

## **Briefing Letter on Electric Utility Smart Meters**

This briefing letter highlights information about wireless smart meters and some of the problems being reported where they have been installed. There is information below about health, safety, security and economic concerns that are being voiced around the country by consumers, utility analysts, economists, internet security experts and parents.

### **What is the Program About?**

The utilities tell us the program is intended to provide a residential energy management tool. It is intended to reduce energy consumption by providing computerized information to customers about what their energy usage is and how they might reduce it by running appliances during 'off-time' or 'lower load' conditions. This will save utilities from having to build new facilities for peak load demand. Your utility will install a new smart meter on every building that it supplies electrical service to. In Southern California, that is about 5 million smart meters in three years for a cost of around \$1.6 billion dollars, which ratepayers will be asked to pay for. Pacific Gas & Electric in northern California is installing them for all customers at \$2.2 billion dollars.

If consumers decide to join the program (so that appliances can report energy usage to the utility), they can be informed about using energy during off-use or low-use periods, but they will be required to install additional wireless power transmitters on appliances inside the home to do so.

*"Proponents of smart meters say that when these meters are teamed up with an in-home display that shows current energy usage, as well as a communicating thermostat and software that harvest and analyze that information, consumers can see how much consumption drives cost -- and will consume less as a result. Utilities are spending billions of dollars outfitting homes and businesses with the devices, which wirelessly send information about electricity use to utility billing departments and could help consumers control energy use."* Wall Street Journal, April 29, 2009.

### **Mandatory Installation**

No one can opt-out. Utilities have received authorization in many states to install them. However, the public can refuse to install the power transmitters on appliances inside their home.

### **Community Concerns and Issues**

The program is expensive with very little demonstration that consumers will want this service, or choose to participate. They include economic concerns, lack of privacy of personal information, easier disconnection of service, health and safety concerns, reliability, increased vulnerability to hacking, increased risk of planting of malicious software on networks, security risks when away from home (burglaries), fire risks, explosions, interference with critical care equipment (medical), and meter overcharges.

### **Economics**

The economic justification these billion dollar programs is that the costs will be offset by energy savings. The system is supposed to allow variable-pricing of electricity to discourage heavy usage during peak periods like hot summer days. The benefit to variable pricing is supposed to

be that it will give people incentive to decrease energy usage when wholesale energy prices are highest. However, the costs to build up the new infrastructure are very high, with little information about whether or when consumers might decide to participate.

Customer compliance might be low, once the ramifications are better known. In order for there to be any energy savings, customers must first choose to participate, and install 10-15 power transmitters that radiate radiofrequency/microwave radiation inside the home to signal the smart meter.

100% compliance, or even 50% compliance is unrealistic. What percent compliance is realistic is unknown, but where consumers are educating themselves on the costs and benefits, there is significant resistance. The business case is not proven. Ratepayers will have to pick up the bill for risky billion-dollar investments that benefit the utilities bottom-line, with no assurance that energy savings will be worth the price. The economics do not look reasonable.

### **Invasion of Personal Privacy**

The use of wireless networks to relay energy information leaves open the potential for misuse of personal data, billing and usage information, and other private information. Privacy breaches have already been documented (illegal access of 179,000 accounts at Hydro Toronto, for example). It also may increase burglary risk, since home electrical usage is made electronically visible. When unoccupied, the home uses less electricity.

Its like advertising to criminals with wireless detection equipment that you are not home.

### **Vulnerability to Hacking and Intentional Sabotage**

Smart meters are alleged to open up the potential for hacking into personal wireless networks used for banking, bill paying, and private communications.

Concerns over the security of the US electrical grid have received widespread media coverage (Wall Street Journal April 27, 2009). Smart meters provide a new vulnerability to intentional sabotage as well as to inadvertent access to private information, since the network is wireless and it adds direct linkage to home computers and personal data.

The wireless network proposed to enable smart grid and smart meter technology is a full-saturation, full-coverage RF blanket of wireless into every home and business that can increase the points of entry for malicious software (malware), to electrical service disruption or disconnection, and to terrorist attack on the electrical and communications grid throughout the country (Wired.com, March 4, 2010).

CNN launched a “Cyber Shockwave” program that detailed national concerns over the security of the internet and of wireless communications, which makes us vulnerable to loss of the electrical grid, internet and wireless communications across the country (February 20, 2010). Banking, transportation and the electrical grid had the biggest vulnerabilities.

### **Accuracy in Billing – Meter Overcharges**

There are widespread reports of excessive charges, due to malfunctioning smart meters. In Bakersfield, CA, where PG&E started installing the first smart meters, more than 100 people attended a meeting held by State Sen. Florez to complain about absurd electric bills. Those with new smart meters had bills 200-400% higher, with no increase in power use as compared to the same months of the previous year. The meters are thought to malfunction because of spurious RF signals (electronic glitches). It is reported that high frequencies can make disc type electric meters spin faster, making it appear that more electricity has been used than actually has. For this reason, electrical bills have also increased near cell antenna towers for the same reason (high radiofrequency environments). A class action lawsuit has already been filed in Bakersfield, CA because of numerous consumer complaints.

### **Health and Environmental Concerns**

Some utilities have provided technical reports on radiofrequency/microwave emissions. They all say the smart meters are “*in compliance with FCC public safety limits*”. However, the RF reports indicate that the smart meter will produce over 300 microwatts/centimeter squared near the meter, and this will produce elevated RF both inside and outside the home. Chronic exposure to radiofrequency and microwave radiation is still considered a potential health risk, and studies continue at NIEHS and at the World Health Agency to determine actual health risks. These smart meter RF/MW levels are far higher than those already reported to cause health risks. Compliance is not safety, since the existing FCC safety limits are under challenge, and have already been called ‘insufficient to protect public health’ by some federal agencies.

The power transmitters that also have to go inside the home (on each appliance that is reporting to the smart meter) produce high, intermittent RF in short bursts. If the consumer does opt-in to a smart meter program, he/she will have to install multiple power transmitters (one per appliance) inside the home at additional cost for the wireless thermostat, power transmitters and wireless display). These power transmitters are another source of RF, and some calculations show they emit short, but powerful bursts of RF up to several thousand microwatts per centimeter squared. These bursts will occur both day and night, perhaps several times a minute.

To date, none of the technical RF reports we’ve reviewed is able to predict the cumulative RF from the smart meter plus the power transmitters inside the home, the intervals of RF transmission, and the additional RF transmissions from neighboring homes that can ‘piggyback’ on your smart meter system. This ‘piggybacking’ part of the system means that other homes can put additional RF signals through your meter, if they don’t have a good signal to the utility’s reporting cell antenna network.

### **Electromagnetic Interference**

Wireless medical devices in use within homes may malfunction. Spurious radiofrequency signals are already reported in published studies to interfere with critical care equipment, ventilators, pain pumps, wireless insulin pumps and other medical devices. There does not appear to be any



testing results on the effect of smart meters and critical care medical implants and devices in advance of their deployment, but the issue is real.

There can also be interference with other electronic devices (home office printers, FAX, scanners, computers, television and cable settings, security systems, etc). Appliances and devices that are electrically connected in the home (plugged into home electrical wiring) may experience RF bursts of high enough intensity to cause malfunction and/or damage. These events are reported where smart meters have been installed.

### **Fires and Explosions**

There are reports in Bakersfield, Berkeley and from some Alabama and New Zealand communities that the installation of smart meters caused fires (15 reported in Bakersfield, one explosion of a smart meter). These reports are in various stages of confirmation, and cannot be fully substantiated at present. There is theoretical reason to believe that, in some cases, wireless smart meter signals may overload electrical wires and cause or contribute to circumstances resulting in house electrical fires. Unintentional re-radiation of RF signal

(with its higher energy) on electrical wires may overload wires, particularly in poorly grounded or ungrounded homes, or homes with older wiring or faulty wiring.

There are reported events that such fires have happened at or around the time smart meters have been installed. This matter needs urgent attention, and an independent investigation by the State Fire Marshall is needed.

It may also increase the risk of wildfire in heavily wooded areas and rural/urban interface areas of the state.

### **Mandate**

The federal government, through the Obama stimulus package, has supported the rollout of this new technology. The California Public Utilities Commission has authorized PG&E, SCE and SDG&E to install new smart meters as part of the SmartGrid energy conservation ideal. In other parts of the country like the State of Connecticut, officials have required a 'go-slow' approach to testing first. However, no agency has mandated that the meters be wireless, thus opening the conversation to "why not hard-wired, shielded cable"? This has few to none of the vulnerabilities raised above, and would likely result in much higher consumer acceptance and buy-in.

Thank you for taking time to read and understand these important issues.

Cindy Sage, MA  
Sage Associates  
Co-Editor, BioInitiative Report  
1396 Danielson Road  
Montecito, CA 93108  
(805) 969-0557

sage@silcom.com