ORIGINAL

OPEN MEETING AGENDA ITEM

Warren Woodward
55 Ross Circle
Sedona, Arizona 86336
928 204 6434

AZ CORP COMMISSION
DOCKET CONTROL

2013 MAR 25 P 12:15

March 23, 2013

Arizona Corporation Commission (ACC)
Docket Control Center
1200 West Washington Street
Phoenix, Arizona 85007

Arizona Corporation Commission
DOCKETED
MAR 25 2013
DOCKETED BY

Re: Docket # E-00000C-11-0328

Commissioners;

Will any of you care that APS is lying again?

APS is distributing a propaganda sheet titled, "Automated Meters: Myth vs. Fact", in which APS states:

> Myth: APS will use automated meters to monitor the actions of its customers.
>
> Fact: Automated meters do not have this capability. Like the old mechanical meters, automated meters measure how much energy customers use, not how they use energy. The automated meter does not store or transmit any personal identification information. The automated meters give APS no indication of who our customers are, what they are doing, nor can they determine what appliances customers are using.

These are simple but very carefully crafted sentences designed to be technically true while at the same time they actually tell a total, utter and complete lie.

Note the clever phrasing of the "Myth" portion: "APS will use...." Of course no one can say what APS *will* do in the future. But since they have lied repeatedly in the past – including about how often and how strongly their "smart" meters broadcast – is there any reason to expect the future will be different?

Additionally, at issue is not just what APS 'will do' with data but what hackers, governments and other third parties will do.

In the "Fact" portion of their statement APS lies outright and uses deceptive language.

This is quite obviously a lie: "The automated meters give APS no indication of who our customers are...." Of course the meters do. If they didn't then how would APS know who was using watt?

APS deceptively says that the meters can't determine what their customers "are doing, nor can they determine what appliances customers are using." Of course the meters cannot, but software analyzing the "smart" meter data can!

I will let the Congressional Research Service (CRS) explain why, how and to what extent APS is lying. And in case you don't know, the Congressional Research Service, in its own words,

> ...works exclusively for the United States Congress, providing policy and legal analysis to committees and Members of both the House and Senate, regardless of party affiliation. As a legislative branch agency within the Library of Congress, CRS has been a valued and respected resource on Capitol Hill for nearly a century.
>
> CRS is well-known for analysis that is authoritative, confidential, objective and nonpartisan. Its highest priority is to ensure that Congress has 24/7 access to the nation's best thinking.

The following is excerpted from the CRS report, "Smart Meter Data: Privacy and Cybersecurity" (http://www.scribd.com/doc/84773482/Smart-Meter-Data-Privacy-and-Cybersecurity-2-3-2012).

For ease of reading I have removed the footnotes. Almost every sentence has one citing evidentiary documentation. Unlike the ACC, the CRS have done their homework on this issue, and thoroughly.

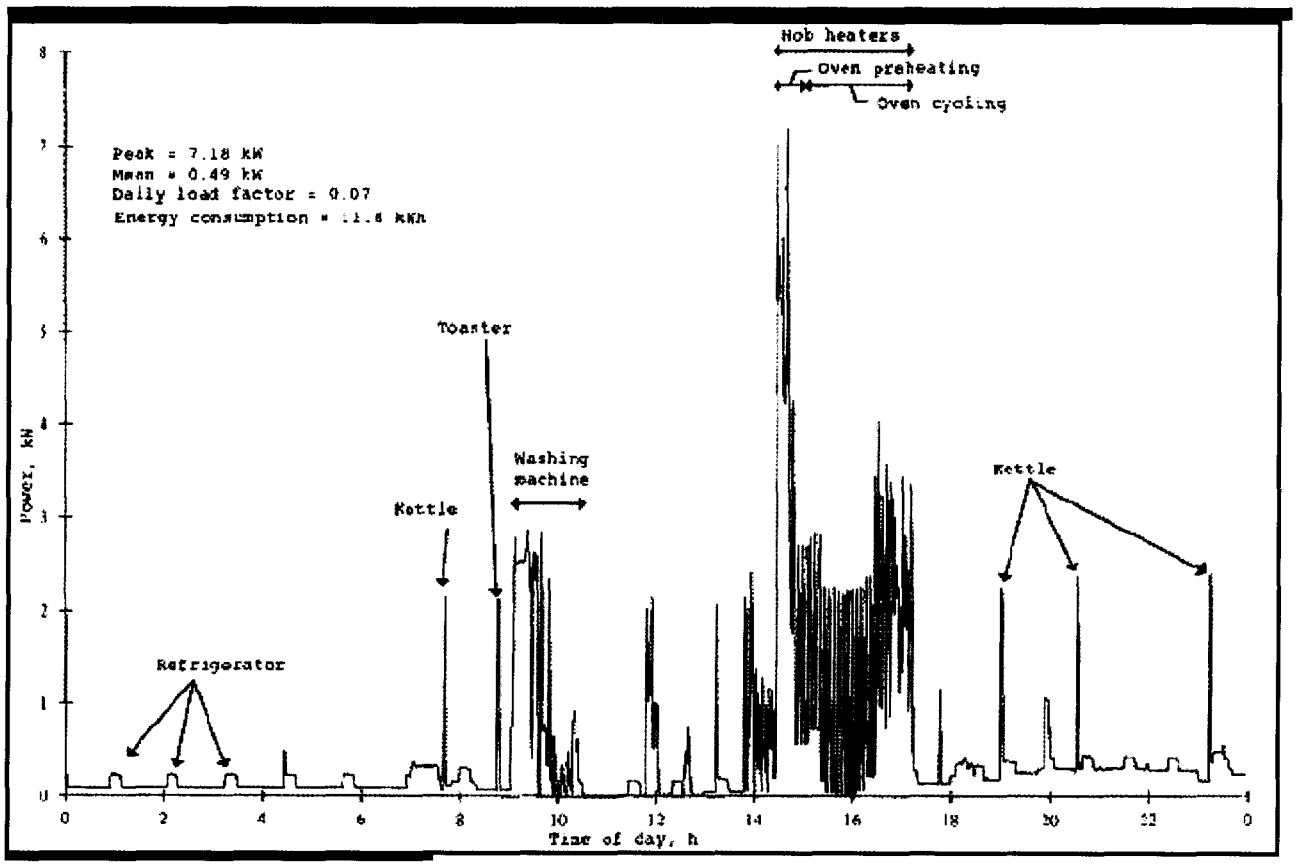
Detailed Information on Household Activities

> Smart meters offer a significantly more detailed illustration of a consumer's energy usage than regular meters. Traditional meters display data on a consumer's total electricity usage and are typically read manually once per month. In contrast, smart meters can provide near real-time usage data by measuring usage electronically at a much greater frequency, such as once every 15 minutes. Current smart meter technology allows utilities to measure usage as frequently as once every minute. By examining smart meter data, it is possible to identify which appliances a consumer is using and at what times of the day, because each type of appliance generates a unique electric load "signature." NIST [National Institute of Standards and Technology] wrote in 2010 that "research shows that analyzing 15-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances." A report for the Colorado Public Utilities Commission discussed an Italian study that used "artificial neural networks" to identify individual "heavy-load appliance uses" with 90%

accuracy using 15-minute interval data from a smart meter. Similarly, software-based algorithms would likely allow a person to extract the unique signatures of individual appliances from meter data that has been collected less frequently and is therefore less detailed.

By combining appliance usage patterns, an observer could discern the behavior of occupants in a home over a period of time. For example, the data could show whether a residence is occupied, how many people live in it, and whether it is "occupied by more people than usual." According to the Department of Energy, smart meters may be able to reveal occupants' "daily schedules (including times when they are at or away from home or asleep), whether their homes are equipped with alarm systems, whether they own expensive electronic equipment such as plasma TVs, and whether they use certain types of medical equipment." **Figure 1,** which appears in NIST's report on smart grid cybersecurity, shows how smart meter data could be used to decipher the activities of a home's occupants by matching data on their electricity usage with known appliance load signatures.

Figure 1. Identification of Household Activities from Electricity Usage Data
Unique Electric Load Signatures of Common Household Appliances



Smart meter data that reveals which appliances a consumer is using has potential value for third parties, including the government. In the past, law enforcement agents have examined monthly electricity usage data from traditional meters in investigations of

people they suspected of illegally growing marijuana. For example, in United States v. Kyllo, a federal agent subpoenaed the suspect's electricity usage records from the utility and "compared the records to a spreadsheet for estimating average electrical use and concluded that Kyllo's electrical usage was abnormally high, indicating a possible indoor marijuana grow operation." If law enforcement officers obtained near-real time data on a consumer's electricity usage from the utility company, their ability to monitor household activities would be amplified significantly. For example, by observing when occupants use the most electricity, it may be possible to discern their daily schedules.

As smart meter technology develops and usage data grows more detailed, it could also become more valuable to private third parties outside of the grid. Data that reveals which appliances a person is using could permit health insurance companies to determine whether a household uses certain medical devices, and appliance manufacturers to establish whether a warranty has been violated. Marketers could use it to make targeted advertisements. Criminals could use it to time a burglary and figure out which appliances they would like to steal. If a consumer owned a plug-in electric vehicle, data about where the vehicle has been charged could permit someone to identify a person's location and travel history.

Even privacy safeguards, such as "anonymizing" data so that it does not reflect identity, are not foolproof. By comparing anonymous data with information available in the public domain, it is sometimes possible to identify an individual—or, in the context of smart meter data, a particular household. Moreover, a smart grid will collect more than just electricity usage data. It will also store data on the account holder's name, service address, billing information, networked appliances in the home, and meter IP address, among other information. Many smart meters will also provide transactional records as they send data to the grid, which would show the time that the meter transmitted the data and the location or identity of the transmitter.

Regarding the security of this data collected on ratepayers, the CRS report says:

...consumer data moving through a smart grid becomes stored in many locations both within the grid and within the physical world. Thus, because it is widely dispersed, it becomes more vulnerable to interception by unauthorized parties and to accidental breach. The movement of data also increases the potential for it to be stolen by unauthorized third parties while it is in transit, particularly when it travels over a wireless network....

And speaking of "widely dispersed" data, I notice that APS billing statements now come with asterisks next to "Metering", "Meter reading" and "Billing". The asterisks refer to a notation that states, "These services are currently provided by APS but may be provided by a competitive supplier." How heartening to know that our data may be outsourced, or "widely dispersed".

Even without dispersal, data security is a pipe dream. As the Microsoft Corporation

succinctly puts it: "There is no way to guarantee complete security on a wireless network." (http://windows.microsoft.com/en-US/windows-vista/How-do-I-know-if-a-wireless-network-is-secure).

Haven't we all been hacked at one point or another? Haven't we all read news reports of individuals, corporations and governments that have been hacked? The "smart" grid will *not* be different. Indeed, it is not different already.

The "smart" grid hacking that I and many others easily predicted has started. Last September Talvent got hacked. Read about it: http://krebsonsecurity.com/tag/telvent-hack/ .

The Department of Homeland Security has also reported 81 cyber-attacks against power companies in the last year alone, including a power plant which was prevented from restarting for several weeks. Read about it here: http://www.marinij.com/ci_22805379/catastrophic-cyberattack-could-hit-utilities-like-pg-e

So here's another easy prediction: As the "smart" grid expands, hacking will just get worse. Associated costs – already estimated at "upward of $14 billion" according to the article cited above – will make meter readers look cheap in comparison, and people will wonder how anyone could have been so foolish as to ruin a system that worked great for about 100 years.

Actually, detailed as it is, the CRS report does not go far enough in evaluating the total extent of "smart" meter technology's in-home spying capability. Based on "smart" meter data, a study by the Computer Security Lab at the Munster University of Applied Sciences in Steinfurt, Germany was able to identify exactly what TV shows people were watching. From the report:

> Our research shows that the analysis of the household's electricity usage profile at a 0.5s−1 sample rate does reveal what channel the TV set in the household was displaying. It is also possible to identify (copyright-protected) audiovisual content in the power profile that is displayed on a CRT, a Plasma display TV or a LCD television set with dynamic backlighting. Our test results indicate that a 5 minutes-chunk of consecutive viewing without major interference by other appliances is sufficient to identify the content. (http://1lab.de/pub/ieee_forensics2012.pdf)

I listened to the minutes of a September 8, 2011 ACC meeting in which the issue of "smart" meter privacy was briefly discussed. A previous commissioner had the audacity, the stupidity and the rudeness to refer to those of us concerned about the proven privacy violating capability of "smart" meters as "the black helicopter crowd".

I would call anyone invading my home, whether physically or electronically, a criminal. And I would categorize anyone who permits such an invasion as complicit.

I also contend that the ACC appears complicit in depriving Arizonans of the their 4th Amendment rights in what amounts to probably the most massive invasion of privacy in the history of the United States.

Most of what I have written in this letter has already been presented to the ACC over the past year and a half by myself and others. Yet the sum total of the ACC's action has been *nothing*. Oh, there's been some talk, a bit of lip service and promises of future promises, but no action. Meanwhile, "smart" meter installations continue as they have from the start – with no regulatory oversight whatsoever – and the surveillance grid grows.

By the way commissioners, the only safe data is the data that never leaves the individual in the first place. So do not waste our time with any false promises about "best practices" and "encryption". Any lock can be picked.

A particularly disturbing example of apparent ACC complicity is the fact that ACC Chairman Bob Stump sits on the Board of Directors of the National Association of Regulatory Utility Commissioners. NARUC, and by extension Stump, must know full well what a violation "smart" meters pose to people's privacy because, in fact, NARUC has discussed the issue. They attempt to address it in Orwellian doublespeak. NARUC's "Resolution on Smart Grid Principles" pretends to protect people's privacy but actually eviscerates it. (http://www.naruc.org/Resolutions/Resolution on Smart Grid Principles.pdf).

In the NARUC "Principles" that deal with privacy and who can and should have access to ratepayers data, NARUC makes high-sounding but vague recommendations like urging regulators to follow "national privacy best practices", whatever those are. Perhaps someone could find out by asking Wikileaks or the National Security Agency. Maybe the CIA would know.

But the NARUC "Principles" also state that, "Rules that govern data access must balance privacy with innovation."

For the Constitutionally illiterate NARUC, Stump and ACC, we already have a privacy policy in place. The "national privacy best practices" is called the 4th Amendment to the U.S. Constitution. As the "Supreme Law of the Land" it is not supposed get "balanced with innovation", corporate greed or governmental arrogance and overreach. And if that's not enough there are state and federal wiretapping laws.

In short commissioners, there is nothing to "balance".

" The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...."

~ 4th Amendment, U.S. Constitution

In case you think you see a possible loophole with the word, "unreasonable", there is nothing "reasonable" about attaching surveillance devices to every home in Arizona and then telling people they can trust APS liars, the government and "third parties" with the information gathered because everyone has supposedly promised to play fair, not look, and because it will never get hacked; honest it won't.

Attempting to make such a massive violation "voluntary" by virtue of an "opt-out" fee paid to not have the surveillance device doesn't stand up either. Paying to be not violated is actually called "extortion", not "voluntary".

So the point remains. APS is lying – again.

APS lied about how often and how strongly their "smart" meters broadcast and now they are lying again about their "smart" meters' surveillance capabilities.

Imagine. The same utility entrusted to run a nuclear power plant is a repeat liar.

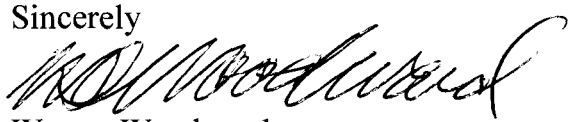
Why do you sit idle and do nothing? Are you incompetent or corrupt?

Indeed, you appear complicit in a conspiracy of long standing to deprive Arizonans of their 4th Amendment rights.

Approving an "opt-out fee" would also compound your crimes and make you a party to extortion.

What are you going to do? When will you wake up?

Sincerely



Warren Woodward

Cc: Governor Jan Brewer, Attorney General Tom Horne