BEFORE THE

PENNSYLVANIA PUBLIC UTILITY COMMISSION

MARIA POVACZ	:	
	:	Docket No. C-2012-2317176
v.	:	
PECO	:	

RECEIVED
OCT 22 2012
PA PUBLIC UTILITY COMMISSION
SECRETARY'S BUREAU

EXCEPTIONS TO THE INITIAL DECISION

MARIA POVACZ

Secretary

PA Public Utility Commission

400 North Street

Commonwealth Keystone Building, 2nd Floor

Harrisburg, PA 17120

DATED: October 22th, 2012

RECEIVED

OCT 22 2012

PA PUBLIC UTILITY COMMISSION
SECRETARY'S BUREAU

TABLE OF CONTENTS

APPENDICES

I. INTRODUCTION

As per the American Recovery and Reinvestment Act of 2009 (ARRA), one of Pennsylvania's utility – PECO, received a $200 million grant, the maximum approved under ARRA, to accelerate the deployment of smart meters throughout its service territory. This deployment is furthered by the Act 129, act that was signed into law October 15, 2008 (effective November 14, 2008). In January 15, 2009 the PUC (Commission) identifies implementation timeline, standards of plan review and resolves other issues (Docket No. M-2008-2069887). On February 5, 2009 the Commission establishes standards for registration of "conservation service providers" (Docket No. M-2008-2074154). On February 20, 2009 the Commission seeks comments on Technical Reference Manual (Docket No. M-2008-2069887). In March 2009 the Commission establishes conservation and peak demand reduction baselines. Commission issued an RFP for statewide program evaluator. On July 1, 2009, the impacted EDCs file energy efficiency and conservation plans and the Commission has 120 day review window. On August 14, 2009, all EDCs with more than 100,000 customers, file smart meter procurement plan. In January 1, 2010 (or end of rate cap) the EDCs file Time of Use and Real Time Price Plan. As per the Smart Meter Procurement and Installation Implementation Order, Docket No. M-2009-2092655 entered June 24, 2009, PECO is obligated to move forward with its smart metering procurement and implementation. (Appendix 01-page 2)

While PECO is responsible to deliver electricity to me as a customer, PECO has no rights in forcing its customers to attach RF transmitting equipment to their house to collect private data. Forcing the customer to attach said device, without customer consent in facilitating and sharing PECOs collection of data from other homes, imposes a permanent physical occupation of my residence without consent and without just compensation hence this constitutes a violation of the Fifth Amendment of the United States Constitution. This is especially true in PA where the customer does not have an option to opt out of this installation. Currently, the duty of usage data collection is however sufficiently and accurately satisfied by the current meter in place.

Furthermore, in its tentative order, at its public meeting held June 30, 2011 "The Commission agrees that these current practices of providing Dual Billing and Bill Ready Consolidated Billing should be approved for the enrollment and billing of EGS customers who purchase service under a real-time and time-of-use pricing option for all EDCs" (Appendix 01-page 5). As I am not enrolled or willing to enroll in a real-time and time of use pricing option, have no use for the Dual Billing, Bill Ready Consolidated Billing nor a smart meter. Furthermore, in the context of the said tentative order (Appendix 01- page 2) noted above, "the Implementation Order required covered EDCs to address, among other things, standards and formats for electronic data communications with customers and customer authorized third parties. Specifically, the Commission noted that these <u>EDCs were required to implement an EDI transaction related to customers enrolled in a real time price or time-of-use rate program</u>, as well as a new historical interval usage transaction, in order to provide customers and their designated agents with 12 months of interval usage data".

Why given the above statement, is the Commission discounting the rights of the customers that have not explicitly enrolled in such real time price or time of use rate programs? As per the above statement, customers must be enrolled in such programs, and I do not have any written documentation consenting to such enrollment. I am

more than capable of managing my electric consumption and saving costs without the use of the real time price or the time of use rate program benefits, programs that the Commission emphasized in its dealings with the EDCs.

Additionally, in the context of the above mentioned document (Appendix 01-page 9), "EDEWG is to review each EDC's current smart meter plan for provision of the following required functionality: a) To provide customers with direct access to hourly usage and price information; b) To provide support for automatic control of a customer's electricity consumption by the customer, the utility or a customer's agent (at the discretion of the customer); and c)To provide direct meter access and electronic access to customer meter data by third parties with customer consent.

I am the customer and I do not wish to be provided with direct access to my hourly usage and price information, I do not wish to be provided with automatic control of my consumption and last but not least I do not wish to have to be provided with direct meter access and electronic access to my data nor I want third parties to have access to any of my data with or without my written consent. These are the bases of smart metering technology as mentioned in the previous citation so if the existence of the smart metering is to satisfy the above 3 reasons and I do not want any of these reasons to be satisfied in the case of my account, why is the smart metering going to be installed?

Furthermore, EDCs may fully recover reasonable costs via customer paying for installation costs (approximate $300 per unit installed). As Act 129 specifies, EDCs shall furnish smart meter technology as follows: (i) Upon request from a customer that agrees to pay the cost of the smart meter at the time of the request; (ii) In new building construction and (iii) In accordance with a depreciation schedule not to exceed 15 years. Electric distribution companies shall, with customer consent, make available direct meter access and electronic access to customer meter data to third parties, including electric generation suppliers and providers of conservation and load management services. Is the word shall in the context of data sharing is also interpreted to also mean every customer? If so, given the Commission's believes that it was the intent of the General Assembly to interpret to word shall to mean every customer receives a meter, (in the context of "Electric distribution companies shall furnish smart meter technology"), why the customer gets to consent on the data sharing and not on the meter installation? How is the customer going to cope with the installation costs in the case of the "depreciation not to exceed 15 years" point above if the customer has no right in agreeing or disagreeing to pay for such device? Are we at the mercy of PECO that could impose such installations costs upon its customers every time equipment is depreciated? If PECO decides on the depreciation timelines (not to exceed a certain number of years) then PECO should support the costs of such installation to allow for the installation of the updated metering technology. If the customer does not have a say in the depreciation timing nor has an option to opt out, then why is the expectation for the customer to fund such changes?

Furthermore, if the customer is given the right to consent on a meter installation and the customer does not give its consent, then the data sharing to third parties becomes a moot point as there is no data to share. Data sharing to third parties allows customer consent but the sole meter installation (where customer pays for the installation

costs approximated at $300 per unit) does not give the customer the right to consent? This seems rather illogical to me as the customer is rather financially impacted by its inability to consent to the meter installation.

PECO did not send any notifications to me related to my rights as a customer in regards to this installation of smart metering project nor PECO educated his customers with regards to the hidden installation costs to be passed on to the customer. Instead, I just received an inconspicuous notice (June 15, 2012 PECO letter previously provided as evidence) mentioning that a new meter will be installed. Why PECO is failing to disclose to its customers, prior to the meter installation, that the customer will be paying for the installation costs of such meter? This is a practice that should be investigated by the Commission. PECO failed to disclose these hidden costs to its customers and rather began installation without customer consent (if the meter is easily accessible). The Office of *Consumer Affairs should also investigate this matter as the Customer is impacted by the lack of nondisclosure and* the later has to pay the costs associated with this smart metering technology via rate increases. This approach is rather discriminatory for those of us that live of fix incomes and do not have these extra funds available.

How are the public interests and specifically my interests being protected when I am requesting in writing that this meter not be installed at my residence and my request is being dismissed? How I am being protected as a customer, when I am being forced to pay for a device I do not want or need? Because of PECOs actions and omissions my family and I have suffered and will continue to suffer injury and irreparable harm and because of dismissal of my Initial Complaint, how are my rights of due process in light of the Fourteen Amendment impacted by the dismissal?

Other customers have expressed similar concerns and have reached out via the Consumer Protection, PA PUC or their state and local representative hence the Bill 2188 now with the Consumer Protection since February 2012. Why are the voices of these consumers discounted and put aside?

Is this a matter of strictly economics? Not allowing a smart meter install supports Pennsylvanian's by allowing the existing meter reader to keep its job rather than joining the unemployment lines. Furthermore, PECO is the sole provider and, I, the consumer, do not have another option aside disconnecting from the grid, disconnect that is not possible under my current circumstances. Monopoly in this case is synonymous with forceful installation or termination of service. Is this the mechanism to compensate outstanding citizens that have never been late in paying their bills? In today's society, electricity is a basic need. I am to be denied of this basic need by the simple refusal to have a smart meter installed?

Furthermore none of the Federal Legislation in any way mandates utility customer participation in a smart *meter program or a smart grid. The Energy Policy Act of 2005 (Public Law 109–58—AUG. 8, 2005 119 STAT. 965* http://www.gpo.gov/fdsys/pkg/PLAW-109publ58/pdf/PLAW-109publ58.pdf (Appendix 2) very clearly establishes an optional standard by which utilities are required to make "time based metering and communication" available upon customer request. I am not interested in participating in this experiment nor, I have been requesting to participate in a time-based rate schedule so the Commission must reconsider its Initial Decision in light of this evidence.

PECO is rushing forward with the installation of these devices throughout my neighborhood despite a long list of safety, health issues, cyber security and privacy concerns some of which involve constitutional violations. I request once more that PECO be required to stop the smart metering installation at my residence until appropriate safeguards are in place and a common sense alternative is made available to the customers that do not wish to participate. By forcing its customers to accept smart meters PECO has not provided the freedom of choice mandated by the Energy Policy Act of 2005 and is therefore in violation of 16 U.S.C. § 2621(d) 14 (a) cited above.

II. EXCEPTIONS

MP Exception No. 1: The Energy Policy Act of 2005 (Public Law 109–58—AUG. 8, 2005 119 STAT. 965) establishes an optional standard by which utilities are required to make "time based metering and communication" available upon customer request.

A. Introduction

The Federal Legislation does not in any way mandates a utility customer participation in a smart meter program or a smart grid. The Energy Policy Act of 2005 (Public Law 109–58—AUG. 8, 2005 119 STAT. 965) very clearly establishes an optional standard by which utilities are required to make "time based metering and communication" available upon customer request (Appendix 02-pages 371 and 372).

B. Customer must request participation in time based metering and communication

As such, as per Section 1252- SMART METERING (a) IN GENERAL—Section 111(d) of the Public Utility Regulatory Policies Act of 1978 (16 U.S.C. 2621(d)) is amended by adding at the end the following: "(14)TIME-BASED METERING AND COMMUNICATIONS—(A) Not later than 18 months after the date of enactment of this paragraph, each electric utility shall offer each of its customer classes, and provide individual customers upon customer request, a time-based rate schedule under which the rate charged by the electric utility varies during different time periods and reflects the variance, if any, in the utility's costs of generating and purchasing electricity at the wholesale level. The time-based rate schedule shall enable the electric consumer to manage energy use and cost through advanced metering and communications technology."

(Appendix 02-pages 371 and 372) http://www.gpo.gov/fdsys/pkg/PLAW-109publ58/pdf/PLAW-109publ58.pdf

C. Conclusion

The Commission shall reconsider its initial response and dismissal of my claim in light of the above findings as the Federal legislation specifies that the customer must consent to the time based metering and communication while the Act 129 is not explicitly allowing for customer opt out. Given it's inexplicitly with regards to customer right to opt out, Representative Mike Reese is seeking to amend Act 129 via Bill 2188 currently referred to Consumer Affairs since February 8, 2012 further providing proof of incompleteness of Act 129 stipulations related to

customer's rights (Appendix 03)
http://www.legis.state.pa.us/cfdocs/billinfo/billinfo.cfm?syear=2011&sind=0&body=H&type=B&BN=2188

MP Exception No. 2 The Commission has administrative power and authority to supervise and regulate all public utilities doing business within this Commonwealth

A. Introduction

The Commission, as per its mission statement, "balances the needs of consumers and utilities to ensure safe and reliable utility service at reasonable rates, protects the public interest; educates consumers to make independent and informed utility choices; furthers economic development; and fosters new technologies and competitive markets in an environmentally sound manner" www.puc.state.pa.us (Appendix 04)

B. PA Title 66 Chapter 5-501

As the Commission is required as per Title 66 Chapter 3 308-2 "to provide consumer information, consumer protection and informal resolution of complaints, the Commission may make such regulations, not inconsistent with law, as may be necessary or proper in the exercise of its powers or for the performance of its duties". Since the Commission represents my only hope for relief, I trust the Commission is guided in its decision making by its mission statement and its powers under PA Title 66 Chapter 5-501 (Appendix 05).

C. Conclusion

As per Section 703 (g), and as stated in the Initial Decision dated September 28, 2012, on page8, the PUC has "....at any time, after notice and after opportunity to be heard as provided in this chapter, rescind or amend any order made by it". I hereby request that the Commission to consider this evidence in its decision-making process with regards to the Initial Decision rendered in my case and prevents PECO in the installation of the smart meter at my residence. Failure to do so will place my family and me at risk to injuries and irreparable harm.

MP Exception No. 3: The Commission needs to assures a Customer Bill of Rights is available to utility customers

A. Introduction

Over the last few years numerous issues and questions have been raised with regards to the implementation of smart metering technology. A customer Bill of Rights needs to be developed in PA during the implementation of the smart metering project and at all times subsequently after its completion. Furthermore, the installation costs are to be supported by the customer in addition to electricity shut off for any customer not complying with the requirements of this forceful installation. In a phone conversation with PECO's customer service representative, I was already

notified about the possibility of account termination should I fail to have such device installed. What and most importantly where are my customer Bill of Rights in this matter?

A. Customer Bill of Rights related to AMI/Smart Metering needs to be implemented

As per the Pennsylvania Constitution (Appendix 06) Section 1- Inherent Rights of Mankind "All men are born equally free and independent, and have certain inherent and indefeasible rights, among which are those of enjoying and defending life and liberty, of acquiring, possessing and protecting property and reputation, and of pursuing their own happiness". Also, as per Section 8- Security from searches and seizures "The people shall be secure in their persons, houses..". The smart meters are constant monitors in contradiction with this Section. Last but not least, in the 1967 Amendment, (Joint Resolution No.1 added present section 26 and renumbered former section 26 to present section 25) Section 27- Natural resources and the public estate "The people have a right to clean air, pure water, and to the preservation of the natural, scenic, historic and esthetic values of the environment. Pennsylvania's public natural resources are the common property of all the people, including generations yet to come. As trustee of these resources, the Commonwealth shall conserve and maintain them for the benefit of all the people" (May 18, 1971, P.L.769, J.R.3). How are we ensuring that the preservation of our natural, scenic, historic and esthetic values of the environment is maintained when we are being bombarded with unseen radiation, radiation that destroys living cells? As per the article publishes in the Chicago Tribune (Appendix 07) on June 21, 2011 by Lisa Madigan, Illinois Attorney General "consumers don't need to be forced to pay billions for so called smart-technology to know how to reduce their utility bills".

C. Conclusion

I herby petition the Commission, for an investigation to evaluate the health, safety, cost, privacy, security regarding the CMPs implementation of smart metering and implement a customer Bill of Rights, to protect the public interest in the implementation of any Advance Metering Infrastructure (AMI) system. Additionally, I hereby petition the Commission to reconsider its prior determination whether this project and its implementation is fair and reasonable to all PECO's customers.

MP Exception No. 4: The Commission needs to review the impact of all Facts and Arguments in support of an investigation of health concerns related to AMI (smart meter) systems deployment and the impact of said technology

A. Introduction

Many questions related to the health and safety of smart meters are raised by various states within the context of various studies and reports. Some of these questions are but not limited to: will we be seeing more deaths attributable to failed peacemakers and defibrillators or more cardiac arrhythmias as a result of this smart grid?; more blindness and sterility cause by damaged eyes and testes?; how about the great risk for those of us that have implanted knees, hearts, hips or pother prostheses?; how would Epileptics of Parkinson's patients with deep-brain stimulators have who's electrodes be shut down by the electromagnetic fields created by the wireless smart grid

cope?; how about our pets that are impacted by the electromagnetic fields of these devices?;what are the electromagnetic exposures attributable to the collectors and repeaters placed on light poles for transmission of the wireless signals generated by the meters, versus the exposures attributable to the meters themselves?; what precautions are taken by the PUC to warn the public of risks of such exposures, and of the locations of this transmission equipment, via a signage or other means, so that the members of the public can better protect themselves against these risks? The House Bill 6358 is acknowledging our right to know the possible RF impact from CP devices, devices that can be turned off or that are not vital to our day to day life (Appendix 08). Should we have such ability to know and refuse Smart Meters in light of this House Bill? Smart Meters cannot be turned off and cannot be refused in PA. These and many other questions remain open and a series of completed or ongoing studies, acts or bill seek further analysis on the RF topic and its harmful health effects.

Furthermore, as per the Sworn Declaration of Dr. David O. Carpenter, M.D., Director, Institute for Health and the Environment, University at Albany and Professor of Environmental Health Sciences within the School of Public Health, formerly Dean of the School of Public Health at the University of Albany and Director of the Wadsworth Center for Laboratories and Research of the New York State Department of Health. United States District Court – District of Oregon - Portland Division - June 2011 (Appendix 09),"Exposure to EMF has been linked to a variety of adverse health outcomes. The health endpoints that have been reported to be associated with ELF and/or RF include childhood leukemia, adult brain tumors, childhood brain tumors, genotoxic effects (DNA damage and micronucleation), neurological effects and neurodegenerative disease (like ALS and Alzheimer's), immune system disregulation, allergic and inflammatory responses, breast cancer in men and women, miscarriage and some cardiovascular effects. The strongest evidence for adverse health effects of EMFs comes from associations observed in human populations with two forms of cancer: childhood leukemia and chronic lymphocytic leukemia in occupationally exposed adults.

Additionally, Dr. David O. Carpenter, M.D., also mentions in the above Sworn Testimony that "There is suggestive to strongly suggestive evidence that RF exposures may cause changes in cell membrane function, cell communication, metabolism, activation of protooncogenes, and can trigger the production of stress proteins at exposure levels below current regulatory limits. Resulting effects can include DNA breaks and chromosome aberrations, cell death including death of brain neurons, increased free radical production, activation of the endogenous opioid system, cell stress and premature aging, changes in brain function including memory loss, retarded learning, performance impairment in children, headaches and fatigue, sleep disorders, neurodegenerative conditions, changes in immune function (allergic and inflammatory responses), reduction in melatonin secretion and cancers" (Appendix 09).

B. <u>Additional research into the health impact of Radio Frequency is being conducted throughout the world</u>

1. World Trade Organization-International Agency for Research on Cancer (Appendix 10)

2. Cell Phone Right to Know H.B 6358 (Appendix 08)

3. American Academy of Environmental Medicine (Appendix 11)

4. Institute of Health and the Environment- University of Albany (Appendix 09)

Conclusion

Since the Commission has the duty in protecting the consumer and provides consumer information, the Commission is called to stand to fulfill this duty. Furthermore, the Commission has to inform the customers of the risks and benefits associated with these meters and protect the customer's rights in the context of these meter installations. If the Commission will fail to do so, would the Commission indemnify its customers, business owners or any other persons, (visitors to the city) for any harm to their health and safety? The Commission must take action in protecting the public's interest since that is within the Commission's duties.

MP Exception No. 5: The Commission shall be able to take advantage of information and other resources from the other states which have already addressed these or similar issues related to AMI/smart meters

A. Introduction

Public Regulatory Commissions in various states have or are actively conducting a series of investigations further looking into a series of issues related to these meters. Such states are but not limited to California, Connecticut, Florida, Main, Maryland, Michigan, Nevada and Texas (Appendix 12).

B. Other states provide customers with opt out programs

Currently, at least 8 states have Opt Out programs. Various other states have imposed or are considering imposing requirements on utilities to inform their customers of their rights, including specifying the existence of certain rights in connection to these metering programs, the procedure whereby customers may invoke these rights, and the terms and conditions, if any, involved in opt-out programs for customers not wishing to have a smart meter installed on their property.

The list is growing by the day as other states join in the investigation of the issues regarding the smart meters. In addition, many states have also investigated recurring complaints of overbilling, billing inaccuracies, meter malfunctions and other customer issues arising from the operation of these wireless devices via the smart meter program. In addition, Vermont has requested its Commissioner of Health and Commissioner of Public Service to issue a join report by January 15, 2013, which shall include the potential of health effects of wireless smart meters (S214 ACT 0140- (Appendix 12- page 4). The PA Commission can be therefore benefited from this wealth of experience in reaching its own conclusion about what is fair and equitable for the customers of any PA utilities.

C. Conclusion

If the Opt Out is not specifically stated in the contexts of Act 129, and if it was the General's Assembly's interpretation that each customer shall receive a meter, why is an Opt Out permissible in other states and not in PA? Pending the approval of Bill 2188, I hereby request that the Commission requires PECO to establish an interim policy that will allow for explicit customer Opt Out process and procedures. As stated earlier in this document,

involvement of the state utility regulatory commission in similar processes has been invoked recently in a number of other states. Furthermore, the Commission, shall be sensitive of the timing related to the promulgation of such ordinance, as some PECO customers may be at risk of having heavy sanctions imposed for not submitting to the installation of a smart meter on their property, without having certification of their rights to refuse to have such meter, and regardless of any customer's wish not to have such a meter, whether based on health, safety, privacy or any other considerations. I seek the Commission's involvement and oversight in any a timely determination of whether or not such policies are in the public's interest and are fair and reasonable for all utility customers.

MP Exception No. 6: The Commission shall be able to place a moratorium on and enforcement related to the proposed forceful installation of smart meters, until the Commission can conclude its investigation of this matter, unless PECO is willingly and voluntarily taking appropriate measures to avoid prejudice to its customers with regards to the cyber security

A. Introduction

The Congressional Research Service published a report on Smart Metering Privacy and Cyber security on February 3, 2012. Excerpts from this report are attached within Appendix 13 however given the page restrictions; I am only able to provide small outlines within the document. Amongst its 48 pages of findings, the document specifies that "The Advance Metering Infrastructure (AMI), promises to increase energy efficiency, bolster electric grid power reliability, and facilitate demand response, among other benefits. However, to fulfill these ends, smart meters must record real-near time data on consumer electricity usage and transmit the data to utilities over great distances via communication networks that serve the smart grid" (Appendix 13- page 2).

The smart gird is a "mesh" system that requires linkage hence communication via Radio Frequency (RF) waves between individual meters and wireless repeaters. Via this system, meters and other sensing devices are used to transmit data in a system that relies usage from point to point until it reaches its final destination at the utility company- PECO. Smart meters are bidirectional devices that will record customer's usage at least hourly or less (page 1 footer of the Initial Decision dated September 28, 2012). These meters can be upgraded remotely by PECO, providing the ability to implement future innovations and adds-on easily. Therefore, a smart meter that is installed by the utility is a communication device that furthers the EDC and goes behind the delivery of electricity to a residence.

B. Cyber Security findings

As the former NSIT (now Federal Energy Regulatory Commission) explains "consumer data moving through a smart grid becomes stored in many locations both within the grid and the physical worlds[55]. Thus because it is widely dispensed, it becomes more vulnerable to interception by unauthorized parties[56] and to accidental breach [57]. The movement of data also increases the potential of it to be stolen by unauthorized third parties while it is in transit, particularly when it travels over a wireless network[58]- or through communication components that might be incompatible with one another or posses outdated security protection[59]". (Appendix 13-page10 CRS Report for

Congress extract and Guidelines for Smart Grid and Cyber Security: Vol 2, Privacy and the Smart Grid published on August 2010).

Last but not least, to further prove the vulnerability of the cyber security of the smart meter, John McNabb, provides a compelling summary related to the vulnerability of the wireless meters network (Appendix 14 entire document contains 37 pages- only few were provided as example).

C. Conclusion

The forceful installation of this device on my personal residence without my ability to opt out, it's remote access capabilities regarding to content of uncertain amount of data related to my occupancy behavior, intimate details of tracking of time patterns and activities within my home therefore constitute an impermissible invasion of privacy in violation of the Fourth Amendment of the United States Constitution in addition to any cyber security treats to my personal data, safety and security. I request that the Commission places a moratorium on any enforcement of the proposed smart meter installation at my residence until the commission has concluded its investigation of the matter, or unless PECO is willingly and voluntarily taking all measures needed to avoid irreparable prejudice to its customer safety and privacy.

MP Exception No. 7: The Commission shall consider customer constitutional privacy rights in relationship to data privacy, data breaches and burglary

A. Introduction

As outlined in the Testimony by Lillie Coney, Associate Director, Electronic Privacy Information Center (EPIC) before the House Committee on Science and Technology Subcommittee on Technology and Innovation on July 1, 2010 (Appendix 15-page 2) "privacy is one of the most fundamental and basic of human rights. Without it, many other rights, such as the freedoms of speech, assembly, religion and the sanctity of the home, would be jeopardized. Although most countries around the world include explicit protection of a right to privacy in their constitutions, it remains one of the more difficult rights to define". Furthermore, (Appendix 15-page 2) "Our legal system has long recognized and protected an individual's right to personal privacy in PII. The drafters of the Constitution "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation "of constitutional principles3. Moreover, public opinion polls consistently find strong support among Americans for legally cognizable privacy rights in law to protect their personal information from government and commercial entities4. More recently, the Supreme Court, in ***Kyllo v. United Statess*** addressed the privacy implications of monitoring electrical use in the home. After reviewing precedent, the Court found that a search warrant must be obtained before the government may use new technology to monitor the use of devices that generate heat in the home." Smart meters are attached to our residences and monitor us without a warrant. How is the Commission going to address this concern?

project, and the Technology and Privacy Advisory Committee of the Department of Defense issued a report recommending that Congress pass laws to protect civil liberties when the government sifts through computer databases containing personal information[29]. The data mining of sensitive personal information transmitted through the Smart Grid raises similar privacy concerns" (Appendix 15- page 6). Furthermore, "Authorized third-parties may also be interested in using data collected through the Smart Grid. The real-time data streaming capabilities of the Smart Grid, in particular, implicate a separate group of privacy risks. Just as appliance manufacturers and insurance companies may want access to appliance usage data, marketing and advertising firms may want access to the data—particularly real-time data—in order to target marketing more precisely[30]. However, power usage data can reveal intimate behavioral information; providing that information to third party marketing and advertising firms surreptitiously would be a repugnant invasion of privacy" (Appendix 15- page 6).

As per the above mentioned testimony, traditionally, utility records have been handled similarly to bank records and telephone records. Several lower federal courts have held that customers do not have a reasonable expectation of privacy in their utility records, thereby permitting warrantless access to these records. In United ***States v. Starkweather***, the Ninth Circuit held that a person does not have a reasonable expectation of privacy in his utility records[134] The panel reasoned that (1) these records were no different from phone records, and thus did not justify a different constitutional result; and (2) the public was aware that such records were regularly maintained, thereby negating any expectation of privacy[135]" (Appendix 13-page 18).

Last but not least, the Commission must consider the identity theft, data breaches, burglary as well as the many privacy issues that could potentially arise from the installation of these devices. Is the Commission prepared to indemnify the public against such issues?

MP Exception No. 8: The Commission shall consider the other findings and ongoing studies related to smart metering technology in the EU-European Consumers' Organization

A. Introduction

In the BEUC draft response on ERGEG public consultation paper on draft guidelines of good practice on regulatory aspects of smart metering, for electricity and gas the European Consumer's Organization states that: "Consumer protection rules must be easily updatable and allow for timely upgrading to protect consumers from any fast moving innovation and technological change which could lead to consumer detriment" (Appendix 16- page 5, section 7)

In the same document, BEUC outlines that "that protections will need to be put in place to protect consumers from misuse of remote disconnection of supply (Appendix 16-page 8, section 6). This is particularly important to protect vulnerable consumers. Similarly clear safeguards will need to be put in place around remote management of appliances within consumers' homes by suppliers. Particular attention will need to be paid to consumer information, safety, and redress and complaint handling if and when things go wrong. BEUC wants to point out that in any case, "the decision whether to participate in remote management or not should be with the

B. Data security, burglary and privacy issues

"Smart meters will increase the frequency of communication from the home to the utility service provider or the third party application user. Traditional meter reading takes place once a month, by a visit from a person affiliated with the electricity service provider or billing company. In contrast, proposals for smart meters discuss "real-time" reporting of usage data[15]. Currently, the design specification is not for electricity consumption information to remain in the home or meter location, which could only be accessed easily by the utility user. Rather, the plan, as suggested in the Cyber Security Strategy, is to instead share the information with the utility company or others. If, as the document suggests, the information will allow customers to make better energy consumption decisions, then only the customer should have access to that information. This is one of many instances in which the design of a Smart Grid application can either favor privacy or ignore it" (Appendix 15- page 4)

Additionally, "Another architectural point which raises privacy implications is the use of wireless communications to transmit Smart Grid data[16]. The Draft Framework proposed to assess "the capabilities and weaknesses of specific wireless technologies"[17]. Although it mentions security as a characteristic of wireless technology that may be relevant to that assessment, privacy is not mentioned. Any wireless technology that would be used to transmit user data must protect personal privacy. Wireless sensors and networks are susceptible to security breaches unless properly secured[18] and breaches of wireless technology could expose users' personal data[19]. Similarly, the potential transmission of Smart Grid data through "broadband over power line" (BPL) implicates users' privacy: A BPL node could communicate with any device plugged into an electrical socket. Capture of a substation node would provide control over messages going to smart appliances or computing systems in homes and offices. A utility may also offer customers BPL as a separate revenue stream. This creates risks that [advanced meter] data could be read or modified over the internet or that common internet attacks could be brought against the electrical grid or individual customers[20]" (Appendix 15- page 4).

Last but not least, "A final architectural problem with the proposed Smart Grid is the interaction between the Smart Grid and plug-in electric vehicles (PEV). It is possible that the Smart Grid would permit utility companies to use PEVs and other sources of stored energy "as a grid-integrated operational asset[22] i.e., to drain the energy stored in the PEVs when the energy is needed to supply other users. This application of the Smart Grid is particularly troubling. If privacy is, as the Supreme Court has said, the "interest in independence in making certain kinds of important decisions[23], then this proposed application could severely damages both privacy interests and consumer rights" (Appendix 15- page 5).

C. Conclusion

The Smart Meter and Smart Gird threatens our privacy in many other ways: misuse of data by PECO, authorized third parties or unauthorized third parties; Power Utilities that are interested in data mining needed to make power distribution decisions; data mining by the government- the Total Information Awareness (TIA), developed by the Defense Advanced Research Projects Agency (DARPA) "proposed to data mine wide swaths of information in order to detect terrorists[28]. However, privacy concerns led the Congress to eliminate funding for the

consumers since they always have to have the possibility of opt out" (Appendix 16-page 8, section 6). If the above points have been pointed by the European Consumer's Organization, how are we the citizens of the U.S and PA respectively any different as consumers?

Furthermore, how can we, the public and customers in PA be heard when the Consumer Advocate Sonny Popovsky, testified on May 8, 212 before the PA House Consumer Affairs Committee regarding smart meter Bill 2188 and stated "once a utility commits to the deployment of an advance metering technology in a geographical area or throughout its service territory, then it is far more economical to serve all customers in that area throughout this technology, rather than serving all but one or few such customers. The most obvious example of that result is meter reading. If a company can read the metering of 100 neighboring customers instantaneously through an electronic signal, but then has to send out an employee to read the meter of one customer in that neighborhood, then the cost to the utility in reading that one meter would be substantial. The question then is who should pay those additional cost, the one customer who opted out of receiving the smart meter or the remaining customers who have permitted the installation of the meters in their homes? The issue has come up in a number of other states and, to my knowledge, each of the states that has allowed customers to opt out of receiving a new meter, has required the individual opt out customers to pay substantial up-front and monthly fees- over and above their normal monthly bills- to cover at least a portion of those additional costs. The alternative, as I said is to charge those costs to the customers. This would be particularly true in Pennsylvania, where it is clear under Act 129 that utilities have a right to recover their incremental smart meter cost from ratepayers" (Appendinx 17- page 4 and 5).

B. European Consumer's Organization findings

The European Consumer's Organization states that "all consumers who wish to use smart meters should have "equal access" to the benefits" (Appendix 16- page 10, section 15). How about for the consumers that do not wish to have access to such benefits? Why the customers in PA specifically do not have the right as other customers in other states or the EU do?

In the testimony of Chairman Robert F. Powelson, PA PUC hearing by the Pennsylvania House Consumer Affairs Committee Regarding House Bill 2186 and House Bill 2188 on May 8,2012, we the customers are told by the Chairman of the PUC "Regardless of the validity of opponents' concerns about health, safety and privacy, some utilities in other states have begun considering and implementing AMI opt-but programs in an effort to diffuse opposition and allow utility companies to move forward with arid modernization plans. Regardless of where their stand in the transition to AMI technology, the industry generally prefers a uniform system of managing customer data, and fears a return to the days of manual meter-readings, which would be needed for those customers who opt out of wireless meters".(Appendix 18- page 5). The use of the word regardless in the context of the above citation is rather disturbing given the Chairman should be concerned as per the PA PUCs mission with the "consumer protection and informal resolution of complaints". Chairman Robert F Powelson, believes that "simply put, there is no compelling reason for an "opt-out program" in PA (Appendix 18- page 7).Customer rights should be one of the compelling reasons for Chairman Powelson.

C. Conclusion

In light of the above findings, Commission must ensure the Customer's rights are indeed a compelling reason. To further my point, I site from the Consumer Advocate Sonny Popovsky testimony on May 8, 212 before the PA House Consumer Affairs Committee regarding smart meter Bill 2188 "As the introduction of the legislation that is the subject of this hearing exemplifies, the implementation of the smart meter mandates of Act 129 has not been without controversy. My Office has received a number of questions and complaints from consumers regarding the smart meter surcharges that have begun to appear on customers' bills and the need for and cost of these new meters. I spoke with one PECO customer just recently who informed me in no uncertain terms that she did not ask for a new meter; that she did not need a new meter; and that she certainly did not want to pay for a new meter in her home. Indeed, in several states that have begun to implement this new technology across the Nation, there have been objections raised by a growing number of consumers regarding not just the cost of the new meters, but also their impacts on the privacy of customer information as well as health concerns arising from their operation". (Appendix 17- page 2 and 3).This indeed serves as proof that that these concerns from the general public are pouring in and that that the public is alerting the appropriate agencies of the inappropriateness of this forceful installation. I am therefore, providing my written complain to the PUC joining the many other customers that are bringing forward this issue and I again urge the Commission to reconsider its Initial Decision related to the forceful installation of a smart meter at my residence.

MP Exception No. 9: Fires and property damage/safety

A. Introduction

PECO began installation of smart meters in my neighborhood on around June 2012. The initial smart meter technology was provided via Sensus, a North Carolina company specializing in the utility metering technology.

After numerous incidents in PA, many of which in Bucks County were I reside, PECO ditches Sensus and re embarks in the installation of the smart metering technology using another utility metering manufacturer, Landis+Gyr (L+G). PECO now replaces the over 96,000 meters previously installed, meters produced by Sensus with new meters produced by the new supplier Landis+Gyr (L+G). Interesting to mention is that the previous manufacturer Sensus, signed other contracts to provide smart metering technology to other electricity company (Southern Company-contract signed December 2007 as an example). PECO was one of the many others that sign an agreement for the smart metering technology. What PECO failed to disclose to us, the customers, is the Case No. CV-10-CO-1377-S filed on May 25, 2010 in the District of Columbia N.D. of Alabama, Southern Division (Appendix 19- page 2).

In this public case, Dan Baker, Plaintiff, alleges under the False Claim Act that the above mentioned utility metering supplier, Sensus, submitted, caused to be submitted and conspired to submit to the United States false claims for payment or funds under the American Reinvestment and Recovery Act of 2009. Mr. Baker had direct and personal knowledge of Sensus and specifically about the serious defects and pose a substantial fire hazard. Since the

fire hazard is explicitly outlined in the above mentioned case and since PECO did not seek qualified providers of such devices concomitantly ensuring such devices are safe, PECOs ability to select qualified provides cannot be trusted. I am not willing to put myself or my family at risk to find out if the secondly selected supplier Landis+Gyr (L+G) has indeed a better technology that do not pose the same risk and hazards as the first supplier (Appendix 20). http://www.environmentalleader.com/2012/10/10/peco-ditches-sensus-smart-meters-resumes-installation-in-pa/

B. Fire hazard

In the BEUC draft response on ERGEG public consultation paper on draft guidelines of good practice on regulatory aspects of smart metering, for electricity and gas the European Consumer's Organization states that "consumers should be informed about fire hazards linked to the use of appliances overnight, such as to be able to take appropriate measures; the delivery of extra help to certain vulnerable customers" (Appendix 16- page 4, section 2). Fires are obviously a hazard in Europe, U.S, Canada, Australia and wherever these meters are install. This is an issue that needs to be address as the Commission should be concerned with the safety and security of the customers. Furthermore, in Bucks Country PA where I currently reside, we had a series of fires caused by the smart meters, fires that prompted the Commission to required PECO to stop installation of smart meters until all investigations related to these incidents were resolved. Various indisputable evident exists within many internet publications and new stations related to these Bucks County PA fires. One example is attached as (Appendix 21). http://abclocal.go.com/wpvi/story?section=news/local&id=8776596

These example serve as testimony that with the new technology, lots of unknowns are hidden to the customers and not only. How is the Commission prepared to compensate the public given fires were caused by the meters that PECO install such dangerous devices under the Commission's authority? I am also providing supporting documentation that outlines in detail, the many incidents, fires, explosions or burnout appliances due to smart meters. The below provides a compilation of cases across not only the U.S but also other countries where this technology is available- Canada, UK, Australia (Appendix 22-only 3 pages out of the 34 pages are provided as samples) http://emfsafetynetwork.org/?page_id=1280

C. Conclusion

Since the Commission is already familiar via the August 17, 2012 letter where it requested 17 questions to be address by PECO related to the fires, PECO Energy's handling of its smart meter program, including failure rates of its meters, the number of overheating incidents and how many overheating incidents resulted in damage, I will not further expand on this point. PECO acknowledged publicly by suspending the installation of meters on August 15, 2012 after some Bucks County fire marshals raised concerns about newly installed smart electric meters overheating and causing house fires. I happen to live in Buck County and I could have been one of the impacted residents. How is the Commission addressing my safety concerns related to fire hazard caused by these devices by dismissing my claim? Clearly, these incidents are real and although in most of the cases PECO, pushed the issue onto consumer's lap under pretenses of loose electrical wires, outdated appliances, or simply discounting the smart meter's involvement in the fires, the Case No. CV-10-CO-1377-S (Attachment 19- page 3 and 4) further proves as a

testimony that indeed the meters were defective and through forceful installation the customers were placed at risk by PECO and the Commission. Failure to be an educated consumer unfortunately resulted in property damage for these unlucky PECO customers. I can only be thankful I was not one of them. I am not going to become a victim and I will not allow this experimental technology to endanger my life, safety and well being. I will certainly not allow my family to be placed at risk simply because a law is incomplete or because an official forgot to explicitly give the customer the sole right of opt out. Clearly the Commission has another opportunity through my case to make the appropriate corrections and take control over the situation by giving the customers the right to opt out. Is the Commission willing to compensate the public it serves in the context of these unnecessary installs? I hereby request the Commission to further consider this evidence and reconsider its Initial Decision related to the smart meter installation at my residence. Failure to do so would pose a risk onto my safety, well being and security, risk the Commission should therefore assume should my case be dismissed once again.
http://www.phillyburbs.com/news/local/courier_times_news/puc-wants-answers-from-peco-about-smart-meters-overheating/article_9c460673-2206-5dda-9baf-ea12c239741d.html

III. CONCLUSSION

In conclusion, I plead with the Commission, via the Exceptions above, requesting that PECO stops the installation of the smart meter at my residence hence eliminating the risks and suffering that my family would suffer with potential irreparable injuries. Citizens from other states have been able to take similar concerns related to smart meters to their state regulators and in such cases, said citizens have won relief. Also, customers that chose to hold on to their existing meter are able to do so by paying a small upfront fee, fee that I am willing to pay.

I also petition the Commission, to review our Constitutional rights in regards to the forceful implementation of this Act 129 in light of the numerous cases that were presented in Federal court, cases that outline this point to a great extent (Appendix 23-Naperville Smart Meter Awareness v. City of Naperville; Appendix 24-Ed Friedman et Al v. Maine Public Utilities Commission and Central Maine Power Company).

I have done my best to provide as much of a complete report as possible under the very short timelines. The Initial Response, although was signed on September 28, 2014 was not received in my hands until October 9, 2012 given the letter prepared by the Commission's secretary was not finalized until October 4, 2012. The 20 day limit for *response is rather a very short time to respond for the customer in light of the above. Since I am not an attorney but* rather a simple citizen, I am not familiar with the Commission's time extension rules and regulations so I trust this document reaches you within the specified time frame respectively October 24, 2012.

Last but not least, as per the § 5.533 of the procedure to except to initial, tentative and recommended decisions, "The exceptions must be concise. The exceptions and supporting reasons must be limited to 40 pages in length. Statements of reasons supporting exceptions must, insofar as practicable, incorporate by reference and citation, relevant portions of the record and passages in previously filed briefs. A separate brief in support of or in reply to exceptions may not be filed with the Secretary under § 1.4 (relating to filing generally)". The 40 page

requirement is rather limiting given the overwhelming amount of information available to the general public so I have tried to be concise under the circumstances and provide the most compelling exceptions towards my case.

I want to thank you for taking the time to read through the above findings and for giving the appropriate consideration to this case.

Maria Povacz
US citizen, PA resident and PECO customer

Date: October 22, 2012

CERTIFICATE OF SERVICE

Re: Maria Povacz
v.
PECO
Docket No. C-2012-2317176

I hereby certify that I have this day served a true copy of the foregoing document Exceptions of the Pennsylvania Public Utility Commission upon parties of record in this proceeding in accordance with the requirements of 52 Pa. Code § 1.54 (relating to Service by a Participant), in the manner and upon the persons listed below:

Dated this 22nd day of October, 2012

SERVICE BY OVERNIGHT/HAND DELIVERY

Secretary ✓
PA Public Utility Commission
400 North Street
Commonwealth Keystone Building, 2nd Floor
Harrisburg, PA 17120

SERVICE BY EFILING

Commission's Office of Special Assistants (OSA)
Ra-OSA@pa.gov

SERVICE BY FIRST CLASS MAIL

Bernard T O'Neil, State Representative District 29
755 York Road, Suite 105
Warminster, PA 18974

Michael Fitzpatrick
US Congressman
1717 Langhorne Newtown Rd, Suite 400
Langhorne, PA 19047

Mike Reese, State Representative
163A East Wing
PO Box 202059
Harrisburg, PA 17120-2059

David Hecker
District Attorney, Office of the District Attorney
Bucks County Courthouse
55 East Court Street
Doylestown PA 18901

Appendix 01

PENNSYLVANIA
PUBLIC UTILITY COMMISSION
Harrisburg, PA. 17105-3265

Public Meeting held June 30, 2011

Commissioners Present:

Robert F. Powelson, Chairman
John F. Coleman, Jr., Vice Chairman
Tyrone J. Christy
Wayne E. Gardner
James H. Cawley

Smart Meter Procurement and Installation — Dockets No. M-2009-2092655

TENTATIVE ORDER

RECEIVED
OCT 22 2012
PA PUBLIC UTILITY COMMISSION
SECRETARY'S BUREAU

BY THE COMMISSION:

The Pennsylvania General Assembly (General Assembly) has directed that electric distribution companies (EDCs) with more than 100,000 customers file smart meter technology procurement and installation plans with the Commission for approval. 66 Pa. C.S. § 2807(f). Act 129 of 2008 (Act 129) requires these EDCs to make available to third parties, including electric generation suppliers (EGSs) and providers of conservation and load management services, with customer consent, direct access to the meter and electronic meter data. 66 Pa. C.S. § 2807(f)(3).

On June 18, 2009, this Commission adopted a *Smart Meter Procurement and Installation Implementation Order*[1] (*Implementation Order*) to establish the standards each plan must meet and to provide guidance on the procedures to be followed

[1] This Order was entered on June 24, 2009, at Docket No. M-2009-2092655.

for submittal, review and approval of all aspects of each smart meter plan. This *Implementation Order* required covered EDCs to work through the Electronic Data Exchange Working Group (EDEWG) to develop electronic data interchange (EDI) transaction standards to fully achieve the capabilities of smart meter technology.[2]

On December 7, 2009, EDEWG submitted a Preliminary Proposal for the Development of Smart Meter Data Exchange Standards (Preliminary Proposal). We have reviewed the Preliminary Proposal and through this Tentative Order propose further direction and clarification about the role of EDEWG and covered EDCs in the development of statewide smart meter data exchange standards and formats.

BACKGROUND

The EDCs obligated to deploy smart meter technology under Act 129 include the Duquesne Light Company (Duquesne); Metropolitan Edison Company, Pennsylvania Electric Company, Pennsylvania Power Company, West Penn Power Company (collectively FirstEnergy); PECO Energy Company (PECO); and PPL Electric Utilities Corporation (PPL). All of these EDCs have filed a Smart Meter Technology Procurement and Installation Plan (Smart Meter Plan) with the Commission for approval. All of these EDCs, with the exception of West Penn Power Company, have received Commission approval of their respective Smart Metering Plans.

The *Implementation Order* required covered EDCs to address, among other things, standards and formats for electronic data communications with customers and customer authorized third parties. Specifically, the Commission noted that these EDCs were required to implement an EDI transaction related to customers enrolled in a real time price or time-of-use rate program, as well as a new historical interval usage transaction, in order to provide customers and their designated agents with 12 months of

[2] *See Implementation Order* at 24-28.

where the EGS calculates its own charges and bills the customer directly, or provides a Bill-Ready EDI 810 transaction to the EDC.[9]

The Commission agrees that these current practices of providing Dual Billing and Bill Ready Consolidated Billing should be approved for the enrollment and billing of EGS customers who purchase service under a real-time and time-of-use pricing option for all EDCs. As such, we propose that covered EDCs be required to submit the appropriate EDI change control requests for the appropriate EDI transactions to EDEWG within 30 days of the entry of a Final Order in this proceeding, and effect implementation of these changes on an immediate, high priority basis.

2. Historical Interval Usage

The Preliminary Proposal stated that the existing 867 Historical Interval Usage (HIU) transaction meets the requirement of the *Implementation Order*, to provide customers and their agents with 12 months of interval usage data at the meter level. The Preliminary Proposal, however, noted that this transaction is currently optional except in the case of PPL, which limits the provision of this data at the account level. Due to the estimated, high volume of 15-minute meter reads over a 12-month period, the Preliminary Proposal recommended that EDEWG explore the use of alternative methods for the provision of HIU data at the meter level.[10]

The Commission agrees that the use of the 867 HIU transaction may not be the most economically efficient method for providing historical interval usage data at the meter level. We, therefore, propose that EDEWG explore its options with covered EDCs and to identify an alternate solution that can be implemented by the EDCs within 180 days of the entry of a Final Order in this proceeding.

---

[9] Preliminary Proposal at 3-6.
[10] Preliminary Proposal at 5.

developed and implemented.[17] With this Tentative Order, we clarify our expectations of the EDEWG team that is working on smart meter interaction with customers and their representatives, as follows:

- Required Functionality

  EDEWG is to review each EDC's current smart meter plan for provision of the following required functionality:
  a) To provide customers with direct access to hourly usage and price information;
  b) To provide support for automatic control of a customer's electricity consumption by the customer, the utility or a customer's agent (at the discretion of the customer); and
  c) To provide direct meter access and electronic access to customer meter data by third parties with customer consent.

- Standardization Efforts

  EDEWG is to perform the following:
  a) Provide detailed descriptions of any proposed statewide standardized transactions or protocols, if any, for each of the EDCs for providing the required functionality;
  b) Provide estimated system and operational costs, both total and annual, for each utility to provide the required functionality;
  c) Review the ability for a statewide solution to provide the required functionality; and
  d) Review costs for a statewide solution to provide the required functionality for all utilities.

We propose that EDEWG submit to the Commission a report outlining its findings and conclusions within 90 days of the entry of a Final Order in this proceeding.

Finally, we propose that EDEWG incorporate this functionality into its current operational documents, i.e. Implementation Guidelines, Testing and Certification

[17] *Id.*

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Appendix 2

PUBLIC LAW 109–58—AUG. 8, 2005

ENERGY POLICY ACT OF 2005

(b) COMPLIANCE.—

(1) TIME LIMITATIONS.—Section 112(b) of the Public Utility Regulatory Policies Act of 1978 (16 U.S.C. 2622(b)) is amended by adding at the end the following: Deadlines.

"(3)(A) Not later than 2 years after the enactment of this paragraph, each State regulatory authority (with respect to each electric utility for which it has ratemaking authority) and each nonregulated electric utility shall commence the consideration referred to in section 111, or set a hearing date for such consideration, with respect to each standard established by paragraphs (11) through (13) of section 111(d).

"(B) Not later than 3 years after the date of the enactment of this paragraph, each State regulatory authority (with respect to each electric utility for which it has ratemaking authority), and each nonregulated electric utility, shall complete the consideration, and shall make the determination, referred to in section 111 with respect to each standard established by paragraphs (11) through (13) of section 111(d).".

(2) FAILURE TO COMPLY.—Section 112(c) of the Public Utility Regulatory Policies Act of 1978 (16 U.S.C. 2622(c)) is amended by adding at the end the following: "In the case of each standard established by paragraphs (11) through (13) of section 111(d), the reference contained in this subsection to the date of enactment of this Act shall be deemed to be a reference to the date of enactment of such paragraphs (11) through (13).".

(3) PRIOR STATE ACTIONS.—

(A) IN GENERAL.—Section 112 of the Public Utility Regulatory Policies Act of 1978 (16 U.S.C. 2622) is amended by adding at the end the following:

"(d) PRIOR STATE ACTIONS.—Subsections (b) and (c) of this section shall not apply to the standards established by paragraphs (11) through (13) of section 111(d) in the case of any electric utility in a State if, before the enactment of this subsection—

"(1) the State has implemented for such utility the standard concerned (or a comparable standard);

"(2) the State regulatory authority for such State or relevant nonregulated electric utility has conducted a proceeding to consider implementation of the standard concerned (or a comparable standard) for such utility; or

"(3) the State legislature has voted on the implementation of such standard (or a comparable standard) for such utility.".

(B) CROSS REFERENCE.—Section 124 of such Act (16 U.S.C. 2634) is amended by adding the following at the end thereof: "In the case of each standard established by paragraphs (11) through (13) of section 111(d), the reference contained in this subsection to the date of enactment of this Act shall be deemed to be a reference to the date of enactment of such paragraphs (11) through (13).".

SEC. 1252. SMART METERING.

(a) IN GENERAL.—Section 111(d) of the Public Utility Regulatory Policies Act of 1978 (16 U.S.C. 2621(d)) is amended by adding at the end the following:

"(14) TIME-BASED METERING AND COMMUNICATIONS.—(A) Not later than 18 months after the date of enactment of this paragraph, each electric utility shall offer each of its customer Deadline.

classes, and provide individual customers upon customer request, a time-based rate schedule under which the rate charged by the electric utility varies during different time periods and reflects the variance, if any, in the utility's costs *of generating and purchasing electricity at the wholesale level.* The time-based rate schedule shall enable the electric consumer to manage energy use and cost through advanced metering and communications technology.

"(B) The types of time-based rate schedules that may be offered under the schedule referred to in subparagraph (A) include, among others—

"(i) time-of-use pricing whereby electricity prices are set for a specific time period on an advance or forward basis, typically not changing more often than twice a year, based on the utility's cost of generating and/or purchasing such electricity at the wholesale level for the benefit of the consumer. Prices paid for energy consumed during these periods shall be pre-established and known to consumers in advance of such consumption, allowing them to vary their demand and usage in response to such prices and manage their energy costs by shifting usage to a lower cost period or reducing their consumption overall;

"(ii) critical peak pricing whereby time-of-use prices are in effect except for certain peak days, when prices may reflect the costs of generating and/or purchasing electricity at the wholesale level and when consumers may receive additional discounts for reducing peak period energy consumption;

"(iii) real-time pricing whereby electricity prices are *set for a specific time period on an advanced or forward* basis, reflecting the utility's cost of generating and/or purchasing electricity at the wholesale level, and may change as often as hourly; and

"(iv) credits for consumers with large loads who enter into pre-established peak load reduction agreements that reduce a utility's planned capacity obligations.

"(C) Each electric utility subject to subparagraph (A) shall provide each customer requesting a time-based rate with a time-based meter capable of enabling the utility and customer to offer and receive such rate, respectively.

"(D) For purposes of implementing this paragraph, any reference contained in this section to the date of enactment of the Public Utility Regulatory Policies Act of 1978 shall be deemed to be a reference to the date of enactment of this paragraph.

"(E) In a State that permits third-party marketers to sell electric energy to retail electric consumers, such consumers shall be entitled to receive the same time-based metering and communications device and service as a retail electric consumer of the electric utility.

Deadline.

"(F) Notwithstanding subsections (b) and (c) of section 112, each State regulatory authority shall, not later than 18 months after the date of enactment of this paragraph conduct an investigation in accordance with section 115(i) and issue a decision *whether it is appropriate to implement the standards set out* in subparagraphs (A) and (C).".

Appendix 3

Regular Session 2011-2012
House Bill 2188

Text

Short Title: An Act amending Title 66 (Public Utilities) of the Pennsylvania Consolidated Statutes, further providing for duties of electric distribution companies.

Prime Sponsor: Representative REESE

Last Action: Referred to CONSUMER AFFAIRS, Feb. 8, 2012 [House]

Printer's No.

Printer's No.	Text	(H) Amendments	(S) Amendments	(H) Fiscal Note	(S) Fiscal Note
3071					
3067					

denotes current Printer's Number

Appendix 4

PENNSYLVANIA PUC PUBLIC UTILITY COMMISSION

PENNSYLVANIA

About the PUC

The PUC funds an authorized complement of 519 employees, including attorneys, rate and service analysts, auditors, economists, engineers, motor transit and railroad specialists, communications specialists, safety inspectors and enforcement investigators. They work, together with administrative, fiscal, computer and clerical personnel in 12 offices and bureaus that report to an Executive Director.

The PUC is funded by assessment of the regulated public utilities. Subject to budget approval, the PUC may assess utilities up to three-tenths of one percent of gross intrastate revenue to cover the cost of regulation. All assessments are paid into the General Fund of the State Treasury through the Department of Revenue for use solely by the Commission. The budget for Fiscal Year 2012-13 is $60,398,000 in state funds and $4,857,000 in federal funds, for a total of $65,255,000.

The Public Utility Commission was created by the Pennsylvania Legislative Act of March 31, 1937 (and the Public Utility Law of May 28, 1937), which abolished the Public Service Commission.

The PUC has 12 offices and bureaus reporting to an Executive Director, with its headquarters in Harrisburg. Regional offices are located in Altoona, Philadelphia, Pittsburgh and Scranton. The regional offices serve as administrative coordinating points for enforcement officers and administrative law judges. The Philadelphia office also has employees from the PUC's Bureau of Consumer Services.

Learn more about the Bureaus and Offices of PUC here.

Mission Statement: The Pennsylvania Public Utility Commission balances the needs of consumers and utilities to ensure safe and reliable utility service at reasonable rates; protect the public interest; educate consumers to make independent and informed utility choices; further economic development; and foster new technologies and competitive markets in an environmentally sound manner.

Appendix 5

Enactment. Chapter 5 was added July 1, 1978, P.L.598, No.116, effective in 60 days.

§ 501. General powers.

(a) Enforcement of provisions of part.--In addition t powers expressly enumerated in this part, the commission have full power and authority, and it shall be its duty t enforce, execute and carry out, by its regulations, order otherwise, all and singular, the provisions of this part, the full intent thereof; and shall have the power to resc modify any such regulations or orders. The express enumer of the powers of the commission in this part shall not ex any power which the commission would otherwise have under the provisions of this part.

(b) Administrative authority and regulations.--The commission shall have general administrative power and au to supervise and regulate all public utilities doing busi within this Commonwealth. The commission may make such regulations, not inconsistent with law, as may be necessa proper in the exercise of its powers or for the performan

Appendix 6

12. Power of suspending laws.
13. Bail, fines and punishments.
14. Prisoners to be bailable; habeas corpus.
15. Special criminal tribunals.
16. Insolvent debtors.
17. Ex post facto laws; impairment of contracts.
18. Attainder.
19. Attainder limited.
20. Right of petition.
21. Right to bear arms.
22. Standing army; military subordinate to civil power.
23. Quartering of troops.
24. Titles and offices.
25. Reservation of powers in people.
26. No discrimination by Commonwealth and its political subdivisions.
27. Natural resources and the public estate.
28. Prohibition against denial or abridgment of equality of rights because of sex.

Adoption. Unless otherwise noted, the provisions of Article I were adopted December 16, 1873, 1874 P.L.3, effective January 1, 1874.

That the general, great and essential principles of liberty and free government may be recognized and unalterably established, WE DECLARE THAT--

§ 1. Inherent rights of mankind.

All men are born equally free and independent, and have certain inherent and indefeasible rights, among which are those of enjoying and defending life and liberty, of acquiring, possessing and protecting property and reputation, and of pursuing their own happiness.

§ 2. Political powers.

All power is inherent in the people, and all free governments are founded on their authority and instituted for their peace, safety and happiness. For the advancement of these ends they have at all times an inalienable and indefeasible right to alter, reform or abolish their government in such manner as they may think proper.

§ 3. Religious freedom.

All men have a natural and indefeasible right to worship Almighty God according to the dictates of their own consciences; no man can of right be compelled to attend, erect or support any place of worship, or to maintain any ministry against his consent; no human authority can, in any case whatever, control or interfere with the rights of conscience, and no preference shall ever be given by law to any religious establishments or modes of worship.

§ 4. Religion.

No person who acknowledges the being of a God and a future state of rewards and punishments shall, on account of his religious sentiments, be disqualified to hold any office or place of trust or profit under this Commonwealth.

§ 5. Elections.

Elections shall be free and equal; and no power, civil or military, shall at any time interfere to prevent the free exercise of the right of suffrage.

§ 6. Trial by jury.

Trial by jury shall be as heretofore, and the right thereof remain inviolate. The General Assembly may provide, however, by law, that a verdict may be rendered by not less than five-sixths of the jury in any civil case. Furthermore, in criminal cases the Commonwealth shall have the same right to trial by jury as does the accused.

(May 18, 1971, P.L.765, J.R.1; Nov. 3, 1998, P.L.1328, J.R.2)

§ 7. Freedom of press and speech; libels.

The printing press shall be free to every person who may undertake to examine the proceedings of the Legislature or any branch of government, and no law shall ever be made to restrain the right thereof. The free communication of thoughts and opinions is one of the invaluable rights of man, and every citizen may freely speak, write and print on any subject, being responsible for the abuse of that liberty. No conviction shall be had in any prosecution for the publication of papers relating to the official conduct of officers or men in public capacity, or to any other matter proper for public investigation or information, where the fact that such publication was not maliciously or negligently made shall be established to the satisfaction of the jury; and in all indictments for libels the jury shall have the right to determine the law and the facts, under the direction of the court, as in other cases.

Constitutionality. The provisions of section 7 relating to criminal libel were declared unconstitutional by the Supreme Court of Pennsylvania in *Commonwealth v. Armao*, 446 Pa. 325, 286 A.2d 626 (1972).

§ 8. Security from searches and seizures.

The people shall be secure in their persons, houses, papers and possessions from unreasonable searches and seizures, and no warrant to search any place or to seize any person or things shall issue without describing them as nearly as may be, nor without probable cause, supported by oath or affirmation subscribed to by the affiant.

§ 9. Rights of accused in criminal prosecutions.

In all criminal prosecutions the accused hath a right to be heard by himself and his counsel, to demand the nature and cause of the accusation against him, to be confronted with the witnesses against him, to have compulsory process for obtaining witnesses in his favor, and, in prosecutions by indictment or information, a speedy public trial by an impartial jury of the vicinage; he cannot be compelled to give evidence against himself, nor can he be deprived of his life, liberty or property, unless by the judgment of his peers or the law of the land. The use of a suppressed voluntary admission or voluntary confession to impeach the credibility of a person may be permitted and shall not be construed as compelling a person to give evidence against himself.

(Nov. 6, 1984, P.L.1306, J.R.2; Nov. 7, 1995, 1st Sp.Sess., P.L.1151, J.R.1; Nov. 4, 2003, P.L. , J.R.1)

§ 10. Initiation of criminal proceedings; twice in jeopardy; eminent domain.

No attainder shall work corruption of blood, nor, except during the life of the offender, forfeiture of estate to the Commonwealth.

(May 16, 1967, P.L.1035, J.R.1)

§ 20. Right of petition.

The citizens have a right in a peaceable manner to assemble together for their common good, and to apply to those invested with the powers of government for redress of grievances or other proper purposes, by petition, address or remonstrance.

§ 21. Right to bear arms.

The right of the citizens to bear arms in defense of themselves and the State shall not be questioned.

§ 22. Standing army; military subordinate to civil power.

No standing army shall, in time of peace, be kept up without the consent of the Legislature, and the military shall in all cases and at all times be in strict subordination to the civil power.

§ 23. Quartering of troops.

No soldier shall in time of peace be quartered in any house without the consent of the owner, nor in time of war but in a manner to be prescribed by law.

§ 24. Titles and offices.

The Legislature shall not grant any title of nobility or hereditary distinction, nor create any office the appointment to which shall be for a longer term than during good behavior.

§ 25. Reservation of powers in people.

To guard against transgressions of the high powers which we have delegated, we declare that everything in this article is excepted out of the general powers of government and shall forever remain inviolate.

(May 16, 1967, P.L.1035, J.R.1)

1967 Amendment. Joint Resolution No.1 repealed former section 25 and renumbered former section 26 to present section 25.

§ 26. No discrimination by Commonwealth and its political subdivisions.

Neither the Commonwealth nor any political subdivision thereof shall deny to any person the enjoyment of any civil right, nor discriminate against any person in the exercise of any civil right.

(May 16, 1967, P.L.1035, J.R.1)

1967 Amendment. Joint Resolution No.1 added present section 26 and renumbered former section 26 to present section 25.

§ 27. Natural resources and the public estate.

The people have a right to clean air, pure water, and to the preservation of the natural, scenic, historic and esthetic values of the environment. Pennsylvania's public natural resources are the common property of all the people, including generations yet to come. As trustee of these resources, the Commonwealth shall conserve and maintain them for the benefit of all the people.

(May 18, 1971, P.L.769, J.R.3)

1971 Amendment. Joint Resolution No.3 added section 27.

§ 28. Prohibition against denial or abridgment of equality of rights because of sex.

Appendix 7

Chicago Tribune

Breaking News, Since 1847

An experiment too expensive for consumers

June 21, 2011 | By Lisa Madigan

Last month, as the Illinois General Assembly's spring session rushed to a close, ComEd, Ameren and their army of lobbyists were able to muscle a bill through the legislature that will mean a decade of higher prices for consumers if it becomes law. That must not happen.

The bill mandates up to $3.76 billion in spending on dubious plans to upgrade the electric grid and replace customers' electric meters with so-called smart meters. While ComEd and Ameren will do the spending, we'll be footing the bill thanks to large annual rate increases — about 9 percent a year. The utilities want to experiment with expensive and unproven smart grid technology, yet all the risk for this experiment will lie with consumers. The utilities cleverly crafted a law that poses no risk for them and guarantees them huge profits.

ComEd and Ameren have failed to prove there's an urgent need for this excessive spending. In fact, even utility executives admit doubts about the benefits of these investments and question whether they are worth the cost. John Rowe, the CEO of ComEd's parent company, Exelon, recently said of the smart grid:

"... it costs too much, and we're not sure what good it will do. We have looked at most of the elements of smart grid for 20 years and we have never been able to come up with estimates that make it pay."

Wow! Really? Then why are ComEd and Ameren pushing so hard to have us pay for this technology?

I believe this legislation is nothing more than a thinly veiled attempt by ComEd and Ameren to protect their revenues for the next decade at great expense to consumers. It would guarantee these monopolies a yearly profit of 10 percent or more.

So far, most legislators have bought the utilities' smart sell and slick ad campaign.

Their pitch is that smart meters will allow consumers to monitor their electricity usage, helping them to reduce consumption and save money. But the $63 million smart grid pilot program consumers are currently paying for has turned in disappointing results that reinforce what Rowe already knows. On hot summer days, people continue to run their air conditioners no matter how much information they have from their smart meter.

Consumers don't need to be forced to pay billions for so-called smart technology to know how to reduce their utility bills. We know to turn down the heat or air conditioning and shut off the lights. The utilities have shown no evidence of billions of dollars in benefits to consumers from these new meters, but they have shown they know how to profit.

I think the only real question is: How dumb do they think we are?

Lisa Madigan is the Illinois attorney general.

Appendix 8

Is your congressional district changing? Find out on (broug

H.R. 6358: Cell Phone Right to Know Act

112th Congress, 2011–2012

To examine, label, and communicate adverse human biological effects associated with exposure to electromagnetic fields from cell phones and other wireless devices, and for other purposes.

Sponsor:

Status: Referred to Committee

Bill titles and the summary above are written by the sponsor.

H.R. stands for House bill.

BILL OVERVIEW

STATUS	Introduced	Aug 03, 2012	RELATED BILLS	Search for
	Referred to Committee	Aug 03, 2012		
	Reported by Committee	(not yet occurred)	SUBJECT AREAS	Use these subject area explore related legisla
	Passed House	(not yet occurred)		

Appendix 9

UNIVERSITY AT ALBANY
State University of New York

Institute for Health and the Environment
and
Department of Environmental Health Sciences
School of Public Health

28 March 2012

Mayor George Pradel
City Manager, Doug Krieger
West Monroe Partners, Fred Pammer & Tom Hulsebosch
Members, Naperville City Council
400 S. Eagle Street
Naperville, Illinois 60540

Re: Smart Meters

Dear Sirs/Madams:

This is concerning potential adverse health effects associated with exposure to radiofrequency (RF) radiation, specifically that from smart meters. I am a public health physician and former Dean of the School of Public Health at the University at Albany. I have been involved in review and analysis of studies on electromagnetic fields, including radiofrequency fields, for many years. I served as the Executive Secretary to the New York State Powerlines Project in the 1980s, and have published several reviews on the subject. In addition I was invited to present to the recent President's Cancer Panel on the subject of powerline and radiofrequency fields and cancer, and the publication that came from that Panel is attached. I have edited two books on effects of EMFs, including RF radiation. I served as the co-editor of the Bioinitiative Report ( ), a comprehensive review of the literature on this subject. The public health chapter from this report was subsequently published in a peer reviewed journal, which is attached. This is a subject which I know well, and one on which I take a public health approach that has as a fundamental principle the need to protect against risk of disease even when one does not have all the information that would be desirable.

There is clear and strong evidence that intensive use of cell phones increases the risk of brain cancer, tumors of the auditory nerve and cancer of the parotid gland, the salivary gland in the cheek by the ear. The evidence for this conclusion is detailed in many publications in the peer-reviewed scientific literature. Smart meters use similar radiofrequency radiation, although the intensity of exposure in the immediate environment is under most circumstances lower than what one gets from holding a cell phone close to your head. The difference between a cell phone and a smart meter environment is that while the cell phone is used only intermittently a smart meter environment is continuous. There is also strong evidence that leukemia rates are increased among people living near to powerful AM radio transmission towers. Because WiFi, radio transmission towers and smart meters all generate similar RF radiation, my conclusion is that if the whole body is exposed, leukemia is the major cancer of concern, while if only the head is exposed as in using a cell phone, one sees increased risk of local cancers, such as brain cancer. There are a variety of other health effects reported as a result of exposure to RF radiation, but in my judgment the increased risk of cancer is both the best documented and the disease of greatest concern.

East Campus, 5 University Place, Room A217, Rensselaer, NY 12144-3429
PH: 518-525-2660 FX: 518-525-2665

UNIVERSITY AT ALBANY
State University of New York

Institute for Health and the Environment
and
Department of Environmental Health Sciences
School of Public Health

There have been no studies specifically of the health effects of smart meters to my knowledge, in great part because they haven't been around very long. But they utilize the same type of RF radiation that is used in cell phones. It should be noted that the World Health Organization this past summer declared radiofrequency radiation to be a possible human carcinogen. While it is true that the nature of exposure to RF from smart meters is not significantly different from that coming from other wireless devices, what is important is cumulative, aggregate exposure. My position is that we should practice "prudent avoidance", which is to say reduce unnecessary exposure to the degree possible until the magnitude of risk is fully understood.

My specific concerns about smart meters are as follows:

1. The benefit of the smart meters is entirely to the utilities, and is economic in nature. If they install smart meters they can fire those individuals who at present are employed to go around reading meters. Thus this is a job-killing proposal, and will increase unemployment which is already too high.
2. When a wireless smart meter is installed residents have no choice in the matter or ability to avoid exposure. But every individual has the option to use or not use other personal wireless devices. There is a major difference between an exposure which an individual chooses to accept and one that is forced on individuals who can do nothing about it.
3. Most wireless smart meters transmit signals to the utility for relatively short periods of time. However, the device continuously generates RF radiation that will expose anyone nearby 24/7.
4. The evidence for adverse effects of radiofrequency radiation is currently strong and grows stronger with each new study. Wired meters with shielded cable do not increase exposure. The same benefit to the utility could be achieved by use of a wired connection and this would not increase exposure of residents to excessive RF radiation.

Thank you for the opportunity to comment on this important public health concern, and on the general issue of smart meters. The use of wireless smart meters is unwise from both a public health point of view, which is where my expertise lies, but and also from a purely short and long-term economic point of view. If

Yours sincerely,

David O. Carpenter, M.D.
Director, Institute for Health and the Environment
University at Albany

East Campus, 5 University Place, Room A217, Rensselaer, NY 12144-3429
PH: 518-525-2660 FX: 518-525-2665

Appendix 10

International Agency for Research on Cancer

World Health Organization

PRESS RELEASE
N° 208

31 May 2011

IARC CLASSIFIES RADIOFREQUENCY ELECTROMAGNETIC FIELDS AS POSSIBLY CARCINOGENIC TO HUMANS

Lyon, France, May 31, 2011 -- The WHO/International Agency for Research on Cancer (IARC) has classified radiofrequency electromagnetic fields as possibly carcinogenic to humans (Group 2B), *based on an increased risk for glioma, a malignant type of brain cancer*[1], associated with wireless phone use.

Background

Over the last few years, there has been mounting concern about the possibility of adverse health effects resulting from exposure to radiofrequency electromagnetic fields, such as those emitted by wireless communication devices. The number of mobile phone subscriptions is estimated at 5 billion globally.

From May 24–31 2011, a Working Group of 31 scientists from 14 countries has been meeting at IARC in Lyon, France, to assess the potential carcinogenic hazards from exposure to radiofrequency electromagnetic fields. These assessments will be published as Volume 102 of the IARC *Monographs*, which will be the fifth volume in this series to focus on physical agents, after Volume 55 (Solar Radiation), Volume 75 and Volume 78 on ionizing radiation (X-rays, gamma-rays, neutrons, radio-nuclides), and Volume 80 on non-ionizing radiation (extremely low-frequency electromagnetic fields).

The IARC Monograph Working Group discussed the possibility that these exposures might induce long-term health effects, in particular an increased risk for cancer. This has relevance for public health, particularly for users of mobile phones, as the number of users is large and growing, particularly among young adults and children.

The IARC Monograph Working Group discussed and evaluated the available literature on the following exposure categories involving radiofrequency electromagnetic fields:

- occupational exposures to radar and to microwaves;
- environmental exposures associated with transmission of signals for radio, television and wireless telecommunication; and
- personal exposures associated with the use of wireless telephones.

International experts shared the complex task of tackling the **exposure data, the studies of cancer in humans**, the **studies of cancer in experimental animals**, and the **mechanistic and other relevant data**.

---

[1] 237 913 new cases of brain cancers (all types combined) occurred around the world in 2008 (gliomas represent 2/3 of these). *Source: Globocan 2008*

IARC CLASSIFIES RADIOFREQUENCY ELECTROMAGNETIC FIELDS AS POSSIBLY CARCINOGENIC TO HUMANS

Results

The evidence was reviewed critically, and overall evaluated as being *limited*[2] among users of wireless telephones for glioma and acoustic neuroma, and *inadequate*[3] to draw conclusions for other types of cancers. The evidence from the occupational and environmental exposures mentioned above was similarly judged inadequate. The Working Group did not quantitate the risk; however, one study of past cell phone use (up to the year 2004), showed a 40% increased risk for gliomas in the highest category of heavy users (reported average: 30 minutes per day over a 10-year period).

Conclusions

Dr Jonathan Samet (University of Southern California, USA), overall Chairman of the Working Group, indicated that "the evidence, while still accumulating, is strong enough to support a conclusion and the **2B classification**. The conclusion means that there could be some risk, and therefore we need to keep a close watch for a link between cell phones and cancer risk."

"Given the potential consequences for public health of this classification and findings," said IARC Director Christopher Wild, "it is important that additional research be conducted into the long-term, heavy use of mobile phones. Pending the availability of such information, it is important to take pragmatic measures to reduce exposure such as hands-free devices or texting. "

The Working Group considered hundreds of scientific articles; the complete list will be published in the Monograph. It is noteworthy to mention that several recent in-press scientific articles[4] resulting from the **Interphone study** were made available to the working group shortly before it was due to convene, reflecting their acceptance for publication at that time, and were included in the evaluation.

A concise report summarizing the main conclusions of the IARC Working Group and the evaluations of the carcinogenic hazard from radiofrequency electromagnetic fields (including the use of mobile telephones) will be published in **The Lancet Oncology in its July 1 issue, and in a few days online.**

---

[2] ***'Limited evidence of carcinogenicity'***: A positive association has been observed between exposure to the agent and cancer for which a causal interpretation is considered by the Working Group to be credible, but chance, bias or confounding could not be ruled out with reasonable confidence.

[3] ***'Inadequate evidence of carcinogenicity'***: The available studies are of insufficient quality, consistency or statistical power to permit a conclusion regarding the presence or absence of a causal association between exposure and cancer, or no data on cancer in humans are available.

[4] a. 'Acoustic neuroma risk in relation to mobile telephone use: results of the INTERPHONE international case-control study' (the Interphone Study Group, in Cancer Epidemiology, *in press*)
b. 'Estimation of RF energy absorbed in the brain from mobile phones in the Interphone study' (Cardis et al., Occupational and Environmental Medicine, *in press*)
c. 'Risk of brain tumours in relation to estimated RF dose from mobile phones – results from five Interphone countries' (Cardis et al., Occupational and Environmental Medicine, *in press*)
d. 'Location of Gliomas in Relation to Mobile Telephone Use: A Case-Case and Case-Specular Analysis' (American Journal of Epidemiology, May 24, 2011. [Epub ahead of print].

IARC, 150 Cours Albert Thomas, 69372 Lyon CEDEX 08, France - Tel: +33 (0)4 72 73 84 85 - Fax: +33 (0)4 72 73 85 75
© IARC 2011 - All Rights Reserved.

IARC CLASSIFIES RADIOFREQUENCY ELECTROMAGNETIC FIELDS AS POSSIBLY CARCINOGENIC TO HUMANS

For more information, please contact
Dr Kurt Straif, IARC Monographs Section, at +33 472 738 511, or straif@iarc.fr; Dr Robert Baan, IARC Monographs Section, at +33 472 738 659, or baan@iarc.fr; or Nicolas Gaudin, IARC Communications Group, at com@iarc.fr (+33 472 738 478)
Link to the **audio file** posted shortly after the briefing:
http://terrance.who.int/mediacentre/audio/press_briefings/

About IARC

The International Agency for Research on Cancer (IARC) is part of the World Health Organization. Its mission is to coordinate and conduct research on the causes of human cancer, the mechanisms of carcinogenesis, and to develop scientific strategies for cancer control. The Agency is involved in both epidemiological and laboratory research and disseminates scientific information through publications, meetings, courses, and fellowships.

If you wish your name to be removed from our press release e-mailing list, please write to com@iarc.fr.

Nicolas Gaudin, Ph.D.
Head, IARC Communications
International Agency for Research on Cancer
World Health Organization
150, cours Albert-Thomas
69008 Lyon
France

Email com@iarc.fr
http://www.iarc.fr/

© IARC 2011 - All Rights Reserved.

Appendix 11

American Academy of Environmental Medicine
[illegible] E Central • Ste 296 • Wichita, KS 67206
Tel: (316) 684-5500 • Fax: (316) 684-5709
[illegible]

Executive Committee

President
A.L. Barrier, M.D., FAAO-HNS
One Hospital Drive
Columbia, MO 65212

President-Elect
Amy Dean, D.O.
1955 Pauline Blvd Ste 100 D
Ann Arbor, MI 48103

Secretary
Charles L. Crist, M.D.
3009 Falling Leaf Ctr, Ste 1
Columbia, MO 65201

Treasurer
James W. Willoughby, II, D.O.
24 Main St.
Liberty, MO 64068

Immediate Past President
Robin Bernhoft, M.D., FAAEM

Advisor
Gary R. Oberg, M.D.,FAAEM

Board of Directors
Craig Bass, M.D.
Amy Dean, D.O.
Stephen Genuis, M.D., FAAEM
Martha Grout, M.D., MD(H)
Janette Hope, M.D.
W. Alan Ingram, M.D.
Derek Lang, D.O.
Glenn A. Toth, M.D.
Ty Vincent, M.D.

Continuing Medical Education
Chairman
James W. Willoughby, II, D.O.
24 Main St.
Liberty, MO 64068

Executive Director
De Rodgers Fox

January 19, 2012

Decision Proposed Decision of Commissioner Peevy (Mailed 11/22/2011)
BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA
On the proposed decision 11-03-014

Dear Commissioners:

The Board of the American Academy of Environmental Medicine opposes the installation of wireless "smart meters" in homes and schools based on a scientific assessment of the current medical literature (references available on request). Chronic exposure to wireless radiofrequency radiation is a preventable *environmental hazard that is sufficiently well documented to warrant immediate* preventative public health action.

As representatives of physician specialists in the field of environmental medicine, we have an obligation to urge precaution when sufficient scientific and medical evidence suggests health risks which can potentially affect large populations. The literature raises serious concern regarding the levels of radio frequency (RF - 3KHz – 300 GHz) or extremely low frequency (ELF – 300Hz) exposures produced by "smart meters" to warrant an immediate and complete moratorium on their use and deployment until further study can be performed. The board of the American Board of Environmental Medicine wishes to point out that existing FCC guidelines for RF safety that have been used to justify installation of "smart meters" only look at thermal tissue damage and are obsolete, since many modern studies show metabolic and genomic damage from RF and ELF exposures below the level of intensity which heats tissues. The FCC guidelines are therefore inadequate for use *in establishing public health standards. More modern literature shows medically* and biologically significant effects of RF and ELF at lower energy densities. These effects accumulate over time, which is an important consideration given the chronic nature of exposure from "smart meters". The current medical literature raises credible questions about genetic and cellular effects, hormonal effects, male fertility, blood/brain barrier damage and increased risk of certain types of cancers from RF or ELF levels similar to those emitted from "smart meters". Children are placed at particular risk for altered brain development, and impaired learning and behavior. Further, EMF/RF adds synergistic effects to the damage observed from a range of toxic chemicals. Given the widespread, chronic, and essentially inescapable ELF/RF exposure of everyone living near a "smart meter", the Board of *the American Academy of Environmental Medicine finds it unacceptable from a* public health standpoint to implement this technology until these serious medical concerns are resolved. We consider a moratorium on installation of wireless "smart meters" to be an issue of the highest importance.

The Board of the American Academy of Environmental Medicine also wishes to note that the US NIEHS National Toxicology Program in 1999 cited radiofrequency radiation as a potential carcinogen. Existing safety limits for pulsed RF were termed "not protective of public health" by the Radiofrequency Interagency Working Group (a federal interagency working group including the FDA, FCC, OSHA, the EPA and others). Emissions given off by "smart meters" have been *classified by the World Health Organization International Agency for Research on Cancer (IARC) as a Possible Human Carcinogen.*

Hence, we call for:

- An immediate moratorium on "smart meter" installation until these serious public health issues are resolved. Continuing with their installation would be extremely irresponsible.
- Modify the revised proposed decision to include hearings on health impact in the second proceedings, along with cost evaluation and community wide opt-out.
- Provide immediate relief to those requesting it and restore the analog meters.

Members of the Board
American Academy of Environmental Medicine

Appendix 12

((o)) for wireless

Smart Meter Opposition Actions across the United States

as of 5/29/12

California	• Installation of smart meters began in 2007. • On February 1, 2012, the California Public Utilities Commission agreed to allow electric customers to keep their current analog meter or reinstall an analog meter if a smart meter had been installed.1 • On April 19, 2012 the California Public Utilities Commission unanimously approved opt-out proposals and allow customers to have their smart meters removed at an additional cost. • Principal of CPUC: ***"Ms. Dorman agreed that there is no law mandating smart meter installation- and that the right to install a smart meter was "just an assumption" by the PUC and the utilities, and not based in law."***
Connecticut	• Installation of smart meter began in 2009. • On August 30, 2011, Connecticut's Department of Energy and Environmental Protection ("DEEP") asked the Public Utilities Regulatory Agency ("PURA") to suspend actions in smart meter cases until it could develop a policy on smart meters as required by Connecticut Public Act 11-80. • On or about October 4, 2011, Connecticut's Attorney General upheld the decision of DEEP and PURA.
District of Columbia	• The Washington, DC Office of the People's Counsel requested to the Washington, DC Public Service Commission that technical and economic feasibility of an opt-out program for Advanced Metering Infrastructure be investigated. In February 2012, the PSC announced that that no investigation was necessary. In response, on March 19, 2012, the Office of the People's Counsel filed an application for reconsideration in case 1065 arguing that the PSC is not fulfilling its public interest obligation. The request was denied.

1 California Public Utilities Commission's Decision Modifying Pacific Gas and Electric Company's SmartMeter Program to Include an Opt-out Plan: http://docs.cpuc.ca.gov/word_pdf/AGENDA_DECISION/158309.pdf

Florida	• *Installation of smart meters began in 2009.* • As of May 1, 2012 the following counties have passed anti smart meter resolutions: Indian River, Volusia, Brevard, and Charlotte • Brevard County Commissioners requested of Florida Power & Light ("FPL") a smart meter opt-out plan for its residents and called upon the Florida Public Service Commission to hold public hearings on the issue of smart meters and their potential benefits and/or potential hazards to Florida residents. FPL is about 20% complete of its smart meter installation in Brevard County.2 • The Florida Public Service Commission announced it will have an opt-out workshop at an unspecified date.
Georgia	• Installation of smart meters began in 2007. • Legislation allowing customers to elect not to have a smart meter installed on their property passed the State Senate but stalled in the State House (S.B. 459).3
Hawaii	• Installation of smart meters began in 2012. • March 2012, opt out approved. • On April 25, 2012, at a federal hearing, the parties agreed the preliminary injunction motion was rendered moot as a result of the defendant utility's oral agreement that it would refrain from installing a smart meter on the plaintiff's home.4
Illinois	• Federal injunction filed. • Hearing to be held on May 31, 2012 has been postponed. No new court date has been announced.
Louisiana	• Installation of smart meters began in 2011. • On February 28, 2012, the City-Parish city council voted to allow Lafayette Utilities System customers to opt-out of smart meters.5
Maine	• Installation of smart meters began in 2010. • Maine Public Utilities Commission allows for customers to opt-out of receiving a smart meter.6 • On May 10, 2012, the Maine Supreme Judicial Court heard oral arguments in a case to oppose opt-out fees.7

2 See Brevard County, Florida, Board of Commissioners Meeting of May 1, 2012, Minute Packet at pp. 14-18: http://brevardcountyfl.iqm2.com/Citizens/Detail_Meeting.aspx?ID=1144

3 S.B. 459: http://www1.legis.ga.gov/legis/2011_12/sum/sb459.htm

4 *Adam Asquith v. Kauai Island Utility Cooperative*, 12-cv-00134-HG-RLP (D. Hawaii 2012)

5 "Council opt-outs on sales tax, opts-in on "opt-out" KATC, February 28, 2012: http://www.katc.com/news/council-opts-out-on-sales-tax-opts-in-on-opt-out-/

6 See "PUC decision puts smart meter choice in consumer's hands" WCSH, May 18, 2011: http://south.wcsh6.com/news/news/puc-decision-puts-smart-meter-choice-consumers-hands/65253

Maryland	• Installation of smart meters began in 2011. • On May 24, 2012, the Maryland Public Service Commission ("MPSC") entered an order allowing individual who are opposed to smart meters to defer installation until MPSC issues a final, permanent order on whether to allow customers to opt-out of receiving a smart meter.8
Michigan	• Installation of smart meters is set to begin in August 2012. • Michigan Attorney General Bill Schuette issued a report on smart meters to the Michigan Public Service Commission, stating, "There must be a sufficient demonstration that implementation of the smart meter programs will actually produce a net economic benefit to customers. Second, customers must be afforded a meaningful and fair opportunity to opt out of smart meter installation without being penalized by unwarranted and excessive costs."9 • On January 12, 2012, the Michigan Public Service Commission opened a review of smart meters.10 • Introduced HB 5411 that requires utilities to allow customers to reject a smart meter, remove a previously installed smart meter from a home, and refrain from selling smart meter data to a third party. • Introduced HB 5439 that provides incentives for having a smart meter and disincentives for opting out. There is a $50 smart meter removal fee; however, this bill does not allow monthly fees imposed on those retaining an analog meter • 21 anti-smart meter resolutions and moratoriums have passed in Michigan.
Nevada	• Installation of smart meters began in 2010. • In February 2012, Nevada Public Utilities Commission approves smart meter opt-out plan.11
Oregon	• Installation of smart meters began in 2009. • On August 10, 2011, Portland General Electric Company offers smart meter opt-out option.12 • On May 17, 2012, City of Ashland offers customers to opt-out at no additional fee

7 *Friedman v. Maine Public Utilities Comm.*, Law Docket No. PUC-11-532

8 Maryland Public Service Commission announcement of Order #84926 dated May 24, 2012: http://webapp.psc.state.md.us/Intranet/sitesearch/Whats_new/Maryland%20PSC%20Issues%20Interim%20Order%20On%20Smart%20Meter%20Opt%20Outs.pdf

9 Michigan Attorney General Bill Schuette's report to Michigan Public Service Commission: http://efile.mpsc.state.mi.us/efile/docs/17000/0408.pdf.

10 Michigan Public Service Commission, Order Opening Docket U-17000: http://efile.mpsc.state.mi.us/efile/docs/17000/0001.pdf

11 "Nevada PUC approves smart meter opt-out plan" LasVegas Herald-Review, February 29, 2012: http://www.lvrj.com/business/nevada-puc-approves-smart-meter-opt-out-plan-140941433.html

12 Portland General Electric Company's Smart Meter Opt-Out Program: http://www.portlandgeneral.com/our_company/corporate_info/regulatory_documents/pdfs/tariff_updates/Update_08_10_11.pdf

Pennsylvania	• Installation of smart meters began in 2012. • In May of 2012, HB 2188 was introduced in the PA General Assembly that allows consumers to opt out of smart-meters. 13
Texas	• Installation of smart meters began in 2010. • The author of legislation authorizing smart metering in Texas, State Representative Dennis Bonnen sent a letter to the Public Utilities Commission clarifying the intent of the HB212914 was not to force smart meters on any customer.15 • On February 16, 2012, the Public Utilities Commission opened a project case entitled "PUC Proceeding to evaluate the feasibility of instituting a smart meter opt-out program."16
Vermont	• Installation of smart meters began in 2004. • On May 18, 2012, Governor Peter Shumlin signed into law S. 214 (Act 0170) allowing for smart meter installation if utility company (1) provides prior written notice to the customer indicating that the meter will use radio or other wireless means for two-way communication between the meter and the company and informing the customer of his or her rights; (2) allows a customer to choose not to have a wireless smart meter installed, at no additional monthly or other charge; and (3) allows a customer to require removal of a previously installed wireless smart meter for any reason and at an agreed-upon time, without incurring any charge for such removal.17 • S. 214 (Act 0170) requires the commissioner of health and commissioner of public service issue a joint report by January 15, 2013, which shall include the potential health effects of wireless smart meters.18
Virginia	• At a hearing before the Virginia State Corporation Commission on March 6. 2012 about demand side management, concerned citizens, members of the Center for Safer Wireless, and members of the Richmond Tea Party, expressed their concerns and outrage at mandatory smart meters in Virginia. • Dominion Power, the power company serving the most customers in Virginia, announced in a letter dated May 15, and cc'd to VA State Corporation Commission, that it "plans to offer opt out offerings, or offerings, before

13 Text of HB 2188: http://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=DOC&sessYr=2011&sessInd=0&billBody=H&billTyp=B&billNbr=2188&pn=3071

14 Text of HB2149: http://www.capitol.state.tx.us/tlodocs/79R/billtext/pdf/HB02129F.pdf#navpanes=0.

15 State Representative Dennis Bonnen's letter to the Public Utility Commission of Texas dated February 10, 2012: http://interchange.puc.state.tx.us/WebApp/Interchange/Documents/40190_12_720818.PDF.

16 See Public Utility Commission of Texas Proceeding to Evaluation the Feasibility of Instituting a Smart Meter Opt-Out Program: http://interchange.puc.state.tx.us/WebApp/Interchange/Documents/40190_1_718594.PDF.

17 S. 214 (Act 0170), AN ACT RELATING TO VERMONT ENERGY ACT OF 2012, at pp. 61-63: http://www.leg.state.vt.us/docs/2012/Acts/ACT170.pdf

18 *Id* at p. 62

deploying smart meters beyond our planned demonstrations areas."

Note: This document was created in cooperation with members of Naperville Smart Meter Awareness and Maryland Smart Meter Awareness.

Appendix 13

Congressional Research Service

Smart Meter Data: Privacy and Cybersecurity

Brandon J. Murrill
Legislative Attorney

Edward C. Liu
Legislative Attorney

Richard M. Thompson II
Legislative Attorney

February 3, 2012

Congressional Research Service
7-5700
www.crs.gov
R42338

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Fueled by stimulus funding in the American Recovery and Reinvestment Act of 2009 (ARRA), electric utilities have accelerated their deployment of smart meters to millions of homes across the United States with help from the Department of Energy's Smart Grid Investment Grant program. As the meters multiply, so do issues concerning the privacy and security of the data collected by the new technology. This Advanced Metering Infrastructure (AMI) promises to increase energy efficiency, bolster electric power grid reliability, and facilitate demand response, among other benefits. However, to fulfill these ends, smart meters must record near-real time data on consumer electricity usage and transmit the data to utilities over great distances via communications networks that serve the smart grid. Detailed electricity usage data offers a window into the lives of people inside of a home by revealing what individual appliances they are using, and the transmission of the data potentially subjects this information to interception or theft by unauthorized third parties or hackers.

Unforeseen consequences under federal law may result from the installation of smart meters and the communications technologies that accompany them. This report examines federal privacy and cybersecurity laws that may apply to consumer data collected by residential smart meters. It begins with an examination of the constitutional provisions in the Fourth Amendment that may apply to the data. As we progress into the 21st century, access to personal data, including information generated from smart meters, is a new frontier for police investigations. The Fourth Amendment generally requires police to have probable cause to search an area in which a person has a reasonable expectation of privacy. However, courts have used the third-party doctrine to deny protection to information a customer gives to a business as part of their commercial relationship. This rule is used by police to access bank records, telephone records, and traditional utility records. Nevertheless, there are several core differences between smart meters and the general third-party cases that may cause concerns about its application. These include concerns expressed by the courts and Congress about the ability of technology to potentially erode individuals' privacy.

If smart meter data and transmissions fall outside of the protection of the Fourth Amendment, they may still be protected from unauthorized disclosure or access under the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), and the Electronic Communications Privacy Act (ECPA). These statutes, however, would appear to permit law enforcement to access smart meter data for investigative purposes under procedures provided in the SCA, ECPA, and the Foreign Intelligence Surveillance Act (FISA), subject to certain conditions. Additionally, an electric utility's privacy and security practices with regard to consumer data may be subject to Section 5 of the Federal Trade Commission Act (FTC Act). The Federal Trade Commission (FTC) has recently focused its consumer protection enforcement on entities that violate their privacy policies or fail to protect data from unauthorized access. This authority could apply to electric utilities in possession of smart meter data, provided that the FTC has statutory jurisdiction over them. General federal privacy safeguards provided under the Federal Privacy Act of 1974 (FPA) protect smart meter data maintained by federal agencies, including data held by federally owned electric utilities.

A companion report from CRS focusing on policy issues associated with smart grid cybersecurity, CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell, is also available.

neighborhood data; (3) the access point—typically the smart meter; and, (4) the HAN—the home network."[50] Energy usage data moves from the smart meter,[51] and then to an "aggregation point" outside of the residence such as "a substation, a utility pole-mounted device, or a communications tower."[52] The aggregation points gather data from multiple meters and "backhaul" it to the utility using fiber, T1, microwave, or wireless technology.[53] Utilities typically rely on their own private networks to communicate with smart meters because they have found these networks to be more reliable and less expensive than commercial networks.[54]

As NIST explains, consumer data moving through a smart grid becomes stored in many locations both within the grid and within the physical world.[55] Thus, because it is widely dispersed, it becomes more vulnerable to interception by unauthorized parties[56] and to accidental breach.[57] 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[58]—or through communications components that may be incompatible with one another or possess outdated security protections.[59]

Smart Meters and the Fourth Amendment

The use of smart meters presents the recurring conflict between law enforcement's need to effectively investigate and combat crime and our desire for privacy while in our homes. With smart meters, police will have access to data that might be used to track residents' daily lives and routines while in their homes, including their eating, sleeping, and showering habits, what appliances they use and when, and whether they prefer the television to the treadmill, among a host of other details.[60] Though a potential boon to police, access to this data is not limitless. The Fourth Amendment, which establishes the constitutional parameters for government investigations, may restrict access to smart meter data or establish rules by which it can be obtained.[61] The Fourth Amendment ensures that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...."[62] This section discusses whether the collection and use of smart meter data may

[50] *Id.*

[51] The home network will be used to provide *consumers* with near real-time data on their energy usage. *Id.* at 13-15.

[52] *Id.* Many urban installations use wireless mesh networks to carry data from the meters to the aggregation point. These networks are more reliable because each smart meter can serve as a router in the network, providing redundant network coverage. *Id.* at 18.

[53] *Id.* at 16, 19.

[54] *Id.* at 4, 19, 44.

[55] NIST PRIVACY REPORT, *supra* note 11, at 23.

[56] *Id.* at 23-24.

[57] *Id.* at 29.

[58] *See id.* at 9, 12, 33, and 36.

[59] MIT GRID STUDY, *supra* note 18, at 209, 213-16.

[60] Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, ¶ 3 (2008).

[61] Additionally, as described below, there are federal statutory protections that may pertain to this data. State constitutional and statutory safeguards may also apply, but these are beyond the scope of this report.

[62] U.S. CONST. amend IV.

disagreed, broadly declaring "the Fourth Amendment does not prohibit the obtaining of information revealed to a third-party and conveyed by him to Government authorities, even if it is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third-party will not be betrayed."[126] The Court further noted that "the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[127]

Three years later, the Court extended the third-party doctrine to outgoing numbers dialed from a person's telephone.[128] In *Smith v. Maryland*, the defendant robbed a woman and began making obscene phone calls to her.[129] Suspecting Smith placed the calls, the police used a pen register to track the telephone numbers dialed from his phone.[130] The police failed to obtain a warrant or subpoena before installing the pen register.[131] The register revealed that Smith was in fact making the phone calls to the woman. In denying Smith's motion to suppress, the Court relied on the third-party doctrine, stating that "this Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[132] As applied to the telephone context, the Court found that "[w]hen he used his phone, [Smith] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [Smith] assumed the risk that the company would reveal to police the numbers he dialed."[133]

Traditionally, utility records have been handled similarly to bank records and telephone records. Several lower federal courts have held that customers do not have a reasonable expectation of privacy in their utility records, thereby permitting warrantless access to these records. In *United States v. Starkweather*, the Ninth Circuit held that a person does not have a reasonable expectation of privacy in his utility records.[134] The panel reasoned that (1) these records were no different from phone records, and thus did not justify a different constitutional result; and (2) the public was aware that such records were regularly maintained, thereby negating any expectation of privacy.[135] The Eighth Circuit has also upheld warrantless police access to utility records in *United States v. McIntyre*.[136] The Eighth Circuit panel distinguished *Kyllo*, declaring that the means of obtaining the information in *Kyllo* (a thermal-imaging device) was significantly more intrusive than simply subpoenaing the records from the utility company.[137] The court held that "the means to obtaining the information is legally significant."[138] Likewise, the court in *United*

(...continued)

for access and use.") (citing Entick v. Carrington, 19 How. St. Tr. 1029 (C.P. 1765)).

[126] *Miller*, 425 U.S. at 443.

[127] *Id.*

[128] Smith v. Maryland, 442 U.S. 735 (1979).

[129] *Id.* at 737.

[130] *Id.*

[131] *Id.*

[132] *Id.* at 743-44.

[133] *Id.* at 744.

[134] United States v. Starkweather, No. 91-30354, 1992 WL 204005, at *2 (9th Cir. Aug. 24, 1992).

[135] *Id.*

[136] United States v. McIntyre, 646 F.3d 1107 (8th Cir. 2011).

[137] *Id.* at 1111.

[138] *Id.*

Appendix 14

Vulnerabilities of Wireless Water Meter Networks

Black Hat USA Las Vegas August 3, 2011
by John McNabb
johnmcnabb@comcast.net

Abstract.

Why research wireless water meters? Because they are a potential security hole in a critical infrastructure, which can lead to a potential leakage of private information, and create the potential to steal water by lowering water bills? It's a technology that's all around us but seems to too mundane to think about.

Because a hacker can't resist exploring technology to see how it works and how to break it... because they are there? In this talk the speaker, who managed a small water system for 13 years, will first present an overview of drinking water security, review reported water system security incidents and the state of drinking water security over the past year, and will then take a deep dive into the hardware, software, topology, and vulnerabilities of wireless water meter networks and how to sniff wireless water meter signals.

ORGANIZATION OF THIS PAPER:

I. INTRODUCTION

US drinking water utilities collect $40 billion annually, and depend on the readings from water meters for this income. Wireless water meters, while providing quantifiable benefits to a local drinking water utility and their customers, may also result in security vulnerabilities. Water utilities have historically been a target for attacks by nation states, terrorists, and others, and need to do more to protect their critical assets from potential attack.

This paper discusses the specific facts and issues concerning wireless water meters, in their various forms as Automatic Meter Reading, Advanced Metering Infrastructure, and as part of an overall "Smart Grid" infrastructure which includes electric and gas utilities. Furthermore, the larger context of drinking water security is also addressed to put this potential risk in context. Finally, the various security and privacy issues raised by wireless water meters are discussed.

Vulnerabilities of the "Smart Grid"

The electric Smart Grid has been under a lot more scrutiny than the drinking water component. While some of the characteristics of the electric grid, such as the complete interdependence of the electric grid, are not mirrored in the drinking water infrastructure, which is highly fragmented, the characteristics of the hardware & firmware used in smart electric meters, and their vulnerabilities, may be applicable to smart water meters.

Jonathan Pollet of Red Tiger Security, in his Black Hat USA presentation[51] last year, listed existing vulnerabilities of the electric grid's AMR and Smart Meters:

- Perimeter Issues. These systems are interconnected with business applications and often also interconnected to operational SCADA and energy Management systems.
- Back End Server/Application issues. The applications have similar vulnerabilities as do business applications, have less secure implementation of protocols, and have old versions of application frameworks.
- Too much trust in the Protocol. Most AMI/AMR vendors trust that the 802.15.4 protocol security implementation will work and haven't considered what to do when it doesn't.
- End devices have limited resources. The meters themselves typically do not have the resources (memory, computational power, etc.) to handle security features.

What could an attacker do to these electric Smart Grid systems, considering those vulnerabilities? Pollet listed the following capabilities exist for an attacker, which his firm has duplicated in their own research:

- Data enumeration - read real time grid data.
- Host enumeration - scanning from meter back to the head-end
- Service enumeration – determine what services are exposed
- Change data (such as change usage & billing data)
- Steal accounts and passwords (man in the middle attacks + Wireshark)
- Damage core system components (i.e. bricking meters)
- Denial of Services (PING FLOOD, malformed packets, etc.)

What could a hacker do to the smart grid?

Smart Grid vulnerabilities have been documented[52] by the Israeli IT security firm C4 following security audits on a water pipeline and two electric grids; they also listed potential attacks based on those vulnerabilities:

(1) DDos attacks are possible where the smart grid uses public IP addresses;
(2) Each meter is a node in the smart grid network; so an attacker who uses the communication module of the smart meter can cause network-wide changes;

---

[51] *Electricity for Free? The Dirty Underbelly of SCADA and Smart Meters*, Jonathan Pollet, Black Hat USA, 2010

[52] *The Dark Side of the Smart Grid – Smart Meters (in)Security*, C4 security, September, 2009. http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf

(3) Many meters did not have any authentication or encryption support, allowing an attacker to impersonate the control center and send unauthorized commands to meters or read metering data;
(4) The protocol between the master meter and slave meter is usually considered of lesser importance because its impact is restricted to a single customer household; however this may allow the insertion of a "man in the middle" device to lower the usage reading, which could be of considerable impact to the utility if such devices are mass produced like pirate cable boxes;
(5) Some slave meters that support disconnection of the customer use wireless protocols, making it possible for an attacker to disconnect multiple customers;
(6) Many meters were unable to improperly handle malformed requests, making them vulnerable to a Buffer Overrun/Overflow Vulnerability; allowing the attacker to execute arbitrary code;
(7) The capability to remotely execute firmware upgrades can allow an attacker to disconnect the meter or take any other action; and
(8) Lack of input validation could allow an attacker to submit a malformed packet which could lead to arbitrary code execution.

What could a hacker do to the water utility control systems?

The Roadmap to Secure Control Systems in the Water Sector listed[53] the following potential impacts from an attacker:

- Interfere with the operation of chemical feed systems, to cause over or under dosing;[54]
- Make unauthorized programming changes, resulting in disabled services, reduced pressure or flows of water into fire hydrants;
- Modify control system software to produce unpredictable results;
- Block data or send false information to operators to prevent them from being aware of alarm conditions;
- Change or disable alarm thresholds;
- Prevent access to account information;
- Cause multiple failures that may be too much for the facility to manage;
- Be used as ransomware

Privacy issues

Privacy of the data collected by the "smart grid" is a major concern. A poll of more than 9,000 consumers in 17 countries by the Accenture consulting form found that about 33% would

[53] *Roadmap*, page 15.
[54] Just as Marc Maiffret was able to do in his pen test of an unnamed California water system. "We did not change anything or go beyond showing access to the control system where an operator could then make changes at the point of access we had. In this specific case the filtration levels of different chemicals could be manipulated. Specifically one of the plant engineers and I came up with the maybe not so funny joke "SCADA Sport Fishing." And I believe that had to do with a modification of chlorine levels..." Email from March Maiffret, April 18, 2011.

be discouraged from using smart metering if it gave the utility more data about their energy use.[55] There are many scenarios where such information could be used as an invasion of privacy, as summarized in this table:

WHO WANTS SMART METER DATA?	HOW COULD THE DATA BE USED?[56]
Utilities	To monitor electricity usage and load; to determine bills
Electricity usage advisory companies	To promote energy conservation and awareness
Insurance companies	To determine health care premiums based on unusual behaviors that might indicate illness
Marketers	To profile customers for targeted advertisements
Law enforcers	To identify suspicious or illegal activity
Civil litigators	To identify property boundaries and activities on premises
Landlords	To verify lease compliance
Private investigators	To monitor specific events
The press	To get information about famous people
Creditors	To determine behavior that might indicate creditworthiness
Criminals	To identify the best times for a burglary or to identify high-priced appliances to steal

Similar concerns may be raised, one would think, with smart water meters, which could show information based solely on the total water usage if reported in short intervals of 5-15 minutes, about whether a house was occupied, and when, when people were awake, how many people were in the house, how many times they took a shower, used the toilet, etc. Especially in addition to smart grid electric load information, one could get a good picture of human activity in a house that would be an invasion of privacy.

In Cary, North Carolina, such concerns were raised about a proposal to retrofit water meters with smart meters:

> Cary's citizens are right to be **concerned** about the information about our **private lives** that our Town staff will be able to collect if the Aquastar/AMI water meter system is implemented as planned. According to **Daniel Burrus**, a technology futurist and keynote speaker at the Autovation conference last September, "As a utility, I could know exactly when you take a shower, exactly when you water the plants or wash the dishes. I could figure out how much water or electricity you are

[55] *Privacy on the smart grid: Are smart meters spies? They don't have to be*, by Ariel Blecher, IEE Spectrum, October 2010. http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid.

[56] Ibid. This table was adapted by Blecher from Table 5-3, pp. 30-32 of *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, NSTIR 7628, National Institute of Standards and Technology, August 2010

using at any point in time, and probably figure out what you are using it for." [57] [emphasis in original.]

A few weeks ago, in early November 2009, the Town of Cary Council approved the purchase and installation of smart wireless water meters at a cost of $17. 9 million. This installation makes Cary the first municipality in North Carolina, the USA and perhaps the world that will have a metering system that will be used by "Water Conservation Technicians" (aka **Water Cops**) to monitor (i.e. **spy**) on our consumption of water on a minute by minute basis, 24 hours per day and 7 days a week for the purpose of enforcing water conservation measures. This equipment gives the water cops the ability to **collect evidence around the clock** and to **issue tickets** to violators of conservation rules. Town ordinances **allow the Town to assess civil and/or criminal penalties** including fines, debt, and termination of service for any period of time for violators. Many citizens are appalled that the Town of Cary has found it necessary to resort to **such extreme measures** to get citizens to conserve water. A civilized society depends upon its citizens to **voluntarily** follow the rules and in most communities this is enough. Do our leaders think of us as **unsophisticated wild animals** that need constant policing to assure compliance? In fact there has been discussion and consideration of **adding water cops** commensurate with population growth. Will we soon have "Block Captains" to report on a resident's behavior and compliance with the rules? Immigrants from eastern Europe tell us that the right to privacy is precious. If you give up this right it won't be long before the government starts to erode all rights. Do we want that in Cary? [58][emphasis in original.]

The Cyber Security Working Group of the Smart Grid Interoperability Panel, in NISTIR 7628 concluded that, yes, there are privacy concerns with the smart grid (for electricity; there is no NISTIR for the water smart grid), and made the following recommendations to mitigate those concerns:

(1) A utility should conduct a Personal Information Assessment (PIA) before deciding to participate in the Smart Grid to identify risks to the personal information that is collected, processed, stored and otherwise handled, and determine other appropriate risk mitigation activities.
(2) Develop and formally document privacy policies and practices drawn from the Organization for Economic Cooperation and Development (OECD) Privacy Principles and other sector's privacy policies, regulations, and laws that may be applicable.
(3) Develop a comprehensive set of privacy use cases that will help utilities and third-party Smart Grid providers to rigorously track data flows and the privacy implications of collecting and using data flows and their privacy implications.

---

[57] *Utility Expert describes privacy invasion through AMI*, The Cary Watchman, January 28, 2010. http://carywatch.net/watermeter.html
[58] *Cary leads the nation, in Water Cops*, The Cary Watchmen, January 4, 2010.

(4) Educate the public about the privacy risks in the Smart Grid and what they as consumers can do to mitigate those risks.
(5) Share information about solutions to common privacy-related problems with other Smart Grid participants.
(6) Manufacturers and vendors of smart meters should collect only the energy and personal data necessary for the purposes the smart meter operations.

Beyond the Smart Grid: Hydrosense

But… it gets better!

The amount and quality of information that can gathered about human activity in a household, which is limited when relying just on the water usage information from the water meter, can be supplemented to provide a complete picture of water use by a new device called HydroSense.

HydroSense[59] is a simple, single point, sensor of pressure of water in a building, which can give accurate information about when each water fixture is turned on and for how long. Each water fixture can be accurately identified by sensing the pressure at a single point in the buildings infrastructure. The information is then sent via wireless – perhaps "backhauled" over the same wireless channel used by the water meter – to the water utility to accumulate the information. Hydrosense works based on the following theory of operation:

- The home plumbing system forms a closed loop pressure system
- The instant a valve is opened or closed a pressure change occurs and a pressure wave, also called a surge or water hammer, is generated;
- The unique transient water hammer signature sensed for a particular fixture depends on the valve type and its location in the plumbing network of the home;
- One can discriminate between fixtures of the same type that are in different locations because their pressure wave impulses traverse different paths through the pips;
- This allows one to use Hydrosense to estimate flow rate, which is related to pressure change via Poiseuille's Law, which is that the volumetric rate of fluid in a pipe Q is dependent on the radius of the pipe r, the length of the pipe l, the viscosity of the fluid μ and the pressure drop ΔP.
- Hydrosense measures the change in pressure ΔP

Hydrosense is a simple, screw-on device that doesn't require the services of a plumber. It operates on battery power, or uses WATTR[60], a self-powered version that uses the flow of water to power the device. Then there is NAWMS[61]: the Nonintrusive Autonomous

---

[59] *Hydrosense: Infrastructure-Mediated Single-Point Sensing of Whole-Home Water Activity*, Froelich, Jon, Eric Larson, Tim Campbell, Conor Haggerty, James Fogarty, and Shwetak N. Patel, *Ubicomp 2009*, Orlando, Florida.

[60] *WATTR: A method for self-powered wireless sensing of water activity in the home*, Campbell, Tim, Eric Larson, Gabe Cohen, Jon Froelich, Ramses Alcaide, and Shwetak N. Patel, *UbiComp, 2010.*

[61] *NAWMS: Nonintrusive Autonomous Water Monitoring System*, Kim, Younghun, Thomas Schmid, Zainul M. Charbiwaia, Jonathan Friedman, and Mani B. Srivastava, *SenSys 2008.*

Water Monitoring System, which uses the flow information from the existing water meter in addition to one or more vibration sensors on water pipes.
These devices are part of a larger effort called *infrastructure-mediated sensing*, which is being applied to detect the use of gas (GasSense) and electronic devices (ElectriSense) as well as for electric devices and for water fixtures.

While these devices would be useful to assist homeowners and utility companies to track and control resource use, with obvious benefits to society, they offer substantial possibilities to the ultimate invasion of privacy, since they could allow one or more utility companies, or the government, an eavesdropper, or an attacker, to know just about anything that is done within the home.

VI. HACKS OF OTHER "SMART METERS" AND WIRELESS DEVICES

Other smart meters and wireless devices have been successfully sniffed & hacked, which lends confidence to the assumption that wireless water meters can also be hacked. Reviewing these case histories can be instructive to understand common elements that would also apply to wireless water meters and the process for attacking them.

Smart Parking Meters – Joe Grand, Jacob Applebaum, & Chris Tarnovsky

This, of course, is a different type of "meter" and the attack didn't involve any wireless component, although it could have. In their presentation *"Smart" Parking Meter Implementations, Globalism, and You*, at Blackhat USA 2009, Grand et al. followed a methodical process to postulate potential attacks, gather information, analyze the hardware, reverse engineer firmware, and analyze the smartcards used.

By looking at oscilloscope capture of San Francisco MTA smart card transactions, they were able to determine how to replay transactions with modified data to "obtain unlimited parking." They used a "shim" between the smart card and the meter to monitor the I/O transaction with a digital oscilloscope, and were able to decode the transmissions by hand. They then developed modified code to show that the card had the maximum possible value, and ported the code to a Silver Card to test on a meter.

They recommended some fixes to make these smart parking meters more secure: daily audit log/serial number correlation/blocklisting, reduce the number of access methods, incorporate antitamper mechanisms into the meter circuitry, abandon the offline system, and have meters communicate with a "mothership" using digital signatures for all transactions.

Smart Subway Fare Meters – Russell Ryan, Zack Anderson, Alessandro Chiesa

In their presentation "*Anatomy of a Subway Hack*" that a court order prevented them from giving at DEF CON 16 in 2008, these three MIT students demonstrated a thorough analysis of the vulnerabilities in the Boston MBTA subway electronic fare system. They attacked the RFID using a MiFare RFID reader/writer, and OpenPCD open design 13.56MHz RFID reader and emulator, and a USRP and GNU radio and a plugin they wrote.

They used GNU radio and a Universal Software Radio Peripheral (USRP) to sniff the RFID toolchain of the Charlie card smartcards communication with the card reader at 13.56 and

12.71 Mhz. They sniffed the handshake and used a KwickBreak FPGA Brute-Forcer to crack the key, allowing them to clone the cards.

They used a MSR206 Stripe card reader/writer that worked with their GPL'd software to read the Charlie Card, then reversed engineered the code to enable them to forge a card with a large stored value. They wrote Python libraries for analyzing magcards and integrated it with the MSR206 card reader/writer to allow them to forge cards.

Smart Electric Meters – IOActive

David Baker, Director of Services at IOActive, writes in the October 2009 Journal of Energy Security that

> "Most alarming is that "worm-able" code execution on standard smart meters has been achieved. The smart meter's chipset used for radio communication is publicly available in a developer kit format, and the radio interface's lack of authentication can be leveraged to produce a worm. If an attacker installed a malicious program on one meter, the internal firmware could issue commands to flash adjacent meters until all devices within an area were infected with the malicious firmware. Once the worm has spread to the meters, the attacker gains several abilities including:
>
> • Connecting and disconnecting customers at predetermined times.
> • Changing metering data and calibration constants.
> • Changing the meter's communication frequency.
> • Rendering the meter non-functional." [62]

In his Black Hat USA 2009 presentation, *Smart Grid Device Security*, Mike Davis described some of the inherent hardware & software problems of an electrical smart meter, an pointed out that the TI MSP430 chip has small stack space, no memory protection, can flash itself, and that malware can hook interrupt vectors allowing 'normal' meter function – that malware can patch and re-patch the firmware! He found that the meters also did not have effective encryption and couldn't tell the difference between another meter and one that was authorized to patch its firmware. He wrote a worm, self-replicating code, and ran it in a simulation of 22,000 nodes, and found that in less than 24 hours the work had taken over 15,000 of the meters.

Smart Electric Meters/Zigbee – Joshua Wright, Inguardians

In Killerbee: *Practical ZigBee Exploitation Framework or "Wireless Hacking and the Kinetic world"*, which he has presented Toorcon 11, Quahogcon, and a number of other conferences, Joshua Wright described ZigBee and the exploitation framework for it which he has developed. ZigBee used 2.4 GHz IEEE 802.15.4, DSSS modulation, and 128-bit AES-CCMP encryption, and is used for a multitude of applications such as smart thermostats, spill gates at dams, lighting, HVAC, and natural gas control, as well as electric meters.

---

[62] *Making a Secure Smart Grid a Reality*, David Baker, Journal of Energy Security, October, 2009

Zigbee keys are sent in plaintext, and has meager replay protection. Killerbee is a low-cost system, using the $40 AVR RZ Raven USB stick and software written by Wright, which can sniff, decrypt, and take over Zigbee controlled devices. NOTE: Inguardians also has prepared *Advanced Metering Infrastructure Attack Methodology*, which is very useful.

"How to sniff strange radio" – Travis Goodspeed

At the April 22, 2010 Source Boston, Travis Goodspeed presented "*Not quite ZigBee; or How to sniff a strange radio*," Travis showed how he reverse engineered a variety of "weird radios," such as radio remote controls, Apple/Nike+Show Pod, Garmin ANT+ Watch, and the Microsoft keyboard. After examining the die badges to identify the internal part number he was able to focus on Chipcon ISM Band, Nordic nRF24E1G, Amicom A7125, and other chips.

His methodology is to dissect a device, get part numbers, chip die photographs, & firmware, determine radio encoding, rate, and frequency, and then build a transceiver (such as the modified IM-ME "pink pager)." He cautioned that one needs to get the part numbers, because vulnerabilities are indexed by part numbers, not the product name; and that it is important to read the whole datasheet, and also read the errata sheets, you are sure to find bugs.

802.11 Frequency Hopping Spread Spectrum (FHSS) Hacks – Rob Havelt

At Black Hat Europe 2009, in *Yes it is Too WiFi, and No It's Not Inherently Secure*, Rob Havelt discussed how he was able to crack Frequency Hopping Spread Spectrum (FHSS) in 802.11 using GNU radio and a USRP 2.0 and how it is not inherently secure. "For legacy 802.11, it was possible to just use a USRP locked to a specific channel band, then feed the raw data into the BBN Adroit code - for kicks, you could set a file as the sniffer interface for Kismet or a tool like that to do analysis at each layer."[63]

Havelt explained that FHSS is still pretty widely used, was originally designed in World War II as a security protocol; but actually provides little to no security at all. Typically, FHSS uses one of 78 different hop sequences defined in the ANSI/IEEE 802.11 standard to hop to a new 1MHz channel about every 400 milliseconds. It was very resistant to narrow band interference and narrow band jamming. FHSS uses the same type of management frames used in 802.11 b/a/n/g – Beacon, Associate, Probe, and Probe Response.

To join a FHSS network, he explained, you need either the SSID, MAC address of an authorized client, or a40 bit WEP key, but usually just the SSID will do. The SSID can be found in the Frame Body. The modulation, hop patterns and other parameters are similar to those in Bluetooth; so one can apply the Bluetooth ideas and methods[64] developed by Dominic Spill and Andrea Bittau, and of Spill and Michael Ossman. But, he finished, its easier than Bluetooth because with 802.11 FHSS you only need to use Software radio to listen for a management frame to hop by.

---

[63] Email from Rob Havelt, February 3, 2011.

[64] See the Bluesniff project at http://gr-bluetooth.sf.net, and *Bluesniff: Eve Meets Alice and Bluetooth* by Spill and Bittau; http://darkircop.org/w00t.pdf, and *Building an All Channel Bluetooth Monitor* by Ossman & Spill; http://www.ossmann.com/shmoo-09/ossmann-spill-shmoo-2009.pdf.

FHSS 900 Mhz Wireless Sniffing – atlas, cutaway & Q

In their Shmoocon 2011 presentation *Hop Hacking Hedy*, atlas, cutaway and Q showed how FHSS was not inherently secure and how to crack it in 900 Mhz wireless devices using the CC1111EMK 868-915 Evaluation Module Kit programmed with Goodfet, using SmartRFstudio and python code they wrote.

They explained that a listener, to "tune in" to an FHSS signal, needs to know the number of frequencies, the hopping sequence, and the dwell time. One must have the hopping pattern; must break the PRBG associated with the algorithm to obtain spread codes, analyze channel data in time domain fast enough to catch the hops until releases start to occur, and generate the entire pattern for all clock values[65].

The goal of their project was to build some devices that can be configured for known ISM bands, automatically analyze channel spacing, can decode FHSS hopping patterns, and utilize a custom code base. The hardware they selected was the CC1111EMK868-915 Evaluation Kit because it was CC111-based, all the pins were broken out, it was programmable via Goodfet, and Goodfet interacts via Data Debug. The CC111 is the USB-enabled version of TI's popular <1 GHz radio, and is the same radio used in the majority of today's smart meters.

Their resulting firmware, after stripping Specan firmware code to remove display and shrink the frequency range and leveraging Goodfet for dumping Data Debug, using Python scripts for halting display, was maxscan, a spectrum analyzer, hoptrans to create a carrier wave where number of channels, channel spacing, and hop timing, is known, and minscan, to detect channel hops. Minscan initializes frequencies, scans frequencies for minimum RSSI, monitors jumps in RSSA, stores detected spikes, dumps data via Goodfet, and data is then analyzed offline.

Their project was still in development; they reported that channel identification was broken but close, there were some bugs in data storage and dumping, they still need to analyze and coalesce the final data better. One of their goals was to port it to the CC1110 of the IM-ME dongle (the "pink pager").

The code is available at http://code.google.com/p/hedyattack/

VII. METHODS THAT I AM WORKING ON TO SNIFF WATER METERS

The above cases, as well as other research, have informed my present efforts to devise one or more methods to sniff the signals from a 900 mhz wireless water meter and hack into the network. Although it seems obvious that it should be possible to do so, one cannot rest on such an assumption but must show how it can be done.

Because most US wireless water meters use the 902 – 928 Mhz ISM band, there are no suitable "off the shelf" devices to easily use, so it took some doing to see what could be put together. As of the date of the submittal of this paper, July 13, I have been working on the following potential methods to sniff & hack a 900 Mhz wireless water meter, and hope to show some success on at least one of these methods when I present this paper on August 3:

[65] They cite *Building an All-Channel Bluetooth Monitor* by Michael Ossman and Dominic Spill from Shmoocon 2009.

(1) **Itron FS3 Handheld Reader,** used, purchased on Ebay. This is the same unit used by water utility's to read the wireless meters onsite. Haven't gotten it to work yet.
(2) **Atmel RZ600 Development Kit.** Has a 900 Mhz antenna and is advertised to be capable of being used as a development platform or just for packet sniffing. However, it did not work right out of the box with the software supplied in the kit, and then their help desk informed me that they don't yet provide the software to use it for packet sniffing. I am experimenting with some software to link it to Wireshark, but no success to date.
(3) **Texas Instruments CC1111 868-915 Mhz Evaluation Module Kit.** Will use to try to replicate the FHSS technique demonstrated by atlas, cutaway & Q, after making a working Goodfet. (Thanks to Travis Goodspeed for sending me 5 Goodfet 31 circuit boards, hopefully I won't break all of them.) May also try Bus Pirate and a TI CC Debugger.
(4) **RFM DNT900DK.** The kit includes: two DNT900P radios installed in DNT900 interface boards, two 2 dBi dipole antennas with two U.FL coaxial jumper cables, two 9 V wall-plug power suppliers, 120/240 VAC, plus two 9 V batteries, and two RJ-45/DB-9F cable assemblies, one RJ-11/DB-9F cable assembly, and two A/B USB cables. Looks promising but haven't tried it yet.
(1) **FunCUBE Dongle Pro.** Just received it as of the date of submission of this paper. The FunCUBE Pro is advertised as a software defined radio that operates in the 64 – 1,700 Mhz range. I will see if I can use it to replicate Havelt's methodology.
(2) **IM-Me.** I am dying to replicate the uses of this pager which was demonstrated in "*Real Men Carry Pink Pagers*" by Travis Goodspeed and Michael Ossmann at ToorCon 2010, and see what other uses I can get out of it. I will try this if I have time.

VIII. CONCLUSION

Water utilities have a number of well-known and documented cyber security vulnerabilities, both in their control systems and in their newer wireless water meter sensor networks. It is vital for the health of the nation's 150,000 water utilities and the 250 million people whom they serve that these vulnerabilities be addressed forthrightly and are resolved. Hopefully this paper has served to advanced that purpose, to make such vulnerabilities known so they can be resolved by the appropriate parties.

RESOURCES FOR SECURITY ISSUES

- **McNabb white paper http://media.blackhat.com/bh-us-11/McNabb/BH_US_11_McNabb_Wireless_Water_Meter_WP.pdf/**

- **McNabb power point from UW Lockdown Conference 7-12-12: Vulnerabilities of smart meters for water utilities; http://www.cio.wisc.edu/lockdown-2012-presentations.aspx**

- **Dark Reading Thursday July 19, 2012**
  Tech Center: Advanced Threats
  Smart Grid Researcher Releases Open Source Meter-Hacking Tool
  'Termineter' unleashed prior to presentations on smart meter security next week at BSides, Black Hat USA

  http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/240004014/smart-grid-researcher-releases-open-source-meter-hacking-tool.html#.UAliWrvmbNY.email

Appendix 15

Testimony
By Lillie Coney
Associate Director
Electronic Privacy Information Center (EPIC)

Before the
House Committee on Science and Technology
Subcommittee on Technology and Innovation

July 1, 2010
Room 2318 Rayburn House Office Building
U.S. House of Representatives

EPIC would like to thank the Subcommittee Chair and Ranking Member for this opportunity to speak with you on a matter that has emerged as one of the leading privacy challenges for our generation.

EPIC is a public interest research center, based in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has a long-standing interest and specialization in privacy and technology issues.[1] EPIC has a particular interest in the privacy implications of the Smart Grid standards, as we anticipate that this change in the energy infrastructure will have significant privacy implications for American consumers.[2] In other similar areas, EPIC has consistently urged federal agencies to minimize the collection of personally identifiable information (PII) and to establish privacy obligations when PII is gathered.

It is rare today to discover an industry that collects, retains, and uses vast amounts of personal information that is also transparent, accountable, and operates collaboratively under state regulations. Utilities "do what they are told," adhering to rules established by public utility commissions and business models based upon fair information practices. The electric utility industry has done this for over one hundred years. It is EPIC's hope that they will adhere to this model of conduct as they move toward full deployment of the Smart Grid.

However, there will be great temptation to monetize the information about consumer electricity consumption in ways that may threaten consumer privacy, competitiveness of businesses, both small and large, and the security of Smart Grid infrastructure should it become a "plug and play" environment.

---

[1] EPIC, Electronic Privacy Information Center, http://www.epic.org (last visited June 29, 2010); EPIC, Privacy, http://www.epic.org/privacy/default.html (last visited June 29, 2010).
[2] EPIC, The Smart Grid and Privacy, http://epic.org/privacy/smartgrid/smartgrid.html (last visited June 29, 2010).

I. PRIVACY AND THE SMART GRID

A. DEFINING PRIVACY AND THE SMART GRID

Privacy is one of the most fundamental and basic of human rights. Without it, many other rights, such as the freedoms of speech, assembly, religion and the sanctity of the home, would be jeopardized. Although most countries around the world include explicit protection of a right to privacy in their constitutions, it remains one of the more difficult rights to define.

The focus for protecting privacy of information stored on computers or exchanged on computing networks is determining whether data is or is not PII. This type of information can locate or identify a person, or it can be used in conjunction with other information to uniquely identify an individual. Historically, PII includes name, social security number, address, phone number, or date of birth. In the Internet Age, the list of PII has grown to include other data, including e-mail addresses, Internet Protocol (IP) addresses, social networking pages, search engine requests, log records, and passwords.

Our legal system has long recognized and protected an individual's right to personal privacy in PII. The drafters of the Constitution "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation" of constitutional principles.[3] Moreover, public opinion polls consistently find strong support among Americans for legally cognizable privacy rights in law to protect their personal information from government and commercial entities.[4]

More recently, the Supreme Court, in *Kyllo v. United States*,[5] addressed the privacy implications of monitoring electrical use in the home. After reviewing precedent, the Court found that a search warrant must be obtained before the government may use new technology to monitor the use of devices that generate heat in the home:

> [I]n the case of the search of the interior of homes–the prototypical and hence most commonly litigated area of protected privacy–there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.[6]

The Court found that even the most minute details of a home are intimate: "[i]n the home, our cases show, all details are intimate details, because the entire area is held safe from prying

---

[3] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
[4] *See generally* EPIC, Public Opinion on Privacy, http://epic.org/privacy/survey (last visited June 29, 2010).
[5] 533 U.S. 27 (2001).
[6] *Id.* at 34.

serial number and the electronic information associated with the meter address, this information is PII.

Smart meters will increase the frequency of communication from the home to the utility service provider or the third party application user. Traditional meter reading takes place once a month, by a visit from a person affiliated with the electricity service provider or billing company. In contrast, proposals for smart meters discuss "real-time" reporting of usage data.[15] Currently, the design specification is not for electricity consumption information to remain in the home or meter location, which could only be accessed easily by the utility user. Rather, the plan, as suggested in the Cyber Security Strategy, is to instead share the information with the utility company or others. If, as the document suggests, the information will allow customers to make better energy consumption decisions, then only the customer should have access to that information. This is one of many instances in which the design of a Smart Grid application can either favor privacy or ignore it.

Another architectural point which raises privacy implications is the use of wireless communications to transmit Smart Grid data.[16] The Draft Framework proposed to assess "the capabilities and weaknesses of specific wireless technologies."[17] Although it mentions security as a characteristic of wireless technology that may be relevant to that assessment, privacy is not mentioned. Any wireless technology that would be used to transmit user data must protect personal privacy. Wireless sensors and networks are susceptible to security breaches unless properly secured,[18] and breaches of wireless technology could expose users' personal data.[19] Similarly, the potential transmission of Smart Grid data through "broadband over power line" (BPL) implicates users' privacy:

> A BPL node could communicate with any device plugged into an electrical socket. Capture of a substation node would provide control over messages going to smart appliances or computing systems in homes and offices. A utility may also offer customers BPL as a separate revenue stream. This creates risks that [advanced meter] data could be read or modified over the internet or that common internet attacks could be brought against the electrical grid or individual customers.[20]

---

[15] *See, e.g.*, Draft Framework, *supra* note 11, at 56.
[16] *See* Draft Framework, *supra* note 11, at 65.
[17] *Id.*
[18] *See, e.g.*, Mark F. Foley, Data Privacy and Security Issues for Advanced Metering Systems (Part 2), http://www.smartgridnews.com/artman/publish/industry/Data_Privacy_and_Security_Issues_for_Advanced_Metering_Systems_Part_2.html ("Wireless sensor networks, for example, are subject to the general security problems of computer networks, ordinary wireless networks, and ad-hoc networks).
[19] *See id.* (breaches could "result in denial of service to customers or utilities (e.g., access to billing information or energy usage), payment avoidance, system overload, reduced quality of service, and violation of power control protocols").
[20] *Id.*

Moreover, wireless communication is especially problematic in light of how easily signals from wireless devices are detectable by bad actors to pick-up valuable information on systems using wireless technology, and the past exploitation of wireless systems by thieves who use techniques known as "wardriving" to seek out unprotected or insufficiently protected wireless communication portals.[21]

Wireless communications to transmitting Smart Grid data would not only provide a significant challenge to privacy of users, but may also pose economic and security threats. Identity theft, third party monitoring of utility use, home invasions, domestic abuse and predatory use of home electricity consumption information strips home owners of the protection from prying eyes provided by the walls of their home.

A final architectural problem with the proposed Smart Grid is the interaction between the Smart Grid and plug-in electric vehicles (PEV). It is possible that the Smart Grid would permit utility companies to use PEVs and other sources of stored energy "as a grid-integrated operational asset,"[22] *i.e.*, to drain the energy stored in the PEVs when the energy is needed to supply other users. This application of the Smart Grid is particularly troubling. If privacy is, as the Supreme Court has said, the "interest in independence in making certain kinds of important decisions,"[23] then this proposed application could severely damages both privacy interests and consumer rights.

C. PRIVACY THREATS

In addition to the architectural weaknesses of the proposed Smart Grid, the application and use of the Smart Grid threatens privacy interests in many other ways.

i. MISUSE OF DATA

The massive amounts of data produced by the Smart Grid can potentially be misused by a number of parties—the power utilities themselves, authorized third parties such as marketing firms, or unauthorized third-parties such as identity thieves.

ii. POWER UTILITIES

Power utilities themselves will likely be interested in conducting complex data mining analysis of Smart Grid data in order to make power distribution decisions. For instance, at the Tennessee Valley Authority (TVA), administrators estimate that they will have 40 terabytes of data by the end of 2010, and that 5 years of data will amount to roughly half a petabyte.[24] The

---

[21] *See, e.g.*, Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 VA. J.L. & TECH. 7 (2004).
[22] Draft Framework, *supra* note 11, at 67.
[23] *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977).
[24] Josh Patterson, Cloudera, *The Smart Grid and Big Data: Hadoop at the Tennessee Valley Authority (TVA)*, June 2, 2009, http://www.cloudera.com/blog/2009/06/02/smart-grid-big-data-hadoop-tennessee-valley-authority-tva.

TVA administrators are actively working to improve their ability to analyze the data, including through "complex data mining techniques."[25] Moreover, the TVA has explored using cloud computing resources to analyze and data mine the data, which raises a separate set of privacy concerns.[26]

iii. DATA MINING AND AUTHORIZED THIRD-PARTIES

Data mining of sensitive personal information raises serious privacy concerns.[27] For example, Total Information Awareness (TIA), developed by the Defense Advanced Research Projects Agency (DARPA), proposed to data mine wide swaths of information in order to detect terrorists.[28] However, privacy concerns led the Congress to eliminate funding for the project, and the Technology and Privacy Advisory Committee of the Department of Defense issued a report recommending that Congress pass laws to protect civil liberties when the government sifts through computer databases containing personal information.[29] The datamining of sensitive personal information transmitted through the Smart Grid raises similar privacy concerns.

Authorized third-parties may also be interested in using data collected through the Smart Grid. The real-time data streaming capabilities of the Smart Grid, in particular, implicate a separate group of privacy risks. Just as appliance manufacturers and insurance companies may want access to appliance usage data, marketing and advertising firms may want access to the data—particularly real-time data—in order to target marketing more precisely.[30] However, power usage data can reveal intimate behavioral information; providing that information to third-party marketing and advertising firms surreptitiously would be a repugnant invasion of privacy.

iv. IDENTITY THEFT AND DATA BREACHES

Further, without privacy standards that protect privacy there will be unauthorized third-parties who will likely also be interested in misusing Smart Grid data, for many of reasons such as identity theft or burglary. Identity theft victimizes millions of people each year.[31] The Federal Trade Commission (FTC) estimated that 8.3 million people discovered that they were victims of identity theft in 2005, with total reported losses exceeding $15 billion.[32] According to the

---

[25] *Id.*
[26] *See* EPIC, Cloud Computing, http://epic.org/privacy/cloudcomputing (last visited June 29, 2010).
[27] *See* EPIC, Terrorism (Total) Information Awareness, http://epic.org/privacy/profiling/tia (discussing government data mining of citizens' personal information) (last visited June 29, 2010).
[28] *See id.*
[29] Department of Defense, *Safeguarding Privacy in the Fight Against Terrorism* (2004), *available at* http://www.epic.org/privacy/profiling/tia/tapac_report.pdf.
[30] *See Privacy and the New Energy Infrastructure*, *supra* note 46, at 46; Rebecca Herold, *SmartGrid Privacy Concerns*, *available at* http://www.privacyguidance.com/files/SmartGridPrivacyConcernsTableHeroldSept_2009.pdf [hereinafter *Privacy Concerns*]; Mark F. Foley, *The Dangers of Meter Data (Part 1)*, *available at* http://www.smartgridnews.com/artman/publish/industry/The_Dangers_of_Meter_Data_Part_1.html [hereinafter "*Dangers (Part 1)*"].
[31] *See generally* EPIC, Identity Theft, http://epic.org/privacy/idtheft (last visited June 29, 2010).
[32] Fed. Trade Comm'n, *2006 Identity Theft Survey Report* 4, 9 (2007) [hereinafter "*FTC Survey Report*"].

Appendix 16

beuc

BEUC DRAFT RESPONSE ON ERGEG PUBLIC CONSULTATION PAPER ON DRAFT GUIDELINES OF GOOD PRACTICE ON REGULATORY ASPECTS OF SMART METERING FOR ELECTRICITY AND GAS

Contact: Monika Stajnarova – energy@beuc.eu
Ref.: X/065/2010 - 10/09/10

www.beuc.eu

1. Key recommendations to improve the consumer experience of smart meters

1. Member State's cost benefit analysis and impact assessment should be transparent and take into consideration the distributional impact of smart metering on different social groups especially low income and vulnerable groups. This impact assessment and cost benefit analysis should form the basis of any smart metering strategy to ensure that all consumers are able to access, as a minimum, the stated benefits of smart metering.

2. A strategy for the realisation of the consumer benefits should be developed, especially to ensure the delivery of those benefits identified in the cost benefit impact assessment where the case for smart metering is deemed positive. This is particularly important where consumers are paying for roll out.

   This should include measures to ensure that smart metering delivers social, financial and environmental benefits to customers. For example it could include:

   - a national communications and social marketing strategy to help consumers engage with smart metering and change behaviour;
   - all consumers offered a free display which shows their real time consumption information to better understand their energy use and have access to consumption data via a media of their choice (phone, hard copy, mobile phone, TV, standalone display);
   - consumers should be informed about fire hazards linked to the use of appliances overnight, such as to be able to take appropriate measures;
   - the delivery of extra help to certain vulnerable customers – this is particularly important when it is unclear if low income groups will get the same benefits from smart metering;
   - the linking up with wider government policies and regulations in other sectors in relation to the environment, health and tackling poverty. Linking up with synergies around water metering and other utilities is also important.

3. The effectiveness of a delivery strategy should be reviewed and mapped against the projections of the cost benefit analysis and impact assessment on a regular basis.

4. Member States should systematically review the protection of consumers in place to ensure that they are fit for purpose in the smart world. This includes remote disconnection and switching, sales and marketing practices, data protection and privacy including guarantees of protection of personal data stored in the meter and new tariffs including time of use deals.

5. Member States should outline a timetable for a review of protection to ensure that safeguards are in place ahead of the roll-out of new technologies.

6. Member States must have a strategy in place to protect low income and vulnerable consumers. For example recognising that many low income households may not be able to take advantage of cheaper priced tariffs if they

are unable to shift their activities and could be adversely impacted by critical peak pricing. Steps must be taken to ensure that consumers do not get concerned about real time feedback on their energy consumption or energy prices and reduce their consumption to a level that is dangerous to their health.

7. Consumer protection rules must be easily updatable and allow for timely upgrading to protect consumers from any fast moving innovation and technological change which could lead to consumer detriment.

8. Transparent mechanisms must be set up to ensure that if costs of smart meter roll-out are passed on to consumers that they are fair and proportionate but also that cost savings are passed on to customers. Consumers should not be expected to pay for inefficient costs but smart meter roll-out must be demonstrably value for money. Measures must be introduced to ensure that the roll-out of smart metering does not increase the hardship of those already struggling to afford their energy bills. Furthermore, consumers should receive clear information about the costs they will be charged for the installation and maintenance of all devices. Industry must be accountable for spending.

9. Mechanisms must be put in place to monitor the quality of roll-out and the customer experience.

10. Campaigns to raise awareness of good practices across Europe would be beneficial to all stakeholders.

11. Guarantees are required for the technical reliability for devices deployed.

2. Proposed amendments to the draft Guidance Paper and to ERGEG's Recommendations

Section 1.1 Background and Scope
On page 11, the reference to consumer empowerment should acknowledge the need for regulators to have a strategy to help consumers engage in the new smart energy market and realise the potential benefits.

Section 1.2 Problem identification
On page 12, the cost benefit analysis should be expanded as described in our recommendations above (distributional impact of smart metering on different social groups especially low income and vulnerable groups). Additionally, clarification is needed as to what is *"active participation"* in the market and what barriers are believed to exist at present with respect to real-time pricing.

Section 1.3 General Provisions and Objective
On page 13, a number of regulatory aspects are excluded from this report on the basis of that they are best dealt with at a national sovereignty. Yet, this document is not a legislative – but a best practice document. The guidelines are weakened by the lack of best practice examples including financing, transparency, sales and marketing and monitoring.

Recommendation 4: Offers reflecting actual consumption patterns

- We have strong reservations about Recommendation 4. No consideration has been given to the detriment that can be caused to consumers and there appears to be a dogged belief that time of use tariffs or critical peak pricing will benefit consumers despite international concerns to the contrary (e.g. US and Australia):

  - Consumers must have a choice in whether or not they have time of use tariffs;
  - Suppliers should not be allowed to put a customer on to a time-of-use tariff without evidence (historic consumption data over a number of seasons) that they would be better off on that tariff;
  - There should be no heavy bias towards time-of-use tariffs;
  - Consideration must be given to the impact on low income and vulnerable consumers;
  - Protections should be developed to ward against bill shocks from new tariffs;
  - Additionally, the reference to frequency of readings should be audited against privacy rules.

Question to stakeholders: When interval metering is applied, which interval should be used for customers and those that both generate and consume electricity? Please specify timeframes and explain.

- BEUC believes that consumers should be provided with more frequent information. Since the high consumption intervals are concentrated over short period, we consider the interval of 30 minutes as acceptable.

- A cross-reference between recommendation 4 and section 8 is required in order to ensure that the legal, privacy implications of this recommendation are picked up.

Recommendation 6: Activation and de-activation of supply

- BEUC believes that protections will need to be put in place to protect consumers from misuse of remote disconnection of supply. This is particularly important to protect vulnerable consumers. Similarly clear safeguards will need to be put in place around remote management of appliances within consumers' homes by suppliers. Particular attention will need to be paid to consumer information, safety, and redress and complaint handling if and when things go wrong. BEUC wants to point out that in any case, the decision whether to participate in remote management or not should be with the consumers since they always have to have the possibility of opt out.

Recommendation 8: Access on customer demand to information on consumption data

- BEUC supports the idea of providing consumers with their consumption data through different ways. At the same time, we would like to stress that this service should be free of charge. A fee for access to consumption data is unacceptable and will negatively impact the functioning of competitive markets and consumers' ability to switch to the best deal for them: data should be provided free of charge in a format that allows comparisons with other tariffs available in the market on a like for like basis - see also comments on recommendation 2 above. It is vital that consumers should be able to access historical information in a timely way.

- The cost benefit analysis should be rigorous and done in a transparent way and the results should be published. Although smart meters have the potential to provide benefits to all parties: network operators, suppliers, consumers, and Government most of the direct benefits are realized by industry. They should thus bear the bulk of the cost. Where the consumer is expected to pay for smart metering, transparent metrics must be developed to ensure that there is a fair and equitable cost-sharing mechanism. Mechanisms need to be put in place to ensure accountability for customer's money and to make sure that cost savings are also passed on to customers. Moreover, the cost benefit analysis should be reviewed regularly and the roll-out strategy adjusted accordingly. Most cost-benefit analyses are based on *theoretical projections. Therefore, the national regulators should evaluate whether* national roll-out objectives in terms of cost-benefit analysis have been met and act accordingly;
- We welcome the recognition that services should be provided in an obvious and easy way that benefits consumers. Best practice should ensure that countries monitor the impact of roll-out (i.e. the financial impact on consumers, the quality of service, and the consumer experience). The extent to which the cost benefit analysis is accurate should be reviewed regularly and the roll out strategy adjusted accordingly; benefits delivered to consumers should be reported in an annual statement.
- We question the list of "Potential benefits for customer" (page 28) specified under this recommendation. If this list is maintained, the rational for how this benefits consumers (as opposed to other stakeholders) should be clarified in each case. Potential consumer benefits missing from the list include social and environmental objectives.
- Recognition should be given to the fact that without regulation there will be losers as well as winners from the smart meter roll out and the resulting changes to the *energy retail market, with many low income and vulnerable consumers potentially* worse off.

In Section 4: Roll-Out – electricity:

Vulnerable consumers should not be prioritised in the smart meter unless it is clear they will reap the benefits. The consultation paper has not yet made a case for this. As with the introduction of any new programme there are likely to be teething problems. It would be wrong to create a situation where some of the most vulnerable customers who may be least able to cope with problems are effectively regarded as test cases. This could also have knock on effects for the wider popularity of smart metering. If costs are passed on at the point of installation, this could result in some of the poorest paying the highest prices for their technology as prices will decline in time. Technology is also likely to evolve quickly. If vulnerable customers are targeted for early roll out, they are likely to receive the least advanced technology yet arguably be in the weakest financial position to upgrade their technology in the future. Priority should be given to community roll out, to maximise customer engagement.

Recommendation 15: All customers should benefit from smart metering

- This recommendation should emphasise that all consumers who wish to use smart meters should have *"equal access"* to the benefits.

Recommendation 20: Offers reflecting actual consumption patterns

According to BEUC, this recommendation is focused more on the electrical model and could result in penalizing customers. Consumers can certainly pay attention when

Appendix 17

BEFORE THE PENNSYLVANIA HOUSE CONSUMER AFFAIRS COMMITTEE

Testimony of

SONNY POPOWSKY
CONSUMER ADVOCATE

Regarding

Smart Meters
House Bills 2186 and 2188

Harrisburg, Pennsylvania
May 8, 2012

Office of Consumer Advocate
555 Walnut Street
Forum Place, 5th Floor
Harrisburg, PA 17101-1923
(717) 783-5048 - Office
(717) 783-7152 - Fax
Email: spopowsky@paoca.org
155774

their homes and businesses, but importantly the General Assembly gave the utilities up to 15 years to complete that deployment. At the same time, the General Assembly authorized the companies to request automatic rate surcharges to begin to recover the costs of their smart meter deployment programs as they were incurred.

The federal government has also promoted the deployment of smart meters and other smart grid technology through substantial grants to utilities under the federal stimulus legislation, the American Recovery and Reinvestment Act of 2009 (ARRA). One Pennsylvania utility – PECO – received a $200 million grant, the maximum approved under ARRA, to accelerate the deployment of smart meters throughout its service territory. Several other Pennsylvania utilities received ARRA grants for smart grid projects in lesser amounts.

In part as a result of the $200 million ARRA grant, PECO has developed the most ambitious schedule to join PPL in completing the installation of truly advanced meters throughout its service territory. The other major Pennsylvania utilities – Duquesne and the four FirstEnergy companies (Met-Ed, Penelec, West Penn, and Penn Power) -- have adopted a less aggressive timeframe to meet the statutorily mandated deadlines of Act 129. All of the utilities, however, have requested and received the right to begin collecting costs through a surcharge on customer bills as those costs are incurred.

As the introduction of the legislation that is the subject of this hearing exemplifies, the implementation of the smart meter mandates of Act 129 has not been without controversy. My Office has received a number of questions and complaints from consumers regarding the smart meter surcharges that have begun to appear on customers' bills and the need for and cost of these new meters. I spoke with one PECO customer just recently who informed me in no uncertain terms that she did not ask for a new meter; that she did not need a new meter; and that she

certainly did not want to pay for a new meter in her home. Indeed, in several states that have begun to implement this new technology across the Nation, there have been objections raised by a growing number of consumers regarding not just the cost of the new meters, but also their impacts on the privacy of customer information as well as health concerns arising from their operation.

House Bill 2188, as originally introduced, would attempt to address some of these concerns by allowing individual customers to "opt out" of receiving smart meter technology on the mandatory schedule established by Act 129. While I certainly understand and appreciate the sponsors' desire to address their constituents' concerns on this issue, my own concern with the opt-out approach is that the costs involved in allowing individual customers to reject these meters may be much greater than the costs of installing and operating them on a uniform basis. That is, once a utility commits to the deployment of advanced metering technology in a geographical area or throughout its service territory, then it is far more economical to serve all customers in that area through this technology, rather than serving all but one or a few such customers. The most obvious example of that result is meter reading. If a company can read the meters of 100 neighboring customers instantaneously through an electronic signal, but then has to send out an employee to read the meter of one customer in that neighborhood, then the cost to the utility of reading that one meter would be substantial. The question then is who should pay those additional costs, the one customer who opted out of receiving a smart meter or the remaining customers who have permitted the installation of the meters in their homes?

This issue has come up in a number of other states and, to my knowledge, each of the states that has allowed customers to opt out of receiving a new meter has required the individual opt-out customers to pay substantial up-front and monthly fees — over and above their normal

monthly bills – to cover at least a portion of those additional costs. The alternative, as I said, is to charge those costs to other customers. This would be particularly true in Pennsylvania, where it is clear under Act 129 that utilities have a right to recover their incremental smart meter costs from ratepayers.

I would note in this regard that an amended version of HB 2188 that was provided to the witnesses at today's hearing by the Committee Staff would change this dynamic by allowing the utilities themselves to refrain from implementing the metering requirements of Act 129. That is, the mandatory deployment requirement imposed on the utilities under the Act would become voluntary. If a utility chooses not to deploy smart meters throughout its service territory, individual customers might have no need to opt out of accepting such a meter in their own home. Here, I think the question is one of both timing and costs. The fact is that each of our major electric utilities already has filed a meter deployment plan that has been approved by the Public Utility Commission, and each utility already has taken steps to varying degrees to implement those plans. As I mentioned earlier, some of our utilities are further along in those plans than others, but to the extent that those utilities already have incurred significant costs to implement their plans, my concern is that some of these costs might become "stranded" investments. That is, some of the costs already incurred might not serve a useful purpose to consumers but would nevertheless be charged to those customers because they were incurred under plans that were approved by the Commission under the prior statutory mandate.

Finally, turning to HB 2186, I believe that this Bill is intended to ensure that government agencies are not permitted to obtain data from customer meters without customer consent. I have no objection to this provision, although it is possible that government agencies are already covered by the language of Act 129 that prohibits release of such data without customer consent

Appendix 18

Hearing by the Pennsylvania House Consumer Affairs Committee
Regarding House Bill 2186 and House Bill 2188

May 8, 2012

Testimony of
Chairman Robert F. Powelson
Pennsylvania Public Utility Commission

programs jeopardize the overall functionality of the AMI system. Opt-out programs limit all customers' ability to have an advanced meter and participate in the programs and benefits it provides end users. The full deployment of AMI has the potential to help attain and even exceed the energy efficiency goals outlined in Act 129.

If exceptions are made, customers opting out should (as California, Maine, and Oregon provide) incur a significant monthly fee for someone to read their meter. This is necessary because much of the costs for the AMI system such as the back office computer systems are incurred whether one customer has an advanced meter. Permitting electric distribution companies to opt out completely should not be allowed. It would be contrary to the energy efficiency and conservation objectives put in place by Act 129 and likely lead to some customer backlash.

Advanced meter opponents have argued for an opt out program for many reasons, including perceived health, safety, privacy and security issues. However, many EDCs and their customers have had AMIs in place for years namely PPL and PECO. Numerous public health officials also point out that advanced meters emit less radiation than cell phones – and advanced meters are not used right next to the head. The Federal Communications Commission approved the use of smart meters by utilities and said their risk was minimal. Environmental health experts also say the advanced meters do not pose a serious health risk.

As for reliability, utilities are continuing their efforts to improve grid reliability and promote energy efficiency while providing improved services to customers. On meter accuracy, while there are technological differences between advanced meters and older mechanical metering devices, the electric industry will point out that it exercises the same due diligence and precision for ensuring the accuracy of advanced meters as it does for older mechanical metering devices for revenue billing application. All meters, regardless of technology and design, are required to meet national standards for meter accuracy and operation before being installed.

The proliferation of opt-out requirements for advanced meter deployment has the potential to cripple efforts to modernize grid technology. Regardless of the validity of opponents' concerns about health, safety and privacy, some utilities in other states have begun considering and implementing AMI opt-out programs in an effort to diffuse opposition and allow utility companies to move forward with grid modernization plans. Regardless of where they stand in the transition to AMI technology, the industry generally prefers a uniform system of managing customer data, and fears a return to the days of manual meter readings, which would be needed for those customers who opt-out of wireless meters.

In Maine, which has received a lot of attention regarding its AMI opt-out, Central Maine Power (CMP) has considered, analyzed and provided substantial cost information relating to a variety of potential solutions or mitigation measures for customers seeking to opt out of CMP's Smart Meter Program. According to CMP's website, there are two options: (1) choosing a digital advanced meter with the wireless transmitter turned off for an initial charge of $20, plus a monthly charge of $10.50; (2) keeping an existing

exacerbates this problem. Our integrated, interconnected electric system in Pennsylvania could have large operational gaps and expansive pockets of weakness. Such a system reduces reliability for all customers as well as the benefits of a completely modernized electric grid. Simply put, there is no compelling reason for an "opt-out" program.

HB 2186

HB 2186 would require customer consent prior to an EDC making customer meter data available to government agencies. Under Act 129, EDCs are required to make electronic access to meter data available to third parties, upon customer consent. The Commission is addressing this issue and has issued a tentative order. Comments are currently being reviewed.

We do not believe that HB 2186 is necessary as the Act already specifies that:

> Electric distribution companies shall, **with customer consent** (emphasis added), make available direct meter access and electronic access to customer meter data to third parties, including electric generation suppliers and providers of conservation and load management services. 66 Pa. C.S. § 2807(f)(3).

Under section 2807 (f)(3), it is our belief that government agencies qualify as third parties and because of that, customer consent already is required before any information can be released. It is important to know that programs such as the federal "Green Button" initiative, which standardizes the presentation of electric usage data for customers and allows customers to download their own detailed energy usage information with a simple click of a button, provides information to customers only. It is not a mechanism to release customer data to the federal government or other entities.

Conclusion

Across the nation, states and utilities have made tremendous progress with the smart grid deployment plans. In Pennsylvania alone, hundreds of millions of dollars and countless hours of manpower are being dedicated to the rollout of smart meters. I can assure this committee that our regulated electric utilities have carefully considered many factors, including technology and costs before adopting metering plan rollouts. In summary:

1. AMI technology eliminates meter reading costs, detects outages more quickly, reduces billing disputes, helps to prevent theft of services and fosters greater innovation in the offering of new products.

2. Consumers will be able to see real-time usage, and electricity providers will be able to offer a variety of rate designs to meet the current and future needs of consumers.

Appendix 19

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

FILED
2010 MAY 25 P 4: 21
U.S. DISTRICT COURT
N.D. OF ALABAMA

UNITED STATES OF AMERICA *ex rel.* DON BAKER,	)	
Plaintiff,	)	
v.	)	Case No: CV-10-CO-1337-S
SENSUS USA, INC., SENSUS METERING SYSTEMS, INC., THE SOUTHERN COMPANY, and ALABAMA POWER COMPANY,	)	**FILED UNDER SEAL**
	)	**DO NOT PLACE IN PRESS BOX**
	)	**DO NOT ENTER ON PACER**
Defendants.	)	**DEMAND FOR JURY**

***QUI TAM* COMPLAINT**

Plaintiff-Relator Don Baker, on behalf of himself and the United States of America, alleges and claims against Defendants Sensus USA, Inc. and Sensus Metering Systems, Inc., doing business as Sensus ("Sensus"); The Southern Company ("Southern Company"); and Alabama Power Company ("Alabama Power"); as follows:

JURISDICTION AND VENUE

1. This action arises under the False Claims Act, 31 U.S.C. §§ 3729-33 (the "False Claims Act"). Accordingly, this Court has jurisdiction pursuant to 28 U.S.C. § 1331. Jurisdiction is also authorized under 31 U.S.C. § 3732(a).

2. Venue lies in this judicial district pursuant to 31 U.S.C. § 3732(a), because Defendants qualify to do business in the State of Alabama, transact substantial business in the State of Alabama, transact substantial business in this judicial district, and can be found here. Furthermore, Defendants committed within this judicial district acts proscribed by 31 U.S.C. § 3729, to-wit: Defendants submitted, caused to be submitted, and conspired to submit to the United States' false claims for payment of funds under the American Reinvestment and Recovery Act of 2009 ("ARRA") for a project that Defendants new was hopelessly flawed and did not qualify for stimulus funding, and submitted false records to get such claims paid.

PARTIES

3. The Southern Company is an Atlanta, Georgia-based conglomerate of electricity providers. Through its subsidiaries, including Alabama Power, Southern Company provides electricity to 4.4 million customers across the southeastern United States. In 2007, Southern Company launched an initiative to upgrade its distribution system to include "smart meters" capable of recording and

transmitting information via radio signal, eliminating the necessity for manual meter reading. In or around May, 2009, Southern Company submitted an Application for Financial Assistance through the Department of Energy Smart Grid Investment Grant Program (SGIG). In October, 2009, Southern Company was awarded $165 million in matching funds for its smart grid project. On April 28, 2010, Southern Company signed an agreement with the Department of Energy with regard to the funds.

4. Sensus is a North Carolina-based concern specializing in utility metering technology. A self-described "global leader in utility management," Sensus designs and markets water, gas, and electric metering systems and develops and markets "Automatic Meter Reading" ("AMR") and "Advanced Metering Infrastructure" ("AMI") technologies designed to function in a "smart grid." In December, 2007, Sensus signed a contract with Southern Company to supply "smart meters" for the company's grid upgrade. Sensus had never before supplied the type of meter required by the Southern Company and Alabama Power and – based on their specifications – designed a new meter dubbed the "iConA."

5. Plaintiff-Relator Baker is an engineer with over fifteen years experience in project management, programming, and scheduling. In 2008, Mr. Baker was hired by Sensus as Alabama Project Manager for Southern Company's AMI Smart Grid project. Along with coordinating the project logistics, Mr. Baker

helped Sensus supply certain information for inclusion in Southern Company's SGIG grant application. In the course of his duties, and as more fully described herein, Mr. Baker became aware that the Sensus iConA meter was not properly tested and was seriously flawed. Among other issues, Mr. Baker discovered that the iConA had a tendency to drastically overheat and melt or burn. When Mr. Baker raised these issues with Sensus management and Alabama Power project managers, he was told to keep quiet. He was eventually terminated for refusing to do so. Mr. Baker has direct personal knowledge that Sensus and Southern Company have installed approximately one million iConA meters in Alabama homes with knowledge that the meters are seriously defective and pose a substantial fire hazard and that at least two Alabama homes have burned as a result. Mr. Baker also has personal knowledge that at the time Southern Company submitted its grant application to the United States, Sensus and Southern Company were well aware that the iConA was defective and that the entire project was seriously flawed and ineligible for an SGIG grant. On or about February 2, 2010, Mr. Baker disclosed the information underlying this complaint to the Office of the United States Attorney for the Northern District of Alabama and an agent of the Federal Bureau of Investigation. Mr. Baker now files this action as original-source Relator under the *qui tam* provisions of the False Claims Act. Plaintiff-Relator is

Appendix 20

October 10, 2012

Peco Ditches Sensus Smart Meters, Resumes Installation in PA

Peco Energy has said it will resume its Philadelphia-area smart-meter installation project, which the company suspended in August after several incidents in which the electronic devices overheated and caught fire.

The utility company is, however, ditching meter manufacturer Sensus, whose devices were linked to two serious house fires in which no one was hurt. Peco says it will resume its meter installation work with Landis+Gyr (L+G) meters, and replace the 96,000 previously installed meters with L+G meters during the next 45 days.

Read more at Energy Manager Today.

Energy Manager News

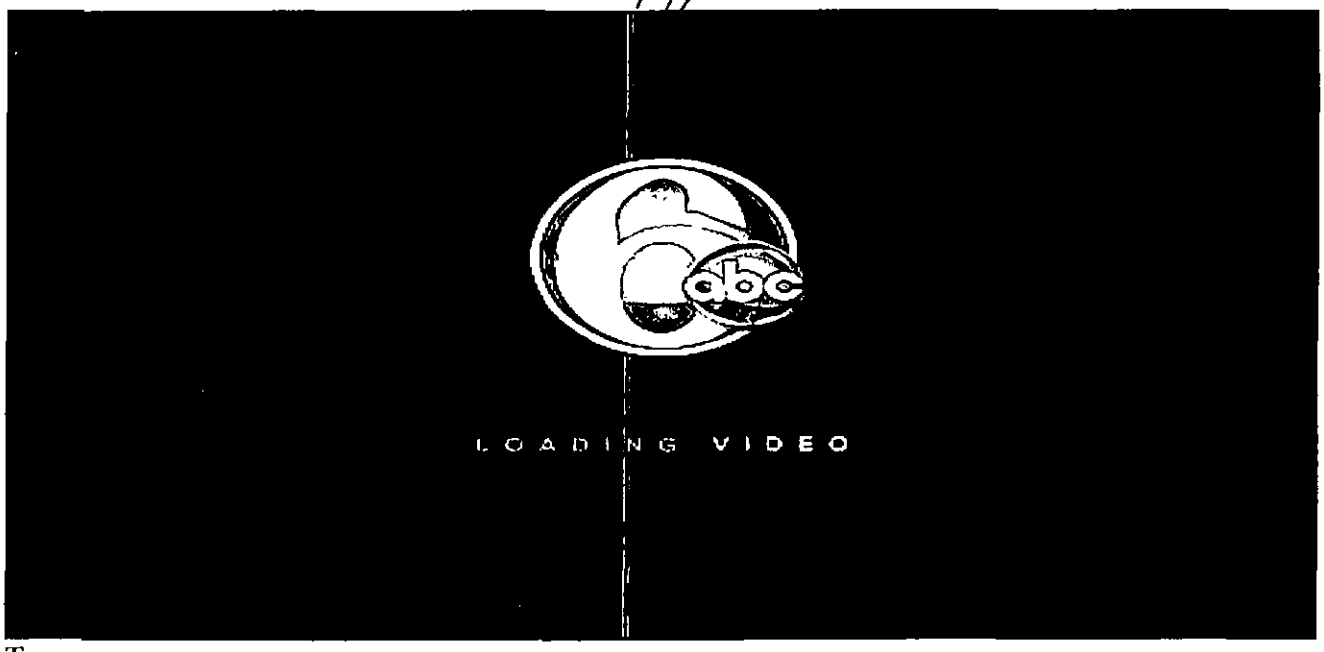
- New York Reviewing Higher Energy Costs
- Solar Panel Install Time Lapse
- Cofely District Energy Awarded Coventry Contract; UK Must Massively Increase District Heat, Report Says
- NJ Program Gives Business a Break on Energy-Efficiency Projects
- *Panasonic to Install PVs Atop 12 Macerich Shopping Malls*
- Buildings Using Energy Star Portfolio Manager Realized Total Savings of 7%
- U. of Arizona Aims to Cut Energy Bill 5-10% Using Online Dashboard
- Bridgeport Hospital Expects 'Lifetime Energy Savings of $5.15m'

Environmental Jobs

View All Jobs >> Post a Job >>

© 2006-2012 Environmental Leader LLC. All rights reserved.

Appendix 21



Tags:
pennsylvania, bucks county, PECO, fire, local/state, john rawlins

- Comment Now
- Email
- Print
- Report a typo
-
-
-
-
-
-

John Rawlins
More: Bio, News Team
Action News

UPPER MAKEFIELD TWP., Pa. - August 16, 2012 (WPVI)-- They're called smart meters, but PECO has acknowledged that they're causing problems.

Workers repaired fire damage to a Bucks County house cause by a newly installed PECO smart meter Thursday afternoon.

This latest incident has prompted PECO to take the unusual step of suspending its big push to install a new generation of government mandated meters.

Related Content

More: Sendit.6abc.com
More: Send a Breaking News alert

Menendez says PECO plans to examine data from the already installed units which go by the name of Sensus meters.

"With that data we will take some of those meters and replace them with another brand of meter. We want to see if there is any difference in performance," Menendez said.

In addition, the remaining Sensus meters will get software upgrades to shut down should they get hot enough to start a fire.

While the problem is indeed real, it has been very rare.

"We have installed 186,000 meters. We've had 15 cases where meters have overheated," Menendez said.

Former meter installer Scott Cummings welcomed the moratorium, saying his team had noticed problems with electrical arcing of smart meters.

"It was causing some fires," Cummings said.

Smart meters are part of the nationwide effort to make the power grid more efficient. Using two way wireless transmissions, utilities say that can help restore blackouts faster.

However, anti smart meter websites blast that wireless technology claiming it can cause health problems.

Critics have posted videos of customers chasing off installers and what's described as a smart meter fire.

If you have one of the 186,000 already installed Sensus meters and have concern it is overheating, PECO has set up this hotline **1-855-741-9011**.

(Copyright ©2012 WPVI-TV/DT. All Rights Reserved.)

Get more Local/State »

Tags:
pennsylvania, bucks county, PECO, fire, local/state, john rawlins

- Comment Now
- Email
- Print
- Report a typo
-
-
-
-
-
-

Recommend Send 85 people recommend this. Sign Up to see what your friends recommend.

Recently Published

Search continues for Autumn Pasquale

Appendix 22

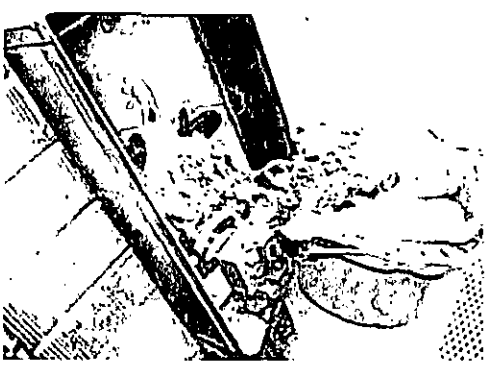
EMF Safety Network

Environmental protections, education and science based precaution for EMF and RF technologies: smart meters, cell phones, cordless phones, cell towers, ice-[illegible] electricity, power lines.

Smart Meter Fires and Explosions

The following is a compilation of reports from the US , Australia and Canada about fires, explosions appliances due to Smart Meter installations. *If you have experienced similar problems, please post* the comment section below.

GEORGIA Family reports smart meter fire. In the photo the holds the charred remains of a smart meter which exploded fire on her home, causing $11,000 worth of damage. Accordi report Georgia installed the same type of meters-Sensus- tha sparked fires in other states. (See video available here)



Smart Meter Causes Dumb Fire

"In June 2010, Shirley Bayliff was sitting at the piano in her Illinois home, giving music lessons to a student, when she he outside the house before the power went out. When she and looked out the window, they saw five-foot flames shooting ou **General Electric** smart meter their utility company had in of a pilot project."..."Since then, two more of the 130,000 sm Commonwealth Edison installed in the area have burst into flames, one in 2011 and one this last Jul to the newspaper.

Three states utility regulators investigating Smart Meter fires

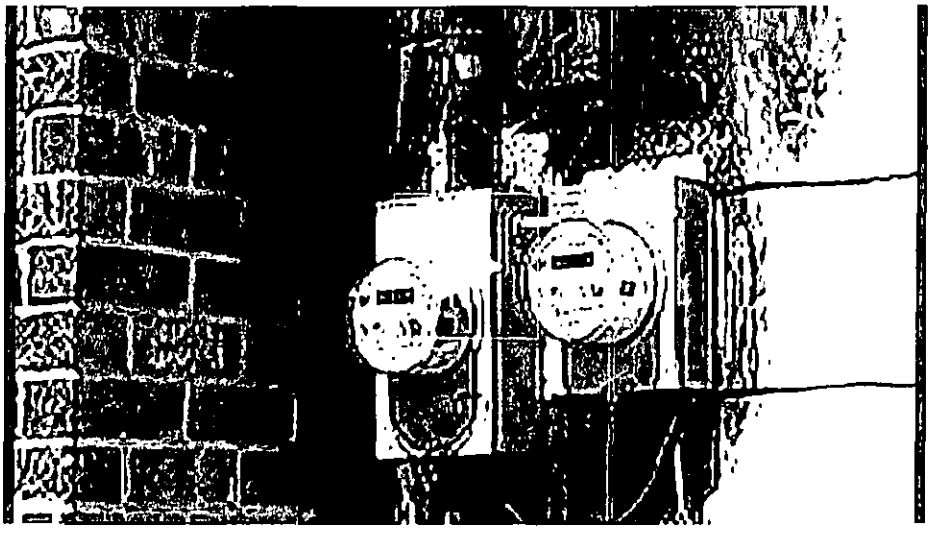
"The Pennsylvania Utilities Commission wants more information about PECO Energy's handling of meter program, including failure rates of its meters, the number of overheating incidents and how n overheating incidents resulted in damage.

...Regulators in other states, including Illinois and Maryland, are investigating allegations of danger overheating electric smart meters and reports of meter fires."

9/7/2012

Home Scorched by PECO "Smart Meter:" Fire Officials

PECO confirms to NBC10 that there have been 26 incidents of smart meters overheating



8/30/2012 Chicago Utility Company admits to Smart Meter related fires

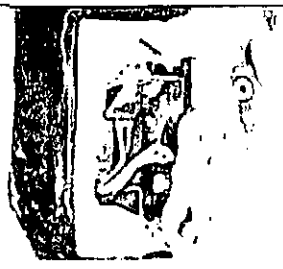
The Chicgo Tribune reports, *"Commonwealth Edison (ComEd) confirmed on Thursday that three o meters, which wirelessly relay power-use data between homes and the company, have been involv fires" in the Chicago region."*

Recently Maryland utility regulators held a hearing with four major electricity companies about sma Baltimore Gas and Electric Co. was reported to admit their company experienced five incidents of th meters overheating.

According to the Tribune, ComEd replaced 15 heat damaged Smart Meters, and is sending its meter independent evaluation, before it deploys more meters next year.

8/25/2012 Woman wants electric company to replace TV (Texas) " Long blames the installation of a at her house for shorting out her flat screen and causing her microwave to act up. She also said her r broadcasts more static than music. "I left the house (to run some errands) and when I came back, nc working," ...It appears an electrical surge fried the TV set and might be responsible for putting the n the fritz. At least, that's what Long said her electrician told her."

8/23/2012 Houston Smart Meter Fire " A southwest Houston woman is blaming a smart meter for a fire that left her home in shambles in July... Harwood provided KHOU 11 news with a document that appears to be from the Houston Fire Department. The letter states "an unspecified electrical malfunction in the electrical meter" caused the fire...." (article includes a video)



Home owner blames smart meter installation for destructive TV BC News)

..."The family says the electrical fire shorted out no fewer tha appliances, and a number of electrical outlets..."I got a panic mom saying that there was a fire in the house. So I ran over a lots of black smoke. Luckily I could put out the fire out fast w extinguisher."...The daughter, who did not want to be identified, says the fire follows the smart mete by BC Hydro, and the damage is far worse than just the microwave..."Really anything you can name house. All the air conditioning is gone, the phone inside the house is gone, the TV boxes, all the elect are gone."... (article includes a video)

Philadelphia Utility Company Halts smart meter installation due to fire risk

Appendix 23

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

NAPERVILLE SMART METER AWARENESS, an Illinois not-for-profit corporation,	)	
Plaintiff,	)	Case No. 11-cv-9299
v.	)	
CITY OF NAPERVILLE,	)	
Defendant.	)	

COMPLAINT FOR INJUNCTIVE RELIEF

The Plaintiff, NAPERVILLE SMART METER AWARENESS ("NSMA" or "Plaintiff"), by its attorney of record, files this Complaint against the CITY OF NAPERVILLE (the "City" or "Defendant").

I. NATURE OF THE ACTION

1. The Defendant is rushing forward with the installation of so-called "smart" meter devices throughout the municipality of Naperville, Illinois despite a multitude of serious health, safety, security, and privacy concerns – some of which involve apparent constitutional and statutory violations.

2. The Plaintiff seeks a judgment requiring the Defendant to cease all smart meter installations until reasonable safeguards are in place and until satisfactory alternative options for all customers are made available.

Appendix 24

MAINE SUPREME JUDICIAL COURT
Decision: 2012 ME 90
Docket: PUC-11-532
Argued: May 10, 2012
Decided: July 12, 2012

Reporter of Decisions

Panel: SAUFLEY, C.J., and LEVY, SILVER, MEAD, GORMAN, and JABAR, JJ.

ED FRIEDMAN et al.

v.

PUBLIC UTILITIES COMMISSION et al.

LEVY, J.

[¶1] Ed Friedman and others (collectively, Friedman) appeal from the Maine Public Utilities Commission's dismissal of their complaint against Central Maine Power Company (CMP) regarding CMP's use of smart-meter technology. Friedman also appeals the Commission's dismissal of those portions of the complaint that were directed at the Commission and raised constitutional concerns regarding orders previously issued by the Commission. Friedman asserts, among other issues, that the Commission erred because its dismissal of his complaint ignored the Commission's statutory mandate to ensure the delivery of safe and reasonable utility services. *See* 35-A M.R.S. §§ 101, 103 (2011). The Commission and CMP contend that the complaint was properly dismissed in all respects. Because we agree with Friedman that the Commission should not have

Appendix 24

STATE OF MAINE
SUPREME JUDICIAL COURT
SITTING AS THE LAW COURT

LAW COURT DOCKET NO. PUC-11-532

ED FRIEDMAN, et al.,

Appellants

v.

MAINE PUBLIC UTILITIES COMMISSION

and

CENTRAL MAINE POWER COMPANY

Appellees.

On Appeal from the Maine Public Utilities Commission

BRIEF OF APPELLEE MAINE PUBLIC UTILITIES COMMISSION

Jordan D. McColman (ME Bar No. 004334)
Leslie E. Raber (ME Bar No. 004736)
Mitchell M. Tannenbaum (ME Bar No. 003154)
MAINE PUBLIC UTILITIES COMMISSION
State House Station 18
Augusta, ME 04333-0018
(207) 287-3831
jordan.d.mccolman@maine.gov
leslie.raber@maine.gov
mitchell.tannenbaum@maine.gov

Counsel for Maine Public Utilities Commission

Appendix 24

SUPREME JUDICIAL COURT
SITTING AS THE LAW COURT

Law Docket No. PUC-11-532

ED FRIEDMAN, et al,

Appellants

v.

MAINE PUBLIC UTILITIES COMMISSION

and

CENTRAL MAINE POWER COMPANY

Appellees

ON APPEAL FROM THE MAINE PUBLIC UTILITIES COMMISSION

BRIEF OF APPELLANTS

Bruce A. McGlauflin, Esquire
Petruccelli, Martin & Haddow, LLP
50 Monument Square, PO Box 17555
Portland, Maine 04112-8555
(207) 775-0200
Attorneys for Appellants

REMELY URGENT

Rush To Addressee

E PRESS FIRMLY

Schedule 1
Print pos

PA 18938
OCT 22 '12
1007

U.S. POSTAGE
PAID
NEW HOPE, PA
18938
OCT 22, '12
AMOUNT
$21.30
00060304-03

n/pickup

FXPRESS MA
TAGE RE

EMS

EXPRESS® MAIL

UNITED STATES POSTAL SERVICE

EI194801399US

REMELY URGENT

ORIGIN (POSTAL SERVICE USE ONLY)		
ZIP Code 13135	Day of Delivery ☐ Next ☐ 2nd ☐ 2nd Del. Day	Postage $ 15.00
Date Accepted Mo. 10 Day 22 Year 12	Scheduled Date of Delivery Month 10 Day 22	Return Receipt Fee $ —
Time Accepted 3:00 ☐ AM ☒ PM	Scheduled Time of Delivery ☐ Noon ☐ 3 PM	COD Fee $ — / Insurance Fee $ —
Wt Rate ☐ or Weight 1 lbs. 7 ozs.	Military ☐ 2nd Day ☒ 3rd Day	Total Postage & Fees $ 21.30
	Int'l Alpha Country Code	Acceptance Emp. Initials

FROM: (PLEASE PRINT) PHONE ( )

[illegible]

FOR PICKUP OR TRACKING
Visit www.usps.com
Call 1-800-222-1811

EMS

EXPRESS MAIL
UNITED STATES POSTAL SERVICE®

Addressee Copy
Label 11-B, March 2004

Post Office To Addressee

DELIVERY (POSTAL USE ONLY)		
Delivery Attempt Mo. Day	Time ☐ AM ☐ PM	Employee Signature
Delivery Attempt Mo. Day	Time ☐ AM ☐ PM	Employee Signature
Delivery Date Mo. Day	Time ☐ AM ☐ PM	Employee Signature

CUSTOMER USE ONLY

☐ WAIVER OF SIGNATURE (Domestic Mail Only)
Additional merchandise insurance is void if customer requests waiver of signature.
I wish delivery to be made without obtaining signature of addressee or addressee's agent (if delivery employee judges that article can be left in secure location) and I authorize that delivery employee's signature constitutes valid proof of delivery.

NO DELIVERY ☐ Weekend ☐ Holiday

Mailer Signature

TO: (PLEASE PRINT) PHONE ( )

[illegible]

ZIP + 4 (U.S. ADDRESSES ONLY. DO NOT USE FOR FOREIGN POSTAL CODES.)

+

FOR INTERNATIONAL DESTINATIONS, WRITE COUNTRY NAME BELOW.

RECEIVED
OCT 22 2012
PA PUBLIC UTILITY COMMISSION
SECRETARY'S BUREAU

TO: PUC SECRETARY BUREAU (PUC
Agency: PUC
Floor:
External Carrier: Express Mai

10/23/2012

EI194801399US

CMPC