thus, manipulation of the smart meter itself or injection of tampered messages in the network must be avoided (or at least detected and compensated). Furthermore, injecting wrong status messages in the communication network might cause problems in the net management, e.g., reporting overload messages might urge the utility company to reshape the power grid's structure."

"Tier 1: Smart Meter Vulnerabilities

Smart meter vulnerabilities are exploited by attacks to the smart meter (device) itself and/or its interfaces in several ways, either by (i) manipulating the hardware, (ii) manipulating the firmware, or (iii) exploiting limitations design and implementation."

"Tier 2: Utility Vulnerabilities

First, a meshed NAN [neighborhood area network] connects smart meters in a peer-to-peer fashion, thus even devices in different houses can communicate with each other. This model foresees neighboring devices as relays if no direct uplink to a concentrator node is available. This model is often assumed when assessing smart grid security, since it would easily enable viruses and worms to spread, and thus a vast field of potential attack strategies. But actually, second, strictly hierarchical topologies are more likely to be implemented, where a meter can report to only one predefined concentrator node and avoids direct communication with other meters."

"***Recently, [the] possibility of spreading worms in a smart grid with a peer-2-peer topology [has been demonstrated]. This would effectively allow an attacker to take over a larger amount of smart meters similar to Internet worms which install backdoors on PCs. Controlling a large-scale 'smart meter botnet' would enable attackers to cause wide-range harm.*** [emphasis added] For instance, sending coordinated fabricated grid overload status messages from numerous devices could prompt the utility to shut down certain

segments of the grid to avoid local overloads. In another scenario, forcing thousands of smart meters to turn off and on simultaneously could cause major trouble due to quickly changing load conditions on the power grid."

"Tier 3: Web Application Vulnerabilities

Basically, attacks on the Web application level will either aim at disrupting meter reading management services or stealing metering data in order to derive higher level information, such as individual consumption profiles. Thus, typical threats are not only the unavailability of services through (D) DoS attacks, but also threats to privacy through user behavior profiling. Aggregating and correlating smart meter readings allows the construction of detailed user profiles which is interesting information, for instance, for advertisement. ***It is essential to support the creation of trust relations between customers and utility providers by establishing transparent billing processes and traceable pricing, as well as informing customers about stored data (personally identifiable information). Nevertheless, appropriate countermeasures, such as anonymization and pseudonymization techniques for metering data need to be employed to prevent misuse from the beginning***. [emphasis added] Notice, that the data backend will make use of a wide variety of standard server software and technology. Thus, this layer is generally vulnerable to all broadly applied server attacks against particular products and versions."

For more information on the above article, refer to the following link:

http://smartgridawareness.org/privacy-and-data-security/smart-grid-vulnerabilities-a-more-detailed-review/a-survey-on-threats-and-vulnerabilities-in-smart-metering-infrastructures/.

Quotations from Article 3: "Security Is Not Enough! On Privacy Challenges in Smart Grids"

"… two issues are widely unsolved: (i) There is no consensus what data can potentially compromise a customer's privacy and to which degree. While for some types, such as individual fine-grained meter readings, it is more obvious, for others it is not. (ii) ***Even the most sophisticated technical and organizational measures to protect sensitive data cannot guarantee the privacy protection in case of successful malicious attacks to the storage backend, e.g., carried out by a disgruntled employee***." [emphasis added]

"An illustrative example of smart meter data exploitation is given in a recent NIST report. Here, the authors impressively demonstrate how electric appliances leave special marks on the wire that can be tracked to learn about used devices

and thus infer people's habits. There are various parties who are particularly interested in meter readings; however, besides legitimate organizations using the data for billing or network services, many other use cases are not desirable, as summed up by Table 1. …

Table 1. Exploitation opportunities for smart metering data

Who wants smart meter data?	How could the data be used?
Utilities	To monitor electricity usage and load; to determine bills
Electricity usage advisory companies	To promote energy conservation and awareness
Insurance companies	To determine health care premiums based on unusual behaviors indicating illness
Marketers	To profile customers for targeted advertisements
Law enforcers	To identify suspicious or illegal activity
Civil litigators	To identify property boundaries and activities on premises
Landlords	To verify lease compliance
Private investigators	To monitor specific events
The press	To get information about famous people
Creditors	To determine behavior that might indicate creditworthiness
Criminals	To identify the best times for a burglary or to identify high-priced appliances

A list of potential consequences when privacy in Smart Grid systems is compromised includes: identity theft, determining personal behavior patterns, determining specific appliances used, performing real-time surveillance, revealing activities through residual data, ***targeted home invasions*** [emphasis added] (latch key children, elderly, etc.), providing accidental invasions, activity censorship, decisions and actions based upon inaccurate data, profiling, unwanted publicity and embarrassment, tracking behavior of renters/leasers, behavior tracking (possible combination with personal behavior patterns), or public aggregated searches revealing individual behavior. ***Some of these threats have been studied extensively, such as behavior profiling***." [emphasis added]

"***A further heavily discussed issue is that most customers might not be aware of these existing threats to their privacy***. [emphasis added] Fine-grained meter readings would be enabled by default, and the legal framework could offer them the opportunity to opt-out in case they feel uncomfortable with this situation. However, in [cases] where personal privacy is at stake, many argue that it would be far better to offer an opt-in feature for services that require high-frequency readings (e.g., demand response management), and by default just enable low-frequency data for billing purposes."

"[Some experts] ***further propose to distinguish between low-frequency readings for billing purposes that do not threaten privacy (one reading per week or month); and high-frequency readings (below a minute) that are required for running the technical infrastructure only and do not necessarily need to be linked to a certain individual***. [emphasis added] While low-frequency data is sent directly to the utility and billing company respectively, high-frequency data can be processed in the next substation (where data is actually needed for load management algorithms) and are not being stored in the utility's backend. With this hybrid approach, basic billing services can be provided directly, while anonymized fine-grained meter readings contribute to technical services. This essentially realizes a clear distinction between customer-specific data and technical data."

For more information on the above article, refer to the following link:

http://smartgridawareness.org/privacy-and-data-security/smart-grid-vulnerabilities-a-more-detailed-review/security-is-not-enough-on-privacy-challenges-in-smart-grids/.

Smart Meter Data Retention

Another important aspect of how consumer privacy interests are being compromised pertains to data retention. Long-term privacy risks could be partially reduced by having the Utility only maintain records of granular data collected by smart meters for a limited period of time, e.g., 90 days, etc., or even selectable through an online portal by the consumer. Instead, consumers are often faced with permanent retention of granular data that can be sought for legal proceedings, etc., essentially forever. Furthermore, in July 2013, a survey of 260 utility industry executives across the smart grid industry found that nearly half (47 percent) of the survey's participants do not think Utilities are prepared to handle the "data explosion from smart grid technologies." The point here is that Utilities are literally collecting mountains of data for which they have no idea on how to effectively utilize and at the same time are putting the consumer unnecessarily at risk.

Misrepresentations of Risks Associated with Smart Grid Technologies

Unfortunately, the consumer and representatives of the Utilities and the smart grid industry cannot even engage in a productive conversation regarding privacy risks associated with smart grid technologies. Why? Because the smart grid industry ignores or actively suppresses the legitimate risk-related information already presented in this document. What follows are some examples of how Utilities and the smart grid industry "inform" or misinform the public regarding privacy and data security risks.

It is frustrating to listen to and read Utilities and smart grid-related groups respond to the general question of "Does a smart meter invade my privacy?" Specific citations from various groups can be presented, and the theme is generally the same, which is as follows:

"Smart meters do not invade your privacy or monitor household activity. They only record total energy usage for the home, just like current analog meters."

Here are a few specific examples of Utility and smart grid industry misinformation:

Example #1

Information disseminated by the Smart Grid Consumer Collaborative (SGCC) is available on a number of utility websites and often includes the following statement from a "Data Privacy and Smart Meters Fact Sheet' available at: http://wp.me/a3nav9-1G6:

> ***"The privacy of electricity usage data is protected now and that will not change with the use of smart meters."***

The above statement is basically an oxymoron because it conflates the terms privacy and confidentiality.

Once someone else, even the Utility, has your private and personal information, it is no longer private. What Utilities can legitimately say is that they will attempt to keep your personal and private information "confidential" to the extent that their systems, programs, and the laws allow. If a consumer allows the Utility to collect granular data that can reveal activities or occupancy of the home, then that consumer has lost a considerable degree of privacy.

Example #2

The SGCC has produced a video on smart meters (named "Separating the Facts from the Fiction about Smart Meters") available at the following link: http://www.youtube.com/watch?feature=player_embedded&v=Nij-_gAMj-4.

On the topic of privacy, the following words are spoken in the video:

> ***"Smart meters only know how much power you are using, not specifically how you are using that power."***

The above statement is a childish, simplistic treatment of the subject matter. It is true that the smart meter is merely a conduit for collecting and transmitting energy-related usage data. Obviously, an inanimate object can't "know" anything. That is not the issue. The issue relates to the incremental and granular type of data that is collected and transmitted by the meter to places where it can be intercepted and stored and analyzed by others (real people) to be able to provide information about human behavior patterns or the usage patterns for individual appliances.

Example #3

From the Lafayette Utilities System website at: http://www.lus.org/site322.php, the following statements are made:

> ***"Smart meters do not monitor household activity. They only record total energy usage for the home or business, just like all current LUS meters."***

The above Utility statement completely ignores the fact that smart meters collect "incremental" energy usage data that can reveal household activity (as opposed to "total" energy usage). From reading the LUS statement, the consumer is expected to believe that there is essentially no difference between an analog meter and a smart meter. Thus, the LUS statement conveys no relevant information and constitutes deception.

Example #4

Specifically for the City of Naperville, there is a question and answer document that asks the question:

> ***"Can the utility monitor my consumption and know when I'm home?"***

The response is given as:

> ***"The utility cannot detect the presence of people in their homes; only the consumption of electricity is measured for billing purposes."***

[Reference: Naperville Smart Grid Initiative Question/ Response Inventory, dated March 25, 2013.]

As can be seen, in response to a question about whether the Utility can "know when I'm home," the City states that "The utility cannot detect the presence of people in their homes." The statement by the City must be properly categorized as *propaganda*. If people are alive and using electricity, their presence is detected and behavior can be inferred. In addition, as had already been demonstrated in this document, the City of Naperville smart meters collect much more data than is required for "billing purposes."

Example #5:

Again for the City of Naperville, Court documents for the Naperville Federal Lawsuit indicate there was the following verbal exchange (Case # 11-CV-09299, Document # 51-2, pp 9,11) :

> City: "Once the meters are installed, there are future phases of this project, one of which will be the implementation of the demand-respond program that will allow our customers to have an E-portal in their homes that will allow them to ... know how much energy by appliance is being used, and so that they can conserve if they so wish."
>
> COURT: "So what you are saying is that the information that the smart meters gather is limited to the aggregate [*] kilowatt hour every 15 minutes, *period*, and does *not* contain the information that the city could -- even ***theoretically*** someone could later use to develop the level of detail that would be available in the demand-response program." [emphasis added]
>
> CITY: "That is correct."
>
> [*] The Author maintains that the term "aggregate" is misused here in that energy usage information collected every 15 minutes represents incremental, granular, fine-grained, high-frequency type of energy usage information as opposed to total monthly aggregate usage information necessary for billing purposes.

Additionally, an affidavit submitted to the Court by the City of Naperville (Case # 11-CV-09299, Document # 53-1, p 6) states:

> ***"There is no way to determine, based upon the information collected and the technology used to collect the information, which appliances are being used or other intimate details going on inside a customer's home, such as medical conditions or sexual activities, or activities of occupants occurring within the home."***

Although the example of smart meter data being used to determine "sexual activities" is a bit extreme, the evidence presented in this Author's documented perspective effectively refutes the entire testimony presented by the City of Naperville as explained in this Example #5 above. It is absolutely "theoretically"

possible with confidence to determine (or infer, that is, reach a conclusion based upon known facts) the appliance usage and other intimate details of what is "going on inside a customer's home" based upon the nature and frequency of energy-related data collected by Naperville smart meters. The Author views the City of Naperville statements recorded through Court documents as false.

Example #6

On the topic of privacy and data security, Florida Power & Light Company (FPL) states that:

> **"*FPL is committed to protecting your personal privacy and security. The data recorded by your smart meter is encrypted and transmitted to FPL via a secure wireless network that complies with the industry's highest standards for cyber security*."**

It has already been established in this document that there are significant threats and concerns regarding smart meter data. The statement by FPL basically consists of empty words that convey no hint of the true cybersecurity risks to the consumer, the smart grid, and to the nation.

[Source: The FPL quotation listed above was viewable at the following website (towards the bottom of the webpage) on February 21, 2014: http://www.fpl.com/energysmart/smartmeter_tertiary.shtml.]

Example #7

There are some Utilities that actually advertise that privacy is increased through smart meters because the Utility "will no longer have to send an employee to the house or business to read the meter, which actually equates to more privacy for the customer." As an example, review the information provided to the consumer on the

issue of privacy at the website maintained by the Eugene Water & Electric Board (EWEB), Oregon's largest customer-owned utility at the following link: http://www.eweb.org/smartmeter/faq

> ***"What about my privacy?***
>
> ***The installation of advanced meters would actually enhance privacy because the utility would no longer have to send meter readers into the backyards of customers to collect usage information."***

For a Utility to state that smart meters actually "enhance" privacy defies belief. Such a Utility completely ignores all facts and risks involved with collection of incremental energy-related data as presented in this document.

With the type of information disseminated by the smart grid industry as shown above, consumers learn "nothing" of the true privacy concerns related to the smart grid unless they seek out that information from alternative sources.

Through misrepresentations and misinformation, it is thus clear that the smart grid industry refuses to publicly recognize a principal factor of why consumer rights and interests are currently being violated during the deployment of smart grid and smart meter technologies. The smart grid industry refuses to acknowledge the unambiguous consumer risks associated with smart metering. More specifically, and because of the associated risks:

Due to increased financial, privacy, physical and data security, and even reputational ***risks*** involved with collecting incremental, granular, fine-grained, high-frequency type of energy usage information, there is ***no business relationship basis*** for current smart grid technologies to be imposed upon consumers without their consent.

Additional Substantiation of the Privacy and Security Issues

Before proceeding further, the Author will digress slightly in order to provide additional perspective on how the consumer has not been given proper consideration during implementation of smart grid technology.

Dr. Massoud Amin is an expert on the U.S. electricity grid and is credited with coining the term "Smart Grid" in 1998. He serves as director of the Technological Leadership Institute at the University of Minnesota and is a professor of electrical and computer engineering. Dr. Amin is someone with impressive credentials in his field and someone who is about as strong an advocate as one could find for implementing a Smart Grid. That said, if you read what follows, it can easily be asserted that the current implementation of the Smart Grid is not consistent with the viewpoints expressed in his writings in terms of addressing consumer stakeholder interests.

In December 2011, Dr. Amin co-authored an article for *IEEE Power & Energy Magazine*, entitled, "Smart Grid — Safe, Secure, Self-Healing." In this article, challenges and opportunities were highlighted with regard to system security, resiliency, and privacy.

In the article, it is stated that: "Upgrading the control and communication systems for the power grid will present many **new security challenges** that must be dealt with **before** [emphasis added] extensive deployment and implementation of smart grid technologies can **begin**." [emphasis added]

A this point, this Author will inject a rhetorical question, "Why are systems being installed as quickly as the DOE grant award dollars can be spent and prior to addressing the many "new security challenges"?

The article also states that “AMI [Advanced Metering Infrastructure] introduces serious privacy concerns, as immense amounts of energy use information will be stored at the meter. Breaches into this data could expose customer habits and behaviors.” The article further states that in order to defend against Smart Grid vulnerabilities, “several security features need to be incorporated into the development of AMI, along with new privacy laws to protect consumers. Current privacy laws in the United States are fragmented and vague and do not specifically address consumer energy usage.” [emphasis added]

So if someone as well-renowned as Dr. Amin recognizes the key privacy concerns mentioned above, why isn’t the public even properly informed about these concerns? Furthermore, the Author is not aware of privacy laws being revised to address smart grid vulnerabilities, at least not in the state of Illinois and certainly not at the Federal level.

So the thrust of this slight digression is to point out that smart grid systems are being implemented prior to fully addressing already known privacy and security concerns that put the consumer at risk. Utilities communicate with customers as if there are ***no*** additional privacy and security concerns with smart meter and smart grid technology as compared to analog meters.

It is painfully obvious that smart grid security and privacy risks have not been fully addressed nor have they been properly communicated to the consumer. In addition, privacy laws have not been updated or upgraded to meet the new challenges posed by smart grid technology. Because of this, it is important that documents discussed earlier***** that have been written to provide common sense guidelines for protecting consumer privacy be given due consideration when Utilities collect more data through smart meters than might be considered necessary or reasonable.

***** [NIST Document NISTIR 7628 and “A Model Privacy Policy for Smart Grid Data.”]

How Specifically Are Privacy Interests Being Compromised?

Utilities may make a claim that residential electric customers do not have an expectation of privacy in the aggregate measurements of their electricity use. One Court opinion (Case # 11-CV-09299, Document # 68-1, page 23), could be referenced which would be consistent with this claim where it states, "Plaintiffs have no reasonable expectation of privacy in the aggregate measurements of their electricity usage…" However, with regard to this assertion, there needs to be clarification in the use of the term aggregate. It is inappropriate for hourly or 15-minute (or sub-15-minute) incremental measurements to be referred to "aggregate" measurements. Such measurements are actually granular, fine-grained, high-frequency types of measurements.

In order to minimize the invasion of individual and behavioral privacy, consistent with guidelines provided earlier, the appropriate aggregate energy usage measurement for the customer is the least invasive measurement needed to calculate a monthly electric bill. This aggregate measurement consists of one energy delivery reading in kWh per month. As previously stated, the incremental energy usage measurements are not necessary for purposes of generating a periodic (i.e., monthly) electric bill, are not aggregate measurements, and, are not essential to utility operations or maintenance of the smart grid system.

It is the assertion of the Author that a Utility exposes residents to unnecessary risks by collecting thousands of times more data than required to calculate a monthly electric bill. That data, consisting of granular, fine-grained, high-frequency type of energy usage measurements, can be used by others either maliciously or inadvertently using existing or developing technology in an unauthorized fashion to infer types of activities or occupancies of a home for specific periods of time.

It is also possible that such information can be sought for legal proceedings as evidence to prove or disprove certain propositions. As news stories have indicated, Utilities must surrender customer information to third parties under subpoena. In June 2013, the *San Francisco Chronicle* and the American Civil Liberties Union reported that California's three big, investor-owned utilities had disclosed individual account information on *thousands* of their customers in 2012, usually to government agencies. Sometimes the agencies were seeking billing, banking, and address information that would help them locate individuals. In more than half the cases, however, investigators received energy-usage data for the customers.

What the Author has documented are completely reasonable privacy concerns from credible sources, e.g., government issued documents and security experts. **For a Utility to deny these legitimate concerns is evidence of obfuscation**.

In one Court opinion on this issue, it was found that the "… Plaintiffs have not alleged that the installed smart meters are presently relaying any such detailed, nonaggregate information about their electricity usage to the [Utility] or that the Defendant's capture of such information is imminent." (Case # 11-CV-09299, Document # 68, p 21) Possibly there is an issue with terminology here, but let it be clear that the Utility and its smart meters collect and relay detailed, granular, fine-grained, high-frequency type of energy delivery information to the Utility in a manner that is identifiable with each residential customer account. To this extent, there is no inference, it is actually occurring. Beyond that, it is primarily through the use of non-intrusive appliance load monitoring (NALM) techniques or other analytical methods that personal activities within the home can be inferred. A Utility may indicate that it has no plans to employ those techniques, yet others, as indicated above, could employ such techniques, creating an unnecessary privacy risk for Utility customers.

During the course of the Naperville Federal Lawsuit, the City of Naperville has previously stated that "Plaintiff [asserts] that its members' consent is only applicable to analog and not smart meters, has no support in law." (Case # 11-CV-09299, Document # 78, p 7)

The City (i.e., the Utility) has likely mischaracterized the "Plaintiff's" assertions. What is more likely is that residential electric customers have only consented to the privacy risks involved with monthly energy usage readings in kWh. Hypothetically, such readings could be accomplished with either analog or digital electrical usage meters.

Legal Criteria for Determining Whether Privacy Rights Have Been Violated

To address the above reference to "no support in law," the Author will now transition this discussion to focusing on the applicable case law and addressing a Court's two stage process of determining whether an individual may invoke application of the Fourth Amendment for privacy expectations.

As one Court has stated (Case # 11-CV-09299, Document # 68, p 19), for a claim invoking the application of the Fourth Amendment, in accordance with *Smith v. Maryland*, 442 U.S. 735, 740 (1979), the inquiry embraces two discrete questions:

> "The first is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy – whether … the individual has shown that he seeks to preserve [something] as private."
>
> "The second question is whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable – whether … the individual's expectation, viewed objectively, is justifiable under the circumstances."

The Author will substantiate that both of these criteria are met in the paragraphs that follow.

Case Law for Privacy Infringements

The subject of case law on electrical usage meters does require some analysis. In general, it is acknowledged that existing case law would generally support a conclusion reached by one Court that "Plaintiffs have no reasonable expectation of privacy in the aggregate measurements of their electricity usage…" (Case # 11-CV-09299, Document # 68, p 23), but as previously explained, only to the extent that is required for billing purposes. Also, as previously stated, one must be precise and accurate in defining what one means by referring to "aggregate measurements." For customers with a fixed rate pricing plan, only one meter reading per customer is required per month. Thus, the measurement of customer electrical usage in kWh from one billing cycle to another would be the proper use of the term "aggregate measurement."

Consistent with the advent of new technology and its capabilities, existing case law must be viewed through a lens that provides a proper interpretation. This view would be consistent with the intent of an opinion expressed on the issue of constitutionally protected privacy interests in *Commonwealth v. Johnson*, 556 Pa. 216, 727 A.2d 1089, 1098 (1999), where it states, "We consider the totality of the circumstances and carefully weigh the societal interests involved when determining the legitimacy of such an expectation."

It is also instructive to review an opinion stated in *State v. Kluss*, 867 P.2d at 252-54 (Idaho Ct. App. 1993):

> "In order to have electricity, Kluss was obliged to obtain the same from [his utility company.] Kluss did nothing to create the records except consume power. The power records in the case at bar reveal only the amount of power usage. The power records were maintained by [the utility company] in the ordinary course of business. They do not identify any activities of Kluss. On a comparative basis they may demonstrate that the power use at the Kluss home is greater or lesser than similar houses or at similar times or that the power use has increased or decreased at different times.

> The information does not provide any intimate details of Kluss's life, identify his friends or political and business associates, nor does it provide or complete a 'virtual current biography.' The power records, unlike telephone or bank records, do not reveal discrete information [emphasis added] about Kluss's activities."

The rationale for the opinion in the above quoted section of case law is consistent with "power records" taken for monthly usage readings. The stated opinion is not consistent with incremental energy usage readings that could "reveal discrete information" about the consumer.

The *Kluss* rationale was also used in *Samson v. State*, 919 P.2d at 173 (Alaska Ct. App. 1996), where Judge Mannheimer, in his concurring opinion in *Samson*, noted that "gross electricity usage reveal[s] no details of the activities that consumed the electricity," whereas "[b]ank records list the details of a customer's financial dealings names of debtors, creditors, and most others with whom the customer does business."

Thus, if electricity usage records contain more than "gross" information and in fact contains incremental usage information that can be shown to "reveal discrete information" about individuals or home occupancies, etc., *then the traditional case law for analog meters does not apply*. In fact, taking into account the "totality of the circumstances," it should be concluded that hourly or 15-minute (or sub-15-minute) incremental, granular, fine-grained, high-frequency type of energy usage measurements collected by digital smart meters should receive a higher level of constitutional privacy protection. This is especially true since the granular information currently being collected by the smart meter is unnecessary for billing purposes.

Incremental energy usage readings of a granular nature must also be viewed in the context of the location for which the readings are being collected, namely, the home. Again, taking into account the "totality of the circumstances," Courts should extend

Constitutional protection for energy usage records of a granular nature since courts have recognized “an interest in protecting the well-being, tranquility, and privacy of the home. *Frisby v. Schultz*, 487 U.S. 474, 484 (1988) (quoting *Carey v. Brown*, 447 U.S. 455, 471 (1980)) (“The State’s interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society.” (quoting *Carey*, 447 U.S. at 471)).

In addition, an individual’s home is unique because it is “the last citadel of the tired, the weary, and the sick.” *Gregory v. Chicago*, 394 U.S. 111, 125 (1969) (Black, J., concurring).

Quoting sections from the Congressional Research Service (CRS) report entitled, “Smart Meter Data; Privacy and Cybersecurity,” February 2012, page 16 (only providing quotation marks as used in the document):

> In the case of smart meters, the information is generated in the home, an area accorded specific textual protection in the Fourth Amendment, and one the Supreme Court has persistently safeguarded. *Payton v. New York*, 445 U.S. 573, 589 (“The Fourth Amendment protects the individual’s privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual’s home -- a zone that finds its roots in clear and specific constitutional terms: ‘The right of the people to be secure in their ... houses ... shall not be violated.’”) (quoting U.S. CONST. amend IV); *Minnesota v. Carter*, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring) (“[I]t is beyond dispute that the home is entitled to special protection as the center of the private lives of our people. Security of the home must be guarded by law in a world where privacy is diminished by enhanced surveillance and sophisticated communication systems.”).
>
> In no uncertain terms the Court has asserted that “[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion.” *Silverman v. United States*, 365 U.S. 505, 511 (1961).

Beyond the adaptation of case law to the developing technology of digital smart meters and the special textual protection by the Fourth Amendment for the home,

there is the added monopoly aspect of the electric utility industry. In Naperville, Illinois, for example, this is especially true since there is absolutely no choice on the electric service provider and where the electric provider, as part of a municipal corporation, is outside the normal purview of a public utility commission, i.e., the Illinois Commerce Commission.

Again quoting the above referenced CRS report, page 21:

> "With banking or telephone services, a customer has the option of transferring his business to another bank or another telephone carrier. To the contrary, because electric utilities are essentially monopolies, the customer cannot simply switch services. The only way to avoid the recordation of his electric usage is to terminate his utility service altogether, an impracticable option in modern society."

Using the City of Naperville as an example, the City has stated that its residents have "agreed" to its smart meter installations on private property because the City has the following statement in its Municipal Code (refer to Case # 11-CV-09299, Document # 53-1, page 2):

> "All electric consumers agree to conform to and abide by the City's ordinance, rules and regulations for the operation of the electrical distribution system, including the provision that all meters are selected, owned and maintained by the city. 8-1B-1-2.1."

Having a rule codified that is unknown to 99% or more of the residents of the City of Naperville does ***not*** constitute "informed consent" to the increased risks associated with the smart grid system. Such an ordinance accomplishes nothing other than the ability for the City to enforce its rules with police action.

Also related to consent issues is a statement in one Court's ruling, where it stated, "That smart meters enable Defendant to read aggregate measurements remotely and more frequently does not permit Plaintiffs to re-capture their already privacy interest in the aggregate measurement of their electricity usage (whether that

aggregate usage is measured monthly, weekly, daily, hourly, or in fifteen minute measurements)." (Case # 11-CV-09299, Document # 68, p 20)

Hopefully, a Court can be persuaded to recognize that the "Defendant" in the case mentioned above misused the term aggregate in referring to incremental, granular, fine-grained, high-frequency type of energy usage measurements as "aggregate" measurements. As earlier stated, all residential electric customers have only consented to the risks involved with the aggregate measurement necessary to calculate their electric bill, which is one energy delivery data point per month measured in kWh (unless they have elected to participate in other voluntary energy control programs).

To be more specific, it is asserted that the only privacy interest ever "surrendered" was for residential electric customers to have electrical usage meters read at a frequency necessary for billing purposes, which is once a month. It is not correct to state that it does not matter whether usage is measured "monthly, weekly, daily, hourly, or in fifteen-minute increments." Any readings taken more frequently than monthly is unnecessary for billing purposes and thus subject residential electric customers to more risk than necessary, consistent with the guidelines of NIST Document NISTIR 7628, where it states that, "Because of the associated privacy risks, only the minimum amount of data necessary for services, provisioning, and billing should be collected." And also, "[a] requirement of receiving this [electrical] service is the disclosure to the power company … of one's identity and the amount of electricity being used. The nature of electrical service requires the disclosure of this information, but that disclosure is only for the limited business purpose of obtaining the service." *In re Restraint of Maxfield*, 133 Wn.2d 332, 341 (Wash. 1997)

Having reached this point in the discussion, the Author will summarize by explaining how the two stage process of determining whether an individual may invoke application of the Fourth Amendment for privacy expectations has been met.

Demonstrated Expectation for Privacy

It has been demonstrated that residential electric customers have a legitimate expectation to preserve individual and behavioral privacy with regard to electrical energy-related data collected at the metering location. Credible government reports and security experts have explained that there are privacy concerns that granular data collected by smart meters will reveal the activities of people inside of a home by measuring their electricity usage frequently over time and that there is deep concern that inadequate cyber security measures surrounding the digital transmission of smart meter data will expose such data to misuse by authorized and unauthorized users of the data. It is not that the meters themselves transmit the activities but that well established and available non-intrusive appliance load monitoring (NALM) techniques or other analytical methods are able to interpret the granular data to profile appliance loads and/or infer human behavior with ***increasing*** accuracy. Residential electric customers have only surrendered a privacy interest to the extent necessary to account for monthly billing by the Utility. Only one energy usage measurement per month is necessary for the billing process.

Expectation for Privacy is "Reasonable"

With regard to society being prepared to recognize as reasonable, viewed objectively, residential electric customers' expectation for privacy as it relates to electrical energy-related data collection is justifiable under the circumstances, for the following reasons:

1. In the United States, the Public Utility Regulatory Policies Act, PURPA Section 111(d), as amended by The Energy Policy Act of 2005, contains language that requires state utility commissions and unregulated utilities to consider whether it is appropriate for Utilities to offer customers smart metering for those who request it. The legislative intent was always that

smart metering was to be considered optional. Therefore, it is reasonable for people not to be forced to accept a smart meter in order to meter activities for which they have no desire to participate and do not want to accept the risks involved with smart metering. The scenario described above would be different if consumers opt-in to timed-based rates or utilize other energy management tools that actually require smart metering of electrical service. In those instances, consumers could consent for the Utility to collect data necessary to implement the smart metering options being requested.

2. Consumer concerns are well founded; they are based upon credible sources of information including government reports and security experts. One government report not yet mentioned in this document is the US General Accounting Office report issued in January 2011, entitled, GAO Report #GAO-11-117, "Electricity Grid Modernization." It is literally filled with significant cyber security issues, including the following concern on page 24: "*There is a lack of security features being built into smart grid systems.* Security features are not consistently built into smart grid devices. For example, our experts told us that certain currently available smart meters [emphasis added] have not been designed with a strong security architecture and lack important security features, including event logging and forensics capabilities which are needed to detect and analyze attacks." It is reasonable for individuals not to be forced to participate in a system which gathers more energy usage data than is required for billing purposes and which subjects them to higher privacy and security risks than traditional monthly meter reads.

3. Although most case law would support a conclusion that there is not a societal expectation for privacy of utility power records, it has been demonstrated that current case law is not applicable to the new technology where information transmitted by digital smart meters can "reveal discrete information" about individual appliance use or home occupancies.

Furthermore, by using existing case law rationale, as shown, it can be concluded that if electricity usage records contain more than "gross" information and in fact contain incremental usage information, then taking into account the "totality of the circumstances," it should be concluded that hourly or 15-minute (or sub-15-minute) incremental, granular, fine-grained, high-frequency type of energy usage measurements collected by digital smart meters should justifiably receive a higher level of constitutional privacy protection. This is especially true since the granular information currently being collected by the digital smart meter is unnecessary for billing purposes.

4. Given the "totality of the circumstances," in the case of smart meters collecting incremental and granular information, it is reasonable that Courts consider the fact that the information is generated in the home, an area accorded specific textual protection in the Fourth Amendment. It is also reasonable that Courts consider the fact that residential electric customers have no practical alternative to obtain electric service from another source.

5. Due to the fact that smart meters currently collect incremental, granular, fine-grained, high-frequency type of energy usage consumption information that is not required for customer billing purposes (for a consumer with a traditional fixed-rate pricing program), there is no business relationship basis for a Utility to impose on the consumer the additional and unnecessary financial, privacy, and data security risks that are associated with having a smart meter that collects incremental usage information installed on one's own property without consent. As previously stated, "[a] requirement of receiving this [electrical] service is the disclosure to the power company … of one's identity and the amount of electricity being used. The nature of electrical service requires the disclosure of this information, but that disclosure is only for the limited business purpose of obtaining the service." *In re Restraint of Maxfield*, 133 Wn.2d 332, 341 (Wash. 1997) It is reasonable that the customer not be

forced to disclose more electrical usage information than is required for the limited business purpose of generating an electric bill. It is reasonable the residential electric customers not be required to surrender privacy interests beyond that required to generate a monthly electric service bill.

6. Utilities have not properly considered the privacy interests of residential electric customers prior to moving forward with plans to modernize the electric grid. Because of this, it is reasonable that Utilities provide analog electrical usage meters to customers requesting them at no additional cost to the customer. Alternatively, it may be possible that a digital usage meter may be used if it can be assured that it is properly programmed to only collect data consistent with information required for billing purposes. Such an implementation would then recognize the privacy interests of the customer and still allow a Utility to move forward with a plan to help realize many of the advertised benefits of smart grid technology for operations and maintenance purposes.

Conclusions and Recommended Actions

Due to the foregoing presentation of factual allegations and substantiating evidence, it has been demonstrated that current Utility collection methods for incremental energy-related data for residential electric customers using smart meters represent an unreasonable invasion of privacy and, for applicable jurisdictions, constitute an unreasonable search in violation of the Fourth Amendment of the United States Constitution.

For instances where a Fourth Amendment allegation is not legally applicable due to a lack of demonstrated government intrusion, the general rationale for showing that smart meter data collection methods constitute an unreasonable invasion of privacy should still be persuasive to any fair-minded legislator, government official, or public utility commissioner.

Let us summarize some key points related to the Author's assertions related to smart meter data collection methods invading the individual and behavioral privacy of consumers.

1. Smart meters significantly expand the amount of data collected in granular form as related to the nature and frequency of energy consumption, thereby opening up more opportunities for general invasion of privacy.

2. Because smart meters collect energy data at much shorter time intervals than in the past (hourly or in 15-minute or sub-15-minute intervals rather than once a month), the information can reveal much more detailed information about the activities within a home or other premises.

3. Smart meter data, consisting of granular, fine-grained, high-frequency type of energy usage measurements, can be used by others either maliciously or inadvertently using existing or developing technology in an unauthorized fashion to infer types of activities or occupancies of a home for specific periods of time. It is also possible that such information can be sought for legal proceedings as evidence to prove or disprove certain propositions. For example, were you home on the night in question for the alleged crime?

4. When Utilities state that the "privacy" of consumer smart meter data is protected, they are conflating the terms privacy and confidentiality. Once someone else, even the Utility, has your private and personal information, it is no longer private. If a consumer allows the Utility to collect granular data that can reveal activities or occupancy of the home, then that consumer has lost a considerable degree of privacy.

5. It was stated in this document by reference to the 2009 report prepared for the Colorado Public Utilities Commission that insufficient oversight of smart metering implementation could lead to unprecedented invasions of consumer privacy. That is exactly what we have due to insufficient oversight and lack of due diligence:

   - Utilities have not considered consumer privacy interests prior to deploying smart meters that collect massive amounts of data not necessary for billing purposes. Utilities collect excessive data from consumers simply because "they can."
   - Current privacy laws in the United States are fragmented and vague and do not adequately address consumer energy usage for smart meter technology.

     NOTE: Acknowledging the obvious here is not intended to imply that this issue can easily be "fixed" with just the right laws. To this point in time lawmakers have failed to acknowledge the necessary premise that the mere collection of granular energy data for each customer by the Utility is an invasion of privacy. Once lawmakers realize that an "opt-in" or explicit consent approach to granular usage data collection is necessary to preserve customer privacy interests, then perhaps progress can be made in this area.

   - With regard to informing consumers of smart grid risk-related information, Utilities and manufacturers have no incentive to inform consumers of these risks since such action could possibly create a consumer backlash against the deployment of the smart grid technologies. Risk-related information is being deliberately suppressed by the smart grid industry, and the public is being provided misinformation which would indicate that there are no additional privacy risks related to smart meters as compared to the old analog meters.

- Contrary to Utility assurances, most currently available smart meters have not been designed with a strong security architecture and lack important security features, including event logging and forensics capabilities which are needed to detect and analyze attacks. The consumer's data are thus exposed to misuse by both authorized and unauthorized users of the data.

- As was mentioned earlier, one avenue of "authorized" privacy invasions would include smart meters installed on multiple building units or apartments. Landlords will likely have access to tenants' smart meter data in cases where the resident is a "consumer" but not a Utility "customer." A landlord could directly access a tenant's smart meter information through an online portal website and use it to observe tenant electrical usage patterns and behavior. The Utility would likely claim that it has no concern or control over such activities, yet the Utility is installing the technology that allows this avenue of privacy invasion to occur. Such ramifications of smart meter installations demonstrate lack of forethought and reckless disregard for consumer privacy interests.

6. Only one data point measured per month of energy usage in kWh (delivered) is necessary for customers with a fixed rate pricing program, for the limited business purpose of calculating a monthly bill. Due to increased financial, privacy, physical and data security, and even reputational risks involved with collecting incremental, granular, fine-grained, high-frequency type of energy usage information, there is no business relationship basis for current smart grid technologies to be imposed upon consumers without their consent.

7. Case law supports the assertion that consumers have a reasonable expectation for privacy of incremental energy usage data and that this expectation should objectively be viewed by society as reasonable. Upon recognition of these preserved privacy interests for incremental energy usage data, it becomes necessary that informed consent be obtained before a Utility can collect incremental energy usage data from the consumer.

The deployment of smart meters and other smart grid technologies have mainly benefited the utility industry and its vendors. In their present form, the smart grid and smart meters offer few or no benefits to consumers, but pose significant risks and costs to them and society.

In order to minimize privacy and data security risks, consumers at a minimum need the ability to ***refuse*** smart meter installations on a cost-free basis. This is only fair in order to properly acknowledge the needs and rights of the consumer.

Recognizing that the ability for individual consumers to refuse smart meter installations is only a partial solution to the many problems identified in this document, what is also urgently needed is a complete moratorium on the deployment of digital smart meters and associated smart grid components. This moratorium would allow time for an objective reassessment (by all relevant stakeholders) of what is actually necessary to modernize the electrical grid system. Rather than developing solutions “on the fly” in an attempt to reach some ill-defined objective and unrealistic time schedule, let us step back and contemplate what is right and safe for our nation and its people.

The smart grid industry should recognize the consumer as a stakeholder and not just a cash paying customer or data subject to be manipulated. If electrical grid modernization were properly planned, organized, and implemented, there might not be a need for individual consumer smart meter refusal rights. For example, digital

smart meters that collect and retain only the data necessary for customer billing and essential utility operations could represent a safe and secure method of metering for electrical usage acceptable to nearly everyone. This is the sort of approach that is necessary to make sustainable progress at achieving a truly "smart grid" that would provide a safe and secure future for our nation.

NOTE: Statements made in this document regarding privacy issues were made notwithstanding the fact that there are other issues to be resolved such as radiofrequency (RF) emissions from wireless smart meters and the associated penalty fees currently being levied by many Utilities for the installation and use of an analog usage meter or a non-wireless meter alternative (NWMA).

Addendum: Additional Supporting Information

In May 2014, a White House report was issued from the Executive Office of the President, entitled, "Big Data: Seizing Opportunities, Preserving Values."

Somewhat remarkably, if one reads the White House report and a specific and relevant referenced paper, one will realize that the document content is consistent with the assertions of this privacy report prepared by SkyVision Solutions. One can conclude that the smart meter deployment activities of many utilities not only unreasonably invade the privacy of customers (with consequential Fourth Amendment violations and/or violations of common law rights to privacy) but are also being implemented in a manner completely at odds with the information presented in Attachment B, "The White House Report on Big Data and Privacy."

ATTACHMENT A
Smart Meter Privacy Invasions by "State Actors"

Assertion

If a private utility company is ordered by a state public utility commission to install privacy invading smart meters as part of a mandate or otherwise ordered to charge a penalty fee for those refusing smart meters, then the private utility arguably becomes an "instrument or agent of the state" and must abide by Fourth Amendment provisions.

Background

To assess whether there has been a Fourth Amendment violation, a primary question must first be asked: whether there was state action; that is, was there sufficient government involvement in the alleged wrongdoing to trigger the Fourth Amendment?

As summarized by the Congressional Research Service (CRS) report entitled, "Smart Meter Data; Privacy and Cybersecurity," Feb. 2012, pp 8-10:

> "It is broadly said that the Fourth Amendment applies only to acts by the government. … The Fourth Amendment may also apply to a private utility if its acts were directed by the government. Generally, searches performed by private actors without police participation or encouragement are not governed by the Fourth Amendment. A search by a private insurance investigator, for instance, was not a 'search' in the constitutional sense, though the evidence was ultimately used by the government at trial. This result differs, however, if there is sufficient government involvement. If the search has been ordered or requested by the government, the private actor will become an 'instrument or agent of the state' and must abide by Fourth Amendment."
>
> "Thus, if a private party is required to perform a search or collect data under federal or state laws or regulations, there will be sufficient state action for the Fourth Amendment to apply. Or, put another way, the government cannot circumvent the Fourth Amendment by requiring a private party to initiate a search or implement an investigative program."

> "***This agency theory might apply to the collection of smart meter data. … If, for example, the government requested the utility to record larger quantities of data than was customary …, this would likely warrant Fourth Amendment scrutiny***." [emphasis added]

Key Point

The "customary" data set that is necessary for calculating a monthly utility bill is a once per month meter read. ***If a state utility commission mandates technology that requires granular data collection from the home that can reveal occupancies or activities within the home, then Fourth Amendment scrutiny is certainly warranted***.

Case Law

The grounds for determining whether a private utility can be considered a "state actor" was made clear in the case of *Palmer v Columbia Gas of Ohio*, 479 F2d 153 (CA 6 1973) where it states:

> "When a privately owned company enjoying a monopoly is in the business of providing a necessity of life it cannot, for purposes of evaluating its relationship to its customers and to the state in which and under whose control it operates, be considered as an independent, free market, common law competitor. …
>
> [W]hen a public function is performed by a private firm whose freedom of decision making has been restricted by governmental regulation and whose freedom of action has been severely circumscribed, the actions of the otherwise private firm become subject to the constitutional limitations placed upon state action. . . . When private individuals or groups are endowed by the state with functions or powers which are of a governmental nature, they become instrumentalities of the state and thus are subject to its constitutional limitations.
>
> [I]nasmuch as the state … is significantly involved in virtually every one of the company's activities, including the specific activity complained of, the conclusion that the regulatory activities of the state have insinuated it into a position of interdependence with the company so that it must be recognized as a joint participant with the company is inescapable."

Palmer provides clear guidance to find that a state public utility commission that orders intrusive and mandated smart meter deployments and/or coupled with a mandated “opt-out” tariff and penalty charges constitutes state action. As such, both the public utility commission and the regulated private utility company are subject to Fourth Amendment limitations under such circumstances.

Furthermore, once the privacy invading technology is determined to invade a customer’s “reasonable expectation of privacy,” it is not permissible for the utility company to withhold electrical service from a customer on the basis of not providing explicit consent for installation of the privacy invading smart meter technology or payment of a tariff and penalty charges due to a smart meter refusal. Such an action would clearly fly in the face of a U.S. Supreme Court case, *Memphis Light, Gas & Water Div. v. Craft, 436 U.S. 1 (1978)*, where it was stated that "Utility service is a necessity of modern life; indeed, the discontinuance of water or heating for even short periods of time may threaten health and safety."

Summary

When a private “investor-owned” utility is ordered by a state public utility commission to install granular data collecting smart meter technology and/or to charge tariffs for those customers refusing such installations, then such orders constitute “state action.” As such, the utility commission and private utility company are subject to the limitations of the Fourth Amendment. If the actions are further determined to constitute an *unreasonable* invasion of privacy, then those organizations have violated the Fourth Amendment rights of the affected customers.

ATTACHMENT B
The White House Report on Big Data and Privacy

The White House Report

In May 2014, a White House report was issued from the Executive Office of the President, entitled, "Big Data: Seizing Opportunities, Preserving Values."

Somewhat remarkably, if one reads the White House report and a referenced paper to be quoted below, one will discover that the content is consistent with the assertions of this privacy report prepared by SkyVision Solutions. ***One can conclude that the smart meter deployment activities of many utilities not only unreasonably invade the privacy of customers (with consequential Fourth Amendment violations and/or violations of common law rights to privacy) but are also being implemented in a manner completely at odds with what you will read below***.

The White House report recognizes the necessary protection of citizen privacy interests where it states:

> "A legal framework for the protection of privacy interests has grown up in the United States that includes constitutional, federal, state, and common law elements. 'Privacy' is thus not a narrow concept, but instead addresses a range of concerns reflecting different types of intrusion into a person's sense of self, each requiring different protections."

Further quoting the White House report:

> "U.S. privacy laws have shaped and been shaped by societal changes, including the waves of technological innovation set in motion by the industrial revolution. The first portable cameras helped catalyze Samuel Warren and Louis Brandeis's seminal 1890 article *The Right to Privacy*, in which they note that '[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual … the right 'to be let alone'… numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' This prescient work laid the foundation for the common law of privacy in

> the 20th century, establishing citizens' rights to privacy from the government and from each other."

"Big data" is described as "large, diverse, complex, longitudinal, and/or distributed datasets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future." Such data would include information collected from utility smart meters, and it was recognized that privacy could be affected by such data collection where the White House report states:

> "***Power consumption data collected from demand-response systems show when you move about your house***;"

and references a document called "A Privacy-Aware Architecture for Demand Response Systems," by Stephen Wicker and Robert Thomas, January 2011.

The Referenced Wicker and Thomas Paper

What follows are several quotes from the Wicker and Thomas paper referenced in the White House report.

From the abstract:

> "We explore the privacy issues implicated by the development of demand response systems. ***We begin by highlighting the invasive nature of fine-granularity power consumption data, showing that the data collected by Advanced Metering Infrastructure (AMI) reveals detailed information about behavior within the home***."

Quoting section 3 of the paper, "**AMI and the threat to privacy**":

> "***It has been shown that the detailed power consumption data collected by advanced metering systems reveals information about in-home activities. Furthermore, such data can be combined with other readily available information to discover even more about occupant's activities***."

[*Commentary: Utilities typically deny that detailed power consumption data can reveal in-home activities.*]

Quoting section 5.2 of the paper, "**Require consent to data collection**":

> "The term 'consent' is loaded with legal implications. For the purposes of privacy protection, consent is the flipside of disclosure – it establishes the disclosure as a contract. A requirement for consent also serves a pedagogical purpose – it alerts the user to the presence of data collection, and may heighten the awareness of the presence of a potential privacy issue."

[*Commentary: Almost no utilities are requiring consent to data collection when installing smart meters. On the contrary, utilities install the privacy invading equipment and apparently assume consent*.]

> "It has been proposed that any subscriber/user of a given communication technology must acknowledge the data collection disclosure before they can use the technology. The **acknowledgement requirement** can take the same form as license agreements for software updates. The user must click an appropriate button on a screen before proceeding to use the technology. …
>
> The technology that underlies a given service may change over time. A residential consumer may be associated with a given power utility for a long period of time, during which power consumption monitoring technology has changed dramatically. If data collection practices change, the user should be notified. Furthermore, user consent to such alterations should take the form of an **opt-in requirement**, as opposed to one of opting out. The former clearly increases the extent to which the consumer understands and acknowledges data collection."

Quoting section 5.3 of the paper: "**Minimize collection of personal data**":

> "'Personal data' is data that identifies or is correlated with the behavior, thoughts, and/or preferences of an individual. It has been shown that residential power consumption data can be correlated with the behavior of individuals within a house; the finer the resolution, the more detailed the disclosure.
>
> ***The first requirement under this heading is probably the most important of all of the design requirements – it is that such collection be necessary."***

[*Commentary: In contrast to minimizing data collection, most utilities appear to be collecting as much data as the purchased equipment can handle, which has nothing to do with what is "necessary."*]

Quoting section 6 of the paper: "**Privacy-aware demand response**":

> "When we view demand response systems through the lens of privacy-aware design, a privacy-preserving solution is apparent. The goal of demand response systems to is modify consumption behavior, whether through inducement or direct control, by exploiting fine-grained pricing information. The behavior of interest – consumption – is highly distributed. With the distributed processing requirement in mind, it becomes clear that it is not the power consumption data that needs to be collected, but it is instead the pricing data that needs to be distributed. ***Fine-grained consumption information need never leave the immediate neighborhood, thus alleviating most privacy concerns***. …
>
> The need to secure AMI data has certainly been noted, but that is not the point. ***If it is not necessary to the mission of the system that the data be collected, then it should not be collected. The potential harm to consumers has been noted elsewhere***. It should also be noted that the utility and the longterm future of the demand response program are also at risk. ***Consumers may become alarmed at the privacy risk, motivating legislation calling for an expensive retooling of the system. Judicial action may also put the program at risk. Whether from public outcry or judicial action, systems that forsake privacy-awareness may find themselves shut down***. …"
>
> "Finally, the utility needs consumption data, temporally precise, but aggregated at the level of the consumer, in order to predict demand and maintain a price model. Typically, ***aggregated real power consumption data at the substation level is sufficient to predict the need for new transmission and distribution lines and generation necessary to service the predicted demand***. A neighborhood aggregator can be used to combine and anonymize data so that the desired temporal granularity is provided without generating information about individual behavior. Aggregator contractual obligations to the utility provides it with information sufficient to determine how much of the predicted demand can be mitigated through pricing mechanisms. ***In any case the utility's need for consumption data should not be at the level of the individual consumer***."

[*Commentary: As indicated above, the utility has no need for consumption data at the level of the individual consumer; therefore there is no basis for its collection and retention unless explicit consent is received from the customer*.]

The Wicker and Thomas paper draws upon work prepared as part of another paper entitled, "Inferring Personal Information from Demand-Response Systems," by Lisovich, Mulligan, and Wicker from 2010. This paper makes some equally profound statements which are worth highlighting:

> "[N]ew data flow removes a structure that once afforded privacy protection for in-home activities (that is, the walls, combined with a low level of detail about energy consumption) and replaces it with a system that breaches the home's walls and exposes real-time consumption data."
>
> "This article details the sorts of conclusions that various players can readily draw from power-consumption data. … ***Our technology discussion and proof-of-concept demonstration show that even the simplest data mining and pattern-matching tools can convert power consumption data into information about events within 'the sacred precincts of private and domestic life,' illustrating the extent to which such players could violate residential privacy by collecting and using power-consumption data***."

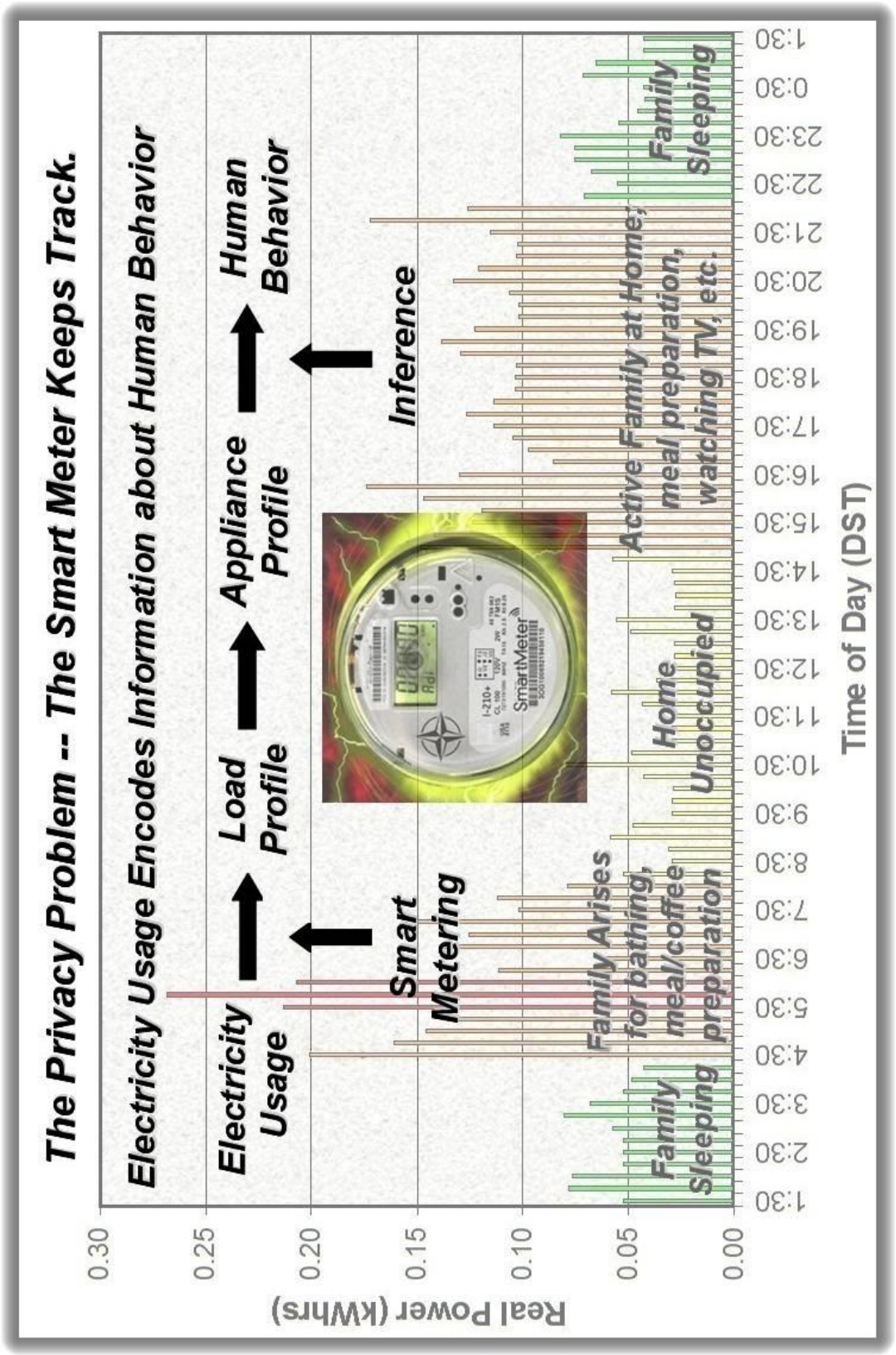
Summary and Conclusion

The White House report and the referenced Wicker and Thomas paper support the assertion that smart meter deployments are currently occurring without proper consideration for the consumer's privacy interests. If utilities were to:

- minimize data collection;
- require explicit consent from the customer for data collection in excess of that required for billing purposes; and
- collect data only to the extent necessary for utility operations at the substation level;

then the privacy interests of the customer could be respected.

Utilities must immediately change course and respect the rights of the citizens. Otherwise, as stated in the Wicker and Thomas paper, those "***that forsake privacy-awareness may [and should] find themselves shut down.***"
Let us protect the "***the sacred precincts of private and domestic life***," for ourselves and our children.


The Privacy Problem -- The Smart Meter Keeps Track.
Electricity Usage Encodes Information about Human Behavior
Electricity Usage
Load Profile
Appliance Profile
Human Behavior
Smart Metering
Inference
Real Power (kWhrs)
0.30
0.25
0.20
0.15
0.10
0.05
0.00
Time of Day (DST)
1:30
0:30
23:30
22:30
21:30
20:30
19:30
18:30
17:30
16:30
15:30
14:30
13:30
12:30
11:30
10:30
9:30
8:30
7:30
6:30
5:30
4:30
3:30
2:30
1:30
Family Sleeping
Family Arises for bathing, meal/coffee preparation
Home Unoccupied
Active Family at Home; meal preparation, watching TV, etc.
Family Sleeping
SmartMeter