

ORIGINAL

Antonio Gill

**Generic Smart Meter
Investigation
E-00000C-11-0328**



0000130312

From: Craig and Monnie R
Sent: Wednesday, Septem
To: Barbara Litrell; Burns
mdinunzio@sedonaa
er@sedonaa.gov; Elizabeth Kelley; Karen Fann;
Council; web.bos.district1@co.yavapai.az.us; web.bos.district2@co.yavapai.az.us; web.bos.district3@co.yavapai.az.us;
drayner@sedonaa.gov; dmclroy@sedonaa.gov; Cheryl Fraulob
Subject: Comments on ACCC Docket Number 11-0328 Security Issues with Smart Meters

I am sending my comments regarding the smart meters on Docket Number E-00000C-11-0328

Your Name: Monnie Ramsell

Address: [Redacted]
Sedona AZ 86336

Docket Number: 11-0328

Utility name: APS

Email address: monnie@ramsell.net

Arizona Corporation Commission

Date: 9/28/11

Phone (Home) [Redacted]
Cell Phone None

DOCKETED

OCT 5 2011

DOCKETED BY [Signature]

RECEIVED
2011 OCT -5 A 11:36
AZ CORP COMMISSION
DOCKET CONTROL

Smart Meters and smart grids are very vulnerable to hacking. No matter how many times the utility companies tell us the technology is safe, they are not. At the very least, these meters are invasion of privacy. I will not be going into what these meters are capable of. That deserves a whole separate comment topic.

I will focus on the vulnerability of the mesh grid. This is should have no debate. It is a known fact by all scientists. Then, I will also address the vulnerability of the meters themselves with step by step guide on how to hack a smart meter posted by hacker just to see how safe his meter is. It does not really take a rocket scientist to do this. Just some basic understanding of electronics and how to decrypt a key. Unless there are safeguards and heavy penalty in place for any breaches of data, these meters should not be installed. Since securing a wireless is virtually impossible, concerned customers should be given the opportunity to opt for other more secure options like fiber optics. Since there is no federal mandate to have wireless smart meter, consumer should have the choice to request a more secured option. Now the Commission has this knowledge, you will also have the responsibility to prevent any of these from happening.

Utility companies really have no rights to penalize customers who want to opt out of any of these wireless option because this option is inferior, untested, unsecured, easily hackable, potentially catastrophic. The potential risks and costs resulting from hacked data or faulty shut-off could be hundred times more than any additional opt-out fees intended by the utility company. Consumers should not be forced to accept an inferior service. The Corporate Commission should set up rules and regulations to safeguard the security and safety of all these data. Of course, protecting and safeguarding data is not usually the duty of this Commission, but if smart grid is to happen, this very serious security issue needs to be discussed and then resolved. Personally, I think we have the cart before the horse. But then it is up the Commission to exercise its caution to prevent any known potential damage. It is not too late to request more independent studies before approving the utility companies to move full steam forward. Ever wonder why some states and cities have chosen to ban the smart technology until further studies are done to prove that it is really to the benefit of the ratepayers? Prudent wisdom always will pay off. The time to act is now to stop this potential disaster.

Finally, I am enclosing a presentation at a hacker conference by Joshua Wright: KillerBee: Practical ZigBee Exploitation Framework or "Wireless Hacking and the Kinetic World".

Before any smart wireless devices are approved for wide-spread use by this Commission, everyone should listen to this presentation. It is both entertaining and informational. Joshua had a very good point. Hacking credit card is not real life events, there is not much "fun" for the hackers. Hacking real life events like bringing down

the grid, opening flood gates, etc. are the major excitement for hackers. Smart grids will attract hackers like bees to honey. The remote shut down feature is especially tempting. Who doesn't dream of shutting down the grid if they can? And yes they knew they could. Anybody who listens to this presentation will totally agree. In case anybody has the urge after listening to Josh to try hacking some meters (to test its safety, of course), just don't try this at home. Yes, this information is widely available to hack the smart meter. And there is still no 100% safety solution at this point.

<http://quahogcon.org/QC2010Archive/audio/wright.mp3> This is the voice presentation (45 minutes)

<http://quahogcon.org/QC2010Archive/slides/wright-killerbee.pdf> This is his power point slides

For the rest of us who wants to understand the issue in more layman's term, watch the next video (11 minutes)

The following is from the expert opinion of Alexander Herrera.

Alexander Herrera is a disabled computer programmer who worked for Dell Computers on their bios. He is expert on networks. He understands how security works on system network. This is how he explains about the security of Smart Meters and the mesh grid. He explains this on the youtube video.

http://www.youtube.com/watch?v=bGhq_bP4BLk

Here is a brief summary of what he said.

Most people thinks WiFi connection and Smart Meter WiFi is the same. This is not the case.

Regular WiFi Router uses password security to prevent listening in and you can make phone call through the router. Good password will jumble and scrambled so no one can hook up to your WiFi. But it is up to you to keep your password a secret.

Smart Meter WiFi is different. Smart Meter WiFi uses the WiFi Mesh which sends your signals to our neighbor's and your neighbor sent theirs to you and the signals are sent back and forth till ALL data are duplicated across the entire mesh and till every meter gets it. Only then will the final data be sent from the mesh to your utility company. Your utility company can also send a signal to the mesh, and then to your meter.

If a password is really good, no problem. It has to be a very good key and a very secret key.

What is so unique about WiFi Mesh is, if you have an encryption device in your hand or even in a lockbox, there is a way and someone will figure out a way to get it.

For example, a copy-protected DVD, you can make copy but you can play it. Once you played it, the code will be in the DVD player machine and an engineer can break it, very easily.

Same with the Smart Meter, according to Forbes Magazine, an engineer easily hacks into his smart meter and break the secret key. The smart meter installed outside each customer's house is the device that holds this code or key. With the key, he can change his usage data and even change his neighbor's usage data, download his neighbors' data, know their lifestyle patterns, habits, etc.

There is really NO possible way to secure a WiFi.

The following quote is taken directly from Microsoft's website.

"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>

If anybody is saying that their WiFi network is 100% secured, at least you know they are lying. All scientists know about this known fact.

Now here is an article from Forbes about the lacking of security of smart meters by Jeffrey Carr.

<http://www.forbes.com/sites/jeffreycarr/2011/01/31/ember-needs-a-wake-up-call-from-the-cia/>

Ember Needs A Wake-Up Call From The CIA

Ember Corporation, a privately-held company based in Boston, MA with offices in the U.K. and China (Hong Kong) is a leading supplier of the "brains" of Smart Grid devices – semiconductor chips that enable the smart meter on your house to wirelessly send data about your power consumption to your power grid provider. It also allows your power company to control the supply of energy to every house in its service area up to and including a complete disconnection of service. It does this through a wireless communications protocol that you've probably never heard of called ZigBee. Unlike Bluetooth which uses too much power, or WiFi, which is too complicated and expensive, Zigbee takes little power, is relatively simple to work with, and is low in cost, which is why Ember Corporation caught the attention of In-Q-Tel, the venture capital arm of the CIA back in 2005.

Here's how In-Q-Tel describes the company and its services:

Ember Corporation's wireless semiconductor solutions help auto mate homes, lower buildings' energy consumption, reduce manufacturing plants' breakdowns, and keep the country's borders and infrastructure safe and secure. With more than 120 customers, Ember's vision is to help create an "Internet of things" by enabling the eight billion microcontrollers built into products each year to support low-cost, low-power networking applications in any industry.

The Problem

The encryption keys that provide for ZigBee's vaunted security are transmitted in plain text. That's the equivalent of using the word "password" as your password. If you don't believe me, or want to test it for yourself, Josh Wright built the KillerBee toolkit ([.pdf](#)) in 2009 to show you how. In early 2010, Travis Goodspeed, a friend and one of the world's best security researchers in this area, explained why he started a smart grid skunkworks mailing list where employees of companies who were otherwise doing nothing about this problem, like Ember, could do some brainstorming about how they might fix it.

Despite having found many vulnerabilities in microcontrollers and LPAN radio chips, I have never seen one single security issue mentioned in the errata sheets of these devices. It has been a year since I first reported to Texas Instruments that the RAM of their Chipcon 8051 core is exposed to an attacker, but there's not one scrap of documentation from the firm to its customers suggesting that they make the simple patch of moving the key variables to Flash memory. The example ZigBee stack for the chip is still vulnerable to this attack, even after recent patches! A year later, exactly two debugger commands are all that are required to extract keys from nearly every ZigBee SEP device with a Chipcon radio, and no one knows to patch their code! **(Do not be smug if you are an Ember customer. The EM2xx chips are unpatchably vulnerable to debugger key extraction, and there is no mention of this in the chip's errata sheet either.)** (emphasis added)

I don't know how much weight In-Q-Tel has with Ember's board of directors but this needs to be addressed at the highest levels. We're talking about Critical Infrastructure here. For companies like Ember and Texas Instruments to simply ignore the repeated warnings of respected security researchers like Travis, Josh, Nick D. and others is, in my opinion, disgraceful behavior. And while I'm not a lawyer, if harm is caused to a power company's customers because this well-known and well-publicized flaw was finally exploited by bad guys, I'd bet the mother of all class-action lawsuits would be waiting on deck.

<http://www.greenbiz.com/blog/2009/09/01/four-ways-hack-smart-grid>

Four Ways to Hack the Smart Grid

By Preston Gralla

Published September 01, 2009

Worried about the security of the Smart Grid? You should be. Security researchers warn that the Smart Grid could become a hacker's playground. As proof, here are four ways the Smart Grid can be hacked.

Technology Review has an excellent article outlining ways in which the Smart Grid is vulnerable. Here, based on the article, are four ways it can be hacked via the smart meters that will be in businesses and people's homes.

Attack Smart Meter RAM

The article says that security researcher Travis Goodspeed warns that attackers will be able to hack directly into smart meter RAM, and by doing that, get free reign. It sounds a little James Bond-ish, but here's how the articles claims says it can be done:

If the meter hasn't been built with protective features, a hacker can use syringes to insert a needle into each side of the device's memory chip. The needle serves as a probe to intercept the electrical signals in the memory chip. By analyzing these signals, the hacker can deduce the device's programming. Even if the meter includes security features, he says, it may be possible to extract the information using customized tools.

Hack the Meter's Digital radio

Godspeed says a similar technique to RAM-hacking can be used to get command of the smart meter's radio, and from there, launch attacks on the grid itself. Here's what the the article says:

The smart meter's two-way radio chip allows the device to be read remotely and to receive commands over the network. The software in the chip contains security codes that an attacker who's cracked the meter's programming can use to get on the network and begin issuing commands. Goodspeed has shown that the codes can be extracted using syringes in a process similar to the attack on the memory.

Hack the Meter Wirelessly

The article says that David Baker, director of services for security firm IOActive, warns that hackers can get into the meter via its wireless networking device for communicating with the network:

An attacker can use a software radio, which can be programmed to emulate a variety of communications devices, to listen in on wireless communications with the network and deduce over time how to communicate with the meters. Another method, Baker says, is to attack the hardware. An attacker could steal a meter from the side of a house and reverse-engineer it. This method, he says, while inexpensive, does require a good knowledge of integrated circuits.

Spread Malware Throughout the Network

Baker says that once someone has gotten access to a smart meter's programming, he could easily launch a worm or other malware to attack the network itself, other smart meters, and other devices attached to the grid. In fact, Baker has already demonstrated that it can be done, the article says:

To demonstrate his attack, Davis crafted a piece of malware that could self-replicate to other meters, allowing an attacker to shut them down remotely. In simulations, Davis showed that if his worm were released in an area where all the houses were equipped with the same brand of meter, the worm could spread to 15,000 homes in the space of 24 hours.

The following is a step by step guide on how to hack a smart meter. Really doesn't sound that difficult at all.

<http://rdist.root.org/2010/02/15/reverse-engineering-a-smart-meter/>

Reverse Engineering a Smart Meter

In 2008, a nice man from PG&E came out to work on my house. He installed a new body for the gas meter and said someone would come by later to install the electronics module to make it a "smart meter". Since I work with security for embedded systems, this didn't sound very exciting. I read up on smart meters and found they not only broadcast billing information (something I consider only a small privacy risk) but also provide remote control. A software bug, typo at the control center, or hacker could potentially turn off my power and gas. But how vulnerable was I actually?

I decided to look into how smart meters work. Since the electronics module never was installed, I called up various parts supply houses to try to buy one. They were quite suspicious, requesting company background info and

letterhead before deciding if they could send an evaluation sample. Even though this was long before IOActive outed smart meter flaws to CNN, they had obviously gotten the message that these weren't just ordinary valves or pipes.

Power, gas, and water meters have a long history of tampering attacks. People have drilled into them, shorted them out, slowed them down, and rewired them to run backwards. I don't think I need to mention that doing those kinds of things is extremely dangerous and illegal. This history is probably why the parts supplier wasn't eager to sell any smart meter boards to the public.

There's always an easier way. By analyzing the vendor's website, I guessed that they use the same radio module across product lines and other markets wouldn't be so paranoid. Sure enough, the radio module for a water meter made by the same vendor was available on Ebay for \$30. It arrived a few days later.

The case was hard plastic to prevent water damage. I used a bright light and careful tapping to be sure I wasn't going to cut into anything with the Dremel. I cut a small window to see inside and identified where else to cut. I could see some of the radio circuitry and the battery connector.

After more cutting, it appeared that the battery was held against the board by the case and had spring-loaded contacts (see above). This would probably zeroize the device's memory if it was cut open by someone trying to cheat the system. I applied hot glue to hold the contacts to the board and then cut away the rest of the enclosure.

Inside, the board had a standard MSP430F148 microcontroller and a metal cage with the radio circuitry underneath. I was in luck. I had previously obtained all the tools for working with the MSP430 in the Fastrak transponder. These CPUs are popular in the RFID world because they are very low power. I used the datasheet to identify the JTAG pinouts on this particular model and found the vendor even provided handy pads for them.

Since the pads matched the standard 0.1" header spacing, I soldered a section of header directly to the board. For the ground pin, I ran a small wire to an appropriate location found with my multimeter. Then I added more hot glue to

stabilize the header. I connected the JTAG cable to my programmer. The moment of truth was at hand — was the lock bit set?

Not surprisingly (if you read about the Fastrak project), the lock bit was not set and I was able to dump the firmware. I loaded it into the IDA Pro disassembler via the MSP430 CPU plugin. The remainder of the work would be to trace the board's IO pins to identify how the microcontroller interfaced with the radio and look for protocol handling routines in the firmware to find crypto or other security flaws.

I haven't had time to complete the firmware analysis yet. Given the basic crypto flaws in other smart meter firmware (such as Travis Goodspeed finding a PRNG whose design was probably drawn in crayon), I expect there would be other stomach-churning findings in this one. Not even taking rudimentary measures such as setting the lock bit does not bode well for its security.

I am not against the concept of smart meters. The remote reading feature could save a lot of money and dog bites with relatively minimal privacy exposure, even if the crypto was weak. I would be fine if power companies offered an opt-in remote control feature in exchange for lower rates. Perhaps this feature could be limited to cutting a house's power to 2000 watts or something.

However, something as important as turning off power completely should require a truck roll. A person driving a truck will not turn off the mayor's power or hundreds of houses at once without asking questions. A computer will. Remote control should not be a mandatory feature bundled with remote reading.

Another expert proving that smart meters can be hacked.

http://articles.sfgate.com/2010-03-27/business/19914351_1_smart-meters-meter-reader-new-meters

Smart meter flaws give hackers power

March 27, 2010|By Jordan Robertson, Associated Press

Utility Computer-security researchers say new smart meters that are designed to help deliver electricity more efficiently also have flaws that could let hackers tamper with the power grid in previously impossible ways.

At the very least, the vulnerabilities open the door for attackers to jack up strangers' power bills. These flaws also could get hackers a step closer to exploiting one of the most dangerous capabilities of the new technology - the ability to remotely turn someone else's power on and off.

The attacks could be pulled off by stealing meters - which can be situated outside of a home - and reprogramming them. Or an attacker could sit near a home or business and wirelessly hack the meter from a laptop, according to Joshua Wright, a senior security analyst with InGuardians Inc. The firm was hired by three utilities to study their smart meters' resistance to attack.

These utilities, which he would not name, have already installed a few smart meters and plan to roll the technology out to hundreds of thousands of power customers, Wright said told the Associated Press.

There is no evidence that the security flaws have been exploited, although Wright said a utility could have been hacked without knowing it. InGuardians said it is working with the utilities to fix the problems.

California's largest utility, Pacific Gas and Electric Co., has installed more than 5 million SmartMeters throughout its territory. Company spokesman Jeff Smith said the utility, based in San Francisco, has taken steps to protect the meters from hacking. For security reasons, he declined to describe those steps.

"We've done extensive preparation to ensure the security of the SmartMeter network," Smith said.

PG&E was not one of the three utilities that hired InGuardians.

Power companies are aggressively rolling out the new meters. In the United States alone, more than 8 million smart meters have been deployed by electric utilities and nearly 60 million should be in place by 2020, according to a list of publicly announced projects kept by the Edison Foundation, an organization focused on the electric industry.

Unlike traditional electric meters that merely record power use - and then must be read in person once a month by a meter reader - smart meters measure consumption in real time. By being networked to computers in electric utilities, the new meters can signal people or their appliances to take certain actions, such as reducing power usage when electricity prices spike.

But the very interactivity that makes smart meters so attractive also makes them vulnerable to hackers, because each meter essentially is a computer connected to a vast network.

Alan Paller, director of research for the SANS Institute, a security research and training organization that was not involved in Wright's work with InGuardians, said it proved that hacking smart meters is a serious concern.

"We weren't sure it was possible," Paller said. "He actually verified it's possible. ... If the Department of Energy is going to make sure the meters are safe, then Josh's work is really important."

Here is another article regarding the security of smart meters.

<http://consumercal.blogspot.com/2010/01/experts-hack-smart-meters.html>

MONDAY, JANUARY 11, 2010

Experts Hack Smart Meters

I've written quite extensively on the growing debate over smart electricity meters and the potential threat they pose to privacy (if we don't take the proper precautions). Public Utilities Commission's (PUC) across the country are currently considering how to implement such a grid, and in response to a rule making by the CPUC, and the lack of attention being paid to the concerns of privacy advocates to date on this issue, **the Consumer Federation of California (CFC) recently joined The Utilities Reform Network (TURN)** in urging the Commission to allow for a more comprehensive review and debate regarding such concerns.

As I have written too, the CPUC has agreed to hold separate privacy specific hearings - with accompanying workshops and public comments.

Today I want to focus on an article in today's North County Times that highlights some of the "security" concerns I have been bringing attention to here.

As I wrote in an editorial on the subject in the California Progress Report a few months back,:

"The paradox of a smart grid system is that what will ostensibly make it an effective tool in reducing energy usage and improving our electric grid - information - is precisely what makes it a threat to privacy: Information (ours). It is this paradox that has led some to suggest that privacy might even be the "Achilles' heel" of the "Smart Grid". What are the unintended consequences of such a system?

Personal privacy issues routinely arise when data collected is harmless in isolation, but becomes a threat when combined with other data, or examined by a third party for patterns. A few principles we should keep in mind as we develop a regulatory framework for such a transition will be consumer control, transparency, and accountability."

In addition, I took on the subject of hackers, saying "**Hackers and criminals might seek to falsify power usage, pass on their charges to a neighbor, install a virus and take down the entire system, disconnect someone else from the grid, and plan burglaries with an unprecedented degree of accuracy.**"

I also delved into the subject of data and system protection:

3. How is your data protected? Utilities should be mandated by law, with strong penalties, to protect information against anyone who would seek to monitor/steal/manipulate it. The challenge here then is how to best protect the 1. Security of the Database and 2. Security of the Data in Transit (which could be trickier as it is wireless).

4. What happens if your data is breached: Consumers should be notified immediately in the event that personal

information has been obtained by a party without the requisite consent.

With that backdrop, let me get to the article in the North Count Timesentitled "Experts Hack New Power Meters".

Eric Wolff writes:

*Utilities say they have been hardening the smart meters since they began development, but security consultants say they are worried: **If criminals cracked the system, they could remotely install a virus that could shut down power for millions of customers.** The new smart meters will have a host of capabilities: They will credit homeowners who produce their own electricity via solar cells or wind mills, be able to wirelessly communicate data to the utility and let utilities turn off the power remotely, among other functions that could be added. "Were it telemetry only, then the only compromise is privacy," said Mike Davis, senior security consultant for the security service IOActive. **"When you add remote disconnect, then you increase the attractiveness of the meter as a target."***

Davis and his team hacked into smart meters last spring as part of a proof-of-concept they showed off at a Las Vegas security conference last summer. They reverse engineered meters they bought on eBay and found in trash bins near installation sites. Then they installed a computer virus that would replicate itself across the wireless network and block the utility from each meter as it went.

...

The demonstration may have also driven the federal government to create standards for smart meters in the previously unregulated smart meter arena. The National Institute of Standards and Technology, a branch of the Department of Commerce, released a draft of standards in September...

The encryption would apply primarily to over-the-air communications from the devices. In theory, a criminal could sit in a car up to a mile away from a site and attempt to hack the WiFi signal of the devices. Baker said that would be pretty hard. "It's called security in depth," Baker said. "The old technology is there's one key that could open every door in the neighborhood. In the systems employed today, you need a different key for every room in your house." Alternatively, a hacker could just try to wire directly into a meter.

...

Davis said he is pleased that there is third-party testing, but he is still worried about creating a monoculture of devices. Because all the smart meters installed by SDG&E and Edison will be made by the same company and use the same software, they're only as strong or as weak as any one unit. "If the attacker finds the vulnerability in one, the entire network is vulnerable," he said. "That's a catastrophic failure."

I can go on and on and bring in many more examples but I think there are enough proofs and enough materials to convince anyone who thinks hacking is some remote possibilities to think again. This is very serious and all experts admit that it is impossible to have 100% security with the wireless mesh grid and the smart meters. Again, I emphasis knowledge comes with responsibility. If the Commission goes ahead with the approval of this seriously flawed technology, then it has to be ready to face the inevitable consequences of potential lawsuits. The experts have spoken. It is up to those with common sense and wisdom to heel the advice. Contact those experts if you want. They will be much more honest and knowledgeable than the utility companies. There is no excuse for any utility company to force something so flawed on the ratepayers. If the smart meters were automobiles, they would be recalled long time ago. We just hope that we don't have to recall these meters. (Actually they did but for different reason. In San Diego 30,000 smart meters have to be swapped out due to software problems causing constant shut down of power to customers).

cc: Sedona City Council, Sedona Mayor Rob Adams, Yavapai County Supervisors, Yavapai County

Antonio Gill

From: Nancy Baer [redrockclass@msn.com]
Sent: Monday, September 26, 2011 4:57 PM
To: Tammy McLeod
Cc: Newman-Web; -web@azcc.gov; Burns-Web; Pierce-Web; Stump-Web; Kennedy-Web; 'Warren Woodward'; consumerinfo@azag.gov; 'Vicki Gray'; spierce@azleg.gov; KFann@azleg.gov; atobin@azleg.gov; 'Councilor Barbara Litrell'; 'Councilor Dan McIlroy'; 'Councilor Dennis Rayner'; 'Councilor Mark DiNunzio'; 'Councilor Mike Ward'; 'Mayor Rob Adams'; 'Vice Mayor Cliff Hamilton'
Subject: Response to your correspondence of 09/20/11 regarding placing smart meter installation "on hold" at my home
Importance: High

Dear Ms. McLeod:

I am in receipt of your letter dated 09/15/11 informing me that you have placed the smart meter installation at my home "on hold."

Apparently, you have misinterpreted my intention to not allow APS to install a "smart meter" on my home. Therefore, let me reiterate the reasons I am rejecting installation of any of your "smart meters," as I am unsure that you fully understand.

1. The Energy Policy Act of 2005, Section 1252, "Smart Metering" of that Law specifically stipulates "(C) Each electric utility subject to subparagraph (A) shall provide each customer **requesting** (not forcing or coercing) a time-based rate with a time-based meter capable of enabling the utility and customer to offer and receive such rate, respectively.

Page 16 of the Arizona regulatory portion of the "Demand Response and Smart Metering Policy Actions Since The Energy Policy Act of 2005: A Summary for State Officials"
http://www.ncouncil.org/Documents/NCEP_Demand_Response_12081.pdf clearly reiterates Federal policy regarding **offering meters to customers who request them.**

2. "Smart metering" is a **generic term** and therefore, there is much variation between these instruments (see "Demand Response and Smart Metering Policy Actions Since The Energy Policy Act of 2005: A Summary for State Officials," pgs. 12, 73 and 79). Your Company has failed to inform its customers and the Arizona Corporation Commission (ACC) details about the "smart meters" they are installing; what inspections those particular meters have had, any pertinent certification by Underwriters Laboratory, etc. That is unacceptable to me and hopefully to ACC.

Secondly, the World Health Organization's declaration that classified smart meters a **Class 2B carcinogen** according to the (100X exposure of cell phone, equivalent of living 500 feet of major cell tower). Furthermore, anyone who has, or had cancer, has a 30% chance of having it again, so any low level of emf is dangerous alone, but when you multiply that to include every dwelling in one's neighborhood, that compounds the effect. Since I am a thyroid cancer survivor, this is of great concern to me.

3. It appears that your Company and the Arizona Corporation Commission have ignored the proper interpretation of the Federal mandate and Arizona's own statement of intention (see above). ACC has failed to properly correct APS regarding its misinterpretation of the Federal and State mandate and its so-called public education outreach.

4. ACC has NOT taken proper steps by utilizing outside consultants to evaluate APS' various "smart meters" overall safety.

Last and not least, my health is of utmost importance to me and as I've stated previously I am not a candidate to be exposed to more radiofrequency than necessary. I call your attention and the Arizona Corporation Commission to the video of Columbia University's Law School "Wireless Hazards Conference in 2009," with Camilla Rees, founder of www.ElectromagneticHealth.org; attorney Whitney North Seymour, Jr., a co-founder of the Natural Resources Defense Council, and Martin Blank, PhD, of the Dept. of Physiology and Cellular Biophysics at Columbia University, a widely published scientist in this field <http://electromagnetichealth.org/electromagnetic-health-blog/columbia-university-law-school-wireless-hazards-panel/>.

Again, you do not have my authorization to install any "smart meter" on my dwelling now, or in the future, and I will exercise whatever legal remedies necessary to insure this.

Sincerely,

Nancy Baer


Sedona, AZ 86336

Antonio Gill

From: Meg Rockey [phxmeg@cox.net]
Sent: Monday, September 26, 2011 11:21 PM
To: Pierce-Web
Subject: About Smart Meters...

Hello Commissioner Pierce,

I want to write a short note to you to express my concerns about my APS smart meter. I understand there is no opt out or removal plan at this time.

My concerns are two-fold. First, the meter is attached directly outside my bedroom wall. I sleep less than 10 feet from this device and safety questions are an issue for me.

Secondly, I did not give APS permission to change my meter and have the capability to track my electrical usage to the extent they now have. I am more than happy to pay my electrical bill each month, but I feel APS is invading my privacy.

Please consider looking into these smart meters and allowing us, the consumer, to decide if this technology is something we wish to use.

Thank you for your attention to this matter.

Regards,

Meg Rockey
Phoenix, AZ

Antonio Gill

From: Craig and Monnie Ramsell [monnie@ramsell.net]
Sent: Monday, September 26, 2011 11:29 PM
To: Sedona City Council; Rob Adams; Cliff Hamilton; Barbara Litrell; Pierce-Web; Newman-Web; Burns-Web; Kennedy-Web; cfraulob@azruco.gov; web.bos.district1@co.yavapai.az.us; web.bos.district2@co.yavapai.az.us; web.bos.district3@co.yavapai.az.us; spierce@azleg.gov; atobin@azleg.gov; mdinunzio@sedonaaz.gov; dmcilroy@sedonaaz.gov; drayner@sedonaaz.gov; mward@sedonaaz.gov; Karen Fann; Sedona City Council; chip.davis@co.yavapai.az.us; Chip Cain; neal.brown@aps.com
Cc: Elizabeth Kelley
Subject: Formal complaint filed with ACC regarding an Itron AMR meter installed without consent on our property located at Unit M of 2085 Mountain Road, Sedona
Attachments: Smart meter whacky 007.JPG; Smart meter whacky 008.JPG

This is a formal complaint filed with ACC dated 9/26/11. I am enclosing an email copy because I was not sure whether the file submitted at the ACC site was transmitted properly. Otherwise, this will serve as a formal consumer email complaint.

Your Name: Monnie Ramsell

Address: [REDACTED]

Sedona AZ 86336

Name that appears on the Bill: Kailasa Enterprises LLC

Name of the Utility Company: APS

Email Address: monnie@ramsell.net

contacted the utility company X

Date: 9/26/11

Phone (Home) [REDACTED]

Cell Phone (don't and can't use one)

Account Number: [REDACTED]

Check here to confirm that you have already

Please summarize your complaint or inquiry:

We had made numerous calls to APS including another one today with the supervisor name Gail, ID Z96293. We had also sent an email on September 20th to Neil Brown at APS but had not heard back from him. We also sent another email to APS via their contact us page on their website. The email was sent after being given the runarounds by APS first claiming that we did not have any smart meter although our Itron meter is confirmed up-gradable to a full smart meter by the manufacturer. Then they changed the answer to not sure whether they could replace a meter for a commercial property even though they had promised they would do so in the first place when we called in to opt out. Then they changed it to customers really have no choice on what meters APS chose to put on their property. Then they told us that because of our rate plan, we need to have this meter. Lies, our rate plan have not changed for the last years. We had the flat rate 24/7 plan that does not require a multimeasurement TOU meter. If this is the only reason, we can switch to another plan that doesn't require one. We have the same rate plan for all the other units which all have analog meters. Then they flatly lied that all our meters were exactly the same. We have photos to prove it, anybody can tell the difference between an analog meter and an Itron AMR meter. At this point, APS could not even come up with any more excuses and told us disconnecting our service would be the only option to have the meter removed. We do not have any choice when ourselves and some of our tenants of the building have multiple sensitivities health issues. Nobody will feel any better until the RF generating meter is removed. We were quite disappointed that the conversation with APS went from blatant lies to pure insanity. Our only option left is to seek the intervention from this Corporation Commission.

We had requested not to have any smart meters or smart grid related devices installed on our commercial property located at the above address because of RF health and privacy concerns. We were assured by APS that our request would be honored and if any RF generating devices were installed, APS would remove and replace them with the analog meters.

We discovered among a bank of analog meters, there is a different meter installed at the above location for unit

M. It is an Itron/Sentinel AMR meter.

We went online to the Itron/Sentinel Site and found out this meter is an AMR meter up-gradable fully to AMI smart meter. At the ACC meeting, both the AMR and AMI meters are discussed. In fact, Tucson Electric Power's and UNS Electric's meters are all Itron AMR meters. This is from TEP's website, *"Although AMR meters lack many features associated with more advanced "smart meters," they can transmit usage data through a wireless radio frequency (RF) signal. These signals are received through fixed network equipment or remote collectors carried by TEP's meter readers."*

APS is having meter readers coming to our site to read these meters with the RF handheld receiver. These meters transmit RF signal.

On these meters, you can clearly read the following: CL 200 240V 3W TA 30 Kh 7.2
FM 2S 60 Hz

The following link is the spec. sheet for our meter.

<https://www.itron.com/na/PublishedContent/SENTINEL%20Solid%20State%20Meter.pdf>

This particular meter was installed on our commercial property without notification, discussion or consent.

When we called APS to request them to remove and replace this meter, the answer was we didn't have an Elster meter and therefore we didn't have a smart meter. When asked why their own website shows an Itron meter as example of what a smart meter looks like. The answer was that Itron was just a kind of technology and got nothing to do with being a Smart Meter. So we went to Itron's site to find out exactly what technology. So here is what Itron's website states,

At Itron, we're dedicated to delivering end-to-end smart grid and smart distribution solutions to electric, gas and water utilities around the globe. Our company is the world's leading provider of smart metering, data collection and utility software systems, with nearly 8,000 utilities worldwide relying on our technology to optimize the delivery and use of energy and water.

Next we contacted the Itron dealers to find out whether ours was a smart meter. Their answer was all models of the Itron meter are up-gradable to fully functional smart meters. So even if they are not presently one, they can easily be programmable and upgraded right there in the fields. In fact, the Sentinel and the Centron are some of the more popular models used. They also told us that it didn't really matter whether our is AMR or AMI, they would all work the same after the upgrades. In fact, they would consider all these meters as smart metering technology. So obviously APS was not telling the truth to their customers, to our city council members, or our county supervisors. APS' representatives lied to their customers while they continue to install smart metering ready meters around Sedona. It is equivalent of saying that your Intel PC is not really an Intel PC because it is a Dell and not a HP. APS' technicians even admitted the fact that ALL these AMR meters could be converted to smart meters. They are also aware of the fact that these meters generate and transmit RF.

The fact that we can no longer trust what APS is telling us regarding smart meters is disturbing. The Itron/Sentinel meter generates and emit RF. Nobody can easily tell whether the meter is upgraded to be a fully functional smart meter just by looking at it. We do not even want a potential smart meter sitting on our property. We have serious health concerns regarding our meter just the way it is.

We request an analog meter be replaced immediately at the earliest possible as promised by APS once upon a time. Analog meter is our only option when Radio Frequency is the issue. With all the thousands of analog meters that APS claimed to have replaced or is replacing, we are sure that they can find one fairly easily. In fact, these analog workhorse meters are still available over the internet. APS said the only option to remove the meter is to disconnect our service. I reminded them that we have been paying consumer and they did not have

the right to do so. What exactly was APS' promise to allow opt-out or temporary hold if our only option is to have our service shut off? Please intervene on our behalf to get this resolved as quickly as possible or we may run the risk of APS disconnecting our electricity. We had contacted APS too many times to try to resolve this issue but were given more lies and unreasonable excuses. This is really our last resort before APS shut our power because we refuse the AMR meter. Please remind APS that there is no federal mandate for the AMR meter or the AMI meter. We cannot have such a meter because of health reason.

Monnie Ramsell

Enclosed:

See attached for photo of our Itron/Sentinel AMR meter and photo of Itron AMR meter among other analog meters. You can clearly see APS is lying when they insisted all our meters are exactly the same.

cc: Sedona City Council, Sedona Mayor Rob Adams, Yavapai County Supervisors, Yavapai County Commissioners, Elizabeth Kelley, MHA.
Co-Coordinator, Arizonans for Safer Technology Infrastructure
Director, Electromagnetic Safety Alliance, Inc.
www.electromagneticsafety.org

This electronic mail transmission contains information from Kailasa Enterprises, LLC that may be confidential or privileged. Such information is solely for the intended recipient, and use by any other party is not authorized. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of this message, its contents or any attachments is prohibited. Any wrongful interception of this message is punishable as a Federal Crime. Although this e-mail and any attachments are believed to be free of any virus or other defect that might affect any computer system into which it is received and opened, it is the responsibility of the recipient to ensure that it is virus free and no responsibility is accepted by the sender for any loss or damage arising in any way from its use. If you have received this message in error, please notify the sender immediately by telephone (928) 282-6318
Thank you.

Donald and Linda Clark
[REDACTED]

Prescott, Az. 86305

APS Meter [REDACTED]

Ref: Complaint / Smart Meter

Dear Sir or Madam,

On Thursday, September 29, 2011 I received a knock at my door and two men from APS said they were here to install a new "Smart Meter" on our house. At first I was reluctant to have the meter installed but after talking with them we definitely did not want it installed. They could not answer if:

Arizona Corporation Commission regulation right now saying that we have to be forced to have the smart meter and no regulation by the Arizona Corporation Commission on what the consequences are if we keep the old one.

Privacy Concerns – do they know (APS) when I am on a computer, how many t.v.'s or computers are running.

Health Concerns –Has it been test for radiation admissions.

Remote Control shut off concerns – Can anyone access my account and add Kilowatt Hours, tap my account and charge me more cost with no way for me to confirm such charges, shut my power off without proper notification (they said the placed a door knocker on our door but we never saw it), because they are able to access my meter is it possible to slowly increase the speed of the meter and charge me more.

They state it has not been investigated or tested by Arizona Corporation Commission, how do we know what is being forced on us or could the concerns above become a reality.

After telling the two APS workers No, I need to investigate the meter first. They said no problem that I would be getting a call from the office and I will have to explain why I wouldn't let them install the meter. I said that is fine with me. On Friday, September 30, 2011 while I was away from my home for 1 ½ hours they returned and installed the meter. What is wrong with this picture? WE DO NOT WANT THE "SMART METER" I want my old meter re-installed. I have been trying to call 602-371-7171 Friday afternoon and today Monday and all I get is a busy signal. Until the Arizona Corporation Commission says they have tested this devise or order me to take it, WE DO NOT WANT IT.

Thank you for your time,

Donald and Linda Clark

Antonio Gill

From: Donald Clark [mrdonaldclark@gmail.com]
Sent: Tuesday, October 04, 2011 11:29 AM
To: Burns-Web
Cc: Newman-Web; Pierce-Web; Stump-Web; Kennedy-Web
Subject: Smart Meter
Attachments: Smart Meter.docx

Dear Ms. Burns,

Yesterday I sent the above attached letter to the Arizona Corporate Commission and today I called APS and explained to Linda (badge #72628) that her construction crews came to my home on Thursday and I told them not to install the Smart Meter until I have time to research it and then, on Friday came back and installed it any way. I asked Linda to re-install the old meter until I have time to investigate the new meter and she said no. She said, We own the meters and we are not going to re-install the old meter. I explained I filled a complaint with the Arizona Corporate Commission and she said they have the approval of the Arizona Corporate Commission and they would not replace my meter with the old meter. All she would say is they would not change out the smart meter. When I asked her for her last name she said I will give you my badge number only.

Don Clark


Antonio Gill

From: Craig and Monnie Ramsell [monnie@ramsell.net]
Sent: Friday, September 30, 2011 4:33 PM
To: Burns-Web; Newman-Web; Kennedy-Web; Pierce-Web; Stump-Web
Cc: Barbara Litrell; Cheryl Fraulob; Chip Cain; chip.davis@co.yavapai.az.us; Cliff Hamilton; dmcilroy@sedonaaz.gov; drayner@sedonaaz.gov; Elizabeth Kelley; Karen Fann; mdinunzio@sedonaaz.gov; mward@sedonaaz.gov; Neal Brown; Sedona City Council; spierce@azleg.gov; atobin@azleg.gov
Subject: Request of proof that APS smart meters transmitter approved for use by FCC

Dear Commissioners and Chairman,

Can we obtain a copy of the TCB (Telecommunications Certification Bodies) Grant of Equipment Authorization Certification issued under the Authority of the Federal communications Commission from APS regarding their Smart Meter Transmitter? This is the official FCC authorization for the APS smart meter transmitter that is being deployed throughout APS's service territory.

On this certification, there are details about exactly what frequency Range (MHZ) out Output Watts are approved for use.

Also it has details regarding the safety distance of the meter from all persons. This is important because APS never provided this safety information to their customers when they installed smart meters. We have to rights to have such information. We also want to find out what other safety restrictions the FCC required. For the Silver Spring one in California, it clearly states that it must not be colocated or operating in conjunction with any other antenna or transmitter except FHSS radio. It also states that End-users (which is us) and installers must be provided with antenna installation and transmitter operating conditions for satisfying RF exposure compliance.

During the special ACC Meeting, the question was raised about what are the Output Watts and APS claimed to be 1/4 Watts. We should see what is stated with the FCC Certification. The Silver Spring Networks has an output of 0.904 Watts. One of the attendee, Warren Woodward had commented that APS smart meters had output of 3 Watts and commissioner Newman was questioning about where the 3 Watts came from. Yes, 3 Watts is printed on the face of all the smart meter. See below. But I don't really think the real output is 3. Therefore, we need to look at this certificate from the FCC to see what output is approved and filed.

Sincerely,

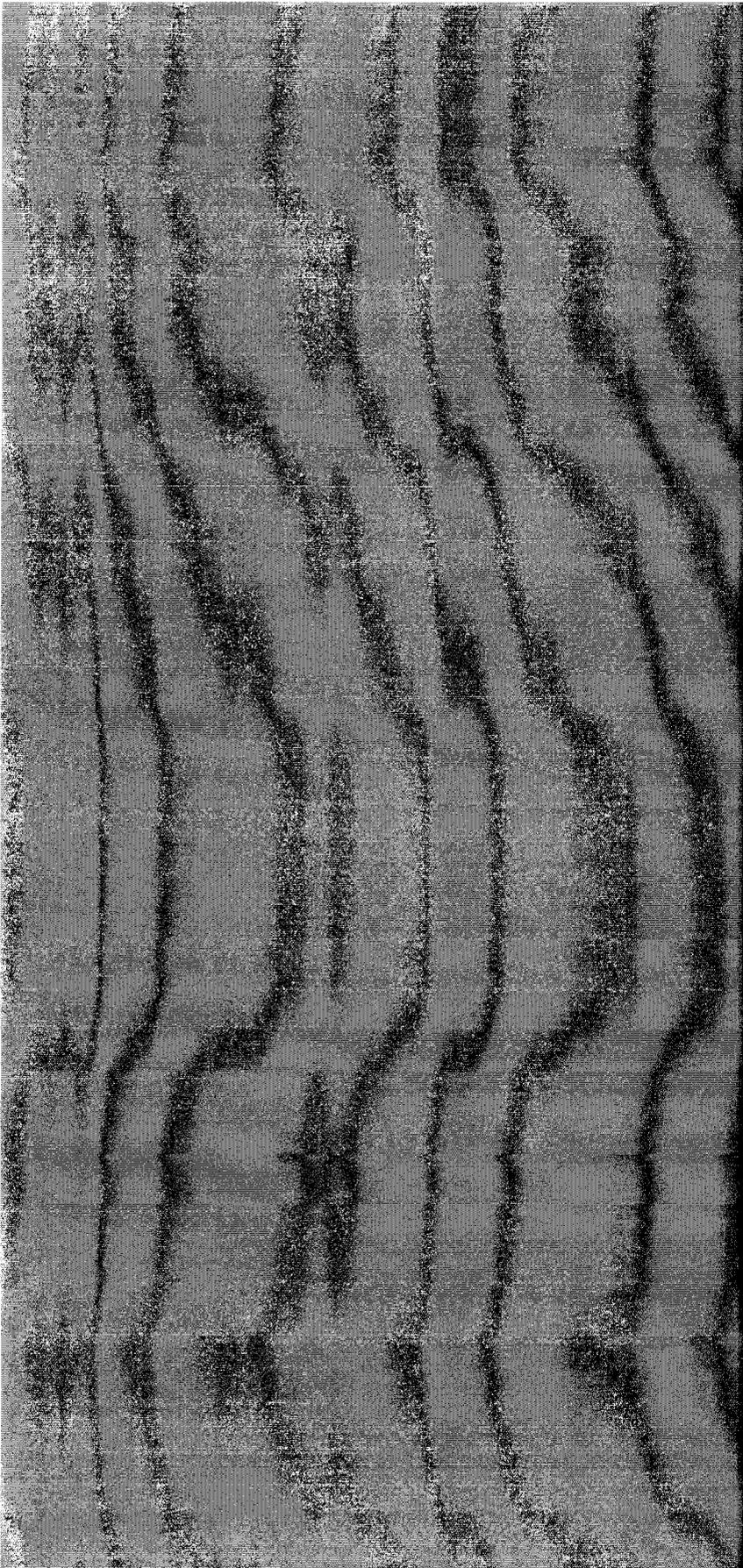
Monnie Ramsell

cc: Sedona City Council, Sedona Mayor Rob Adams, Yavapai County Supervisors, Yavapai County Commissioners, Elizabeth Kelley, MHA.
Co-Coordinator, Arizonans for Safer Technology Infrastructure
Director, Electromagnetic Safety Alliance, Inc.
www.electromagneticsafety.org

Encl:

This certificate looks something like this one for Silver Spring Networks in California.

<http://stopsmartmeters.org/wp-content/uploads/2011/09/OWS-NIC5071.pdf>

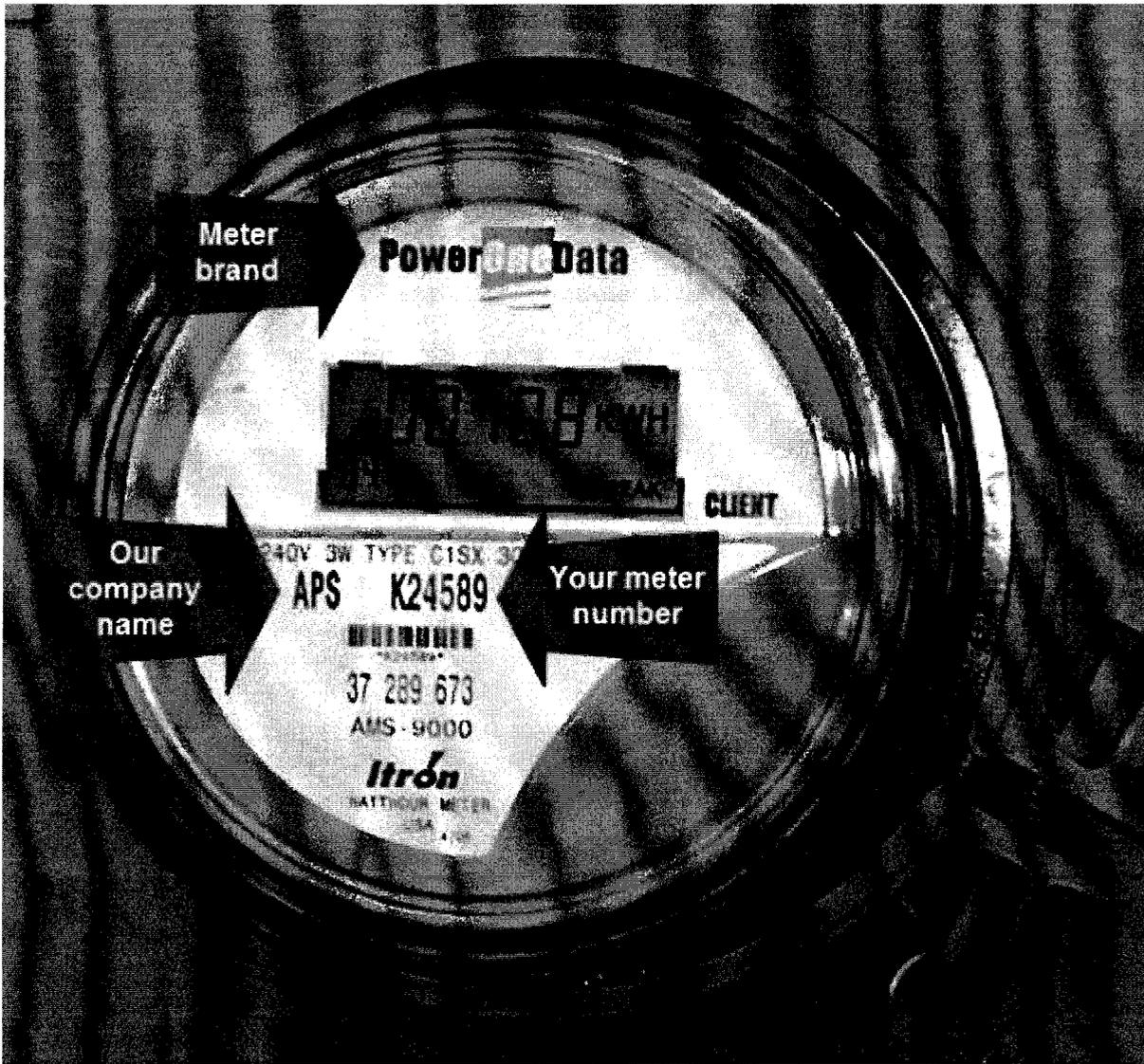


Name of Grantee: **Silver Spring Networks**

Equipment Class: **Part 15 Spread Spectrum Transmitter**
Notes: **Electric Meter Radio Module**
Modular Type: **Limited Single Modular**

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHZ)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
	15C	902.3 - 926.9	0.904		

Class II permissive change filing. Output power listed is conducted. Limited single module approval requires professional installation. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter except FHSS radio as documented in this filing. End-users and installers must be provided with antenna installation and transmitter operating conditions for satisfying RF exposure compliance.



Antonio Gill

From: Kristin Monday [kristinmonday@yahoo.com]
Sent: Sunday, October 02, 2011 11:28 AM
To: neal.brown@aps.com
Cc: Newman-Web; Burns-Web; Pierce-Web; Stump-Web; Kennedy-Web
Subject: Neal, Smart meters and the take down of our country

Neal,

I know you have a job and want to keep your job and you need think about what is really going on with smart meter deployment.

Arizona needs to be saved from smart meters (real people and families).

There comes a point in life were money is not the be all and end all. We need to be cleaning up our environment, not polluting it further.

These smart meters and the smart appliances will turn into a mass genocide of illness and disease for humans and wildlife.

Smart meters are a small cell phone tower on the side of every house, all talking to each other and all the appliances; this is human folly at its greatest.

<http://theintelhub.com/2011/09/30/they-want-us-dead-%E2%80%93-red-level-alert-america/>

I hear APS is no longer giving an opt out option? Is this true? No one knows what will happen when a smart meter is on and all the appliances are smart enabled also. I think it common sense to expect even more people to become RF sensitive, higher cancer rates, more sleep disorders, etc., etc..

Kristin

cc: Arizona Corporate Commission

Here is a letter recently sent to the CPUC by engineer Rob States:

[To view a video of a recent presentation by Rob, click [here](#).]

Two engineers have been diligently working on Smart Meter dirty power and RF issues – the combined team possess two MS degrees from MIT, a California P.E. license (Professional Engineer's License), and a PhD from Stanford in Electrical Engineering, Magna Cum Laude. They have been working on this nearly continuously for the last four months.

The scientific data tells us that 5% of the population will get sick immediately from RF disease, and another 10% will develop the disease over time. This means about 4.5 million people in California are potential victims.

Since individuals with no history of RF disease are experiencing symptoms the first day the meter is installed, we can assume the meter's RF emissions are not the only problem. The RF network is activated months after initial meter installation.

Extensive measurements have demonstrated that all of the meters measured so far, including ABB, GE, and Landis Gyr, emit noise on the customer's electric wiring in the form of high frequency voltage spikes, typically with an amplitude of 2 volts, but a frequency any were from 4,000 Hertz, up to 60,000 Hz. **The actual frequency of the phenomena is influenced by the devices that are plugged into the customer's power.** Some houses are much worse than others, and this observation has been confirmed by PG&E installers that have talked to us.

Since 85% of the population is not immediately effected by this phenomena, the knowledge about what is causing symptoms in PG&E's customers will be slow to evolve. We expect word of mouth to be the primary information source since the media is so disconnected from this phenomena.

The scientific literature has studied microwave illness since the 1930's when radar operators became ill. Radar equipment emits radiation that is intermittent, and recent scientific papers have increasingly reported that pulsed radiation is significantly worse than continuous radiation. Humans have been exposed to continuous microwave transmissions from radio for decades. Exposure that Smart Meters present to California citizens is new and unlike previous electromagnetic emissions.

PG&E has published none of the functional specifications of the meters now being installed, including their BLOCK DIAGRAMS, SCHEMATICS, or BILL OF MATERIALS. The scientific community has been prevented from identifying any of the design problems prior to their installations.

The decisions by PG&E and the CPUC to conduct NO SAFETY STUDIES has forced them to discover the current problem after the meters have been installed and after significant capital has been invested in this project. Even a rudimentary safety test with 100 randomly selected people would have probably uncovered this problem long before its appearance in PG&E's customer base.

The fix for preventing dirty power disease in PG&E customers is expensive. Because the dirty power must be stopped in the customer's LOW IMPEDANCE house wiring, all of the filter components must handle high power, and therefore are expensive. Current estimates put the end customer cost at \$500, and that does not include fixing dirty power interactions that Smart Meter causes with devices already in the customer's home, such as computers, FAX machines, copiers, plasma TV's, and the like. Merely treating 15% of the California households puts the total liability for after market problems at \$2B, approximately equal to the entire cost of the existing program's roll out.

Though 15% of the population has early and obvious symptoms, a large number of microwave disease related health problems will not surface for some time. As science advances, the links between microwave disease and its sources will only improve, causing ever increasing liability for societal institutions that are responsible for the offending emissions. Though the cell phone industry has purchased immunity from liability through their extensive lobbying efforts, the experience of the tobacco and chemical industries has shown that this immunity can fade as priorities of the general population affects the political process.

Though microwave disease is not directly observed in 85% of the population, the asymptomatic effects (meaning effects that have no apparent symptoms) are well published in the scientific literature, and span a wide variety of lethal and debilitating diseases, including cancers, auto immune diseases, suicide risk, depression, tinnitus (ringing in the ears), and a host of others. Steve Job's pancreas and liver problems are particularly conspicuous when manifested in a life long vegetarian who was chronically exposed to pulsed microwave emissions from wifi, computer power supplies, and the like. Liability for microwave diseases could explode in the future, as data in the cell phone industry already suggests.

Among the population of affected individuals, there are sure to be attorneys who are experienced in class actions suits, and who clearly recognize a \$2B avoidable cost has been imposed on an unwilling public. This type of law suit has been responsible for some of the largest corporate liabilities in our civilization's history, and has already affected PG&E and the CPUC in the past (i.e. hexavalent chromium in Hinkley CA).

Once the California real estate community becomes aware that 15% of the general population will no longer be able to live, work, or shop in their properties, the potential liability will be in the trillions of dollars, and will effect a population of wealthy individuals who have significant political influence in Sacramento **(think Sedona and Scottsdale here)**. These entrepreneurs have been particularly skilled at legally punishing institutions that are responsible for declines in their asset values. In fact, the asset base of the retirement trust of California's state employees is significantly exposed to California's real estate market.

A reasonable person could conclude that the potential liability PG&E currently faces, both immediately and in the evolving future, could be significantly larger than their asset base. Their long term survival as a corporation could be at risk, and a potential outcome could include the wholesale transfer of their asset base into receivership pending settlement of outstanding liabilities.

Legal liability could force PG&E (**APS**) to approach the CPUC (**ACC**) for a doubling of the existing utility rate. This would be a politically untenable request, and could result in the dissolution of the CPUC's existing regulator authority.

The future for both the CPUC and PG&E is uncertain, and potentially disastrous. A prudent course would be to treat the entire Smart Grid project in California as a major risk, and to aggressively engage in damage control. Since the technology that is actively being dismantled by the CPUC and PG&E has previously demonstrated none of the current risks, an aggressive plan to offer an analog meter opt out is a prudent option. Since so much damage has already been done, there are no guarantees that even this measure will prevail.

PG&E's current course of relying on PR spin has little chance of stemming the trends that have already been set in motion.

Rob States, M.S., P.E.
Chief Engineer, Wave Dry, LLC.
415-927-2739 Office
415-596-2718 Cell
=====

THIRTEEN FATAL FLAWS OF SMART METER TECHNOLOGY

- 1) **WHO International Agency for Research on Cancer classifies RF-EMF as a 2B (Possible) Carcinogen (May 31, 2011 in Lyon, France)**
This is the same kind of RF-EMF as smart meters produce and at equivalent levels to those on which the IARC finding was made.
- 2) **Excessive Billing** (monthly electric bills doubling or tripling every month, with no increase in energy usage)
- 3) **Excessive Cost to Ratepayers** to install additional power transmitters and home LAN (wireless devices) at later date
- 4) **No Evidence of Energy Savings** for Ratepayers (not a green, energy-saving program as promoted)
- 5) **Incompatibility with Solar** (at present, wireless smart meters = no solar = an energy conservation disincentive)

- 6) **Threat to Privacy of Personal and Financial Information** (utilities have no experience and no competence to protect wireless information)
- 7) **Threat to the National Electric Grid** (from hacking and terrorism (well-documented by the Department of Homeland Security, the National Security Agency, and the CNN program CyberAttack (2010) on risks from electronic hacking of electric, banking and transportation systems at national level.
<http://www.wired.com/threatlevel/>
latimes.com/news/nationworld/nation/la-na-cyber-war-20110328,0,6416856.story
<http://www.dailymail.co.uk/news/article-1254305/Terrorists-hijack-new-meters-cause-blackouts.html>
- 8) **Threat to Personal Safety** (wireless systems including security systems, wireless locks, baby monitors are hackable and may be disabled: and home use patterns, including your vacation schedule, may be visualized by wireless hacking from the street).
- 9) **Violation of FCC Public Safety Standards**
<http://sagereports.com>
- 10) **Health Effects of Low-Intensity Radiofrequency and "Dirty Electricity" Effects on Health and Well-being** (on healthy populations and on those with chronic diseases, those being treated for cancer or neurological diseases, those with sleep disorders, and on the developing fetus and on children whose central nervous systems continue to develop into their late teens).
- 11) **Threat to People with Medical Implants** (The Department of Justice Americans With Disabilities Act is taking testimony now).
- 12) **Threat to Use of Electronic and Wireless Devices** (already in use in homes and businesses – think wireless security systems).
- 13) **Threat to Electrical Wiring Safeguards** (arc-fault interrupters, ground-fault interrupters that are mandated under the NEC) and fires and explosions following installation of wireless smart meters. <http://www.click2houston.com/news/28147128/detail.html>
<http://www.wfaa.com/news/Fires-Spark-During-Smart-Meter-Installations-101115429.html>
- 14) **Dead appliances and devices** that need to be replaced due to damage caused by smart meters. This will lead to billions being spent on new smart appliances!

"PG&E has determined that certain models of Ground Fault Interrupter (GFI) breakers (such as those used in hot tubes) may be impacted if they are in close proximity of the meter" (Structure Consulting Group Overview, p 32). GFIs are a safety feature in residential and commercial electrical systems that are intended to protect people from electric shock and possible electrocution. The GFIs also disconnect electrical circuits when they are overloaded to prevent fires and other property damage. Although PG&E has asked the Smart Meter manufacturers to develop low power transmitter solutions to the GFI interference issue, and has trained the installation contractors to listen for GFI

tripping upon installation of a new meter, this does not protect people where the current generation of Smart Meters that have been or will be installed (David L. Wilner, 2010)

y...