FILE

THE PUBLIC UTILITY COMMISSION OF OHIO

Gregory Peck 3268 US Highway 52 Felicity, Ohio 45120	)	
Complainant	)	**Motion to Supplement the Record**
vs.	)	Case No. 16-2338-EL-CSS
Duke Energy Ohio, Inc.	)	
Respondent	)	

Motion to Supplement the Record

Now comes Gregory Peck as an Ohio Citizen pursuant to Article IV, §2 ,of the 1791 Constitution, to supplement the record based on further research concerning privacy issues as they are related to Duke Energy Ohio's smart meters. Claimant believes a smart meter has the capability now and in the future to invade his privacy. Claimant believes Duke Energy Ohio, Inc. should have strict limitations placed on the installation of smart meters unless it has permission of the home dweller to use in ways beyond a standard monthly meter read.

Duke Energy Ohio, Inc. claims it is using the National Institute of Standards and Technology, NIST, as the standard for its cybersecurity of smart meters it installs on homes throughout Ohio. The information contained within this supplement is evidence that the granular use of smart meters is an invasion of privacy per §14 of the 1851 Constitution of Ohio. The Claimant has raised concerns over an invasion of privacy whereby Duke Energy Ohio has the ability to enter Claimant's home at 15 minute or sub-15 minute intervals to retrieve information of Claimant's behavior patterns. Duke Energy Ohio admits it enters the home in 15 minute intervals to retrieve data on the use of electricity which can be used to identify certain behavioral patterns.

Because installation of smart meters is in its infancy, very few cases have been adjudicated concerning the privacy or other issues. Claimant contends Duke Energy Ohio, Inc. and the Public Utility Commission of Ohio have not given full consideration to how smart meters can be used resulting in an invasion in the privacy of Ohio Citizens.

The following comments from the **NIST Document NISTR 7628 "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid,"**

On page 14 of NIST Document NISTIR 7628, research shows that analyzing 15-minute interval household energy consumption data can by itself pinpoint the use of most major home appliances. As has already been established, it is essential that the amount of data collected by smart meters be limited to the bare minimum necessary to accomplish Utility objectives.

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

"Energy consumption patterns have historically not risen to the level of public concern given to financial or health data because (1) electrical meters had to be physically accessed to obtain usage data directly from buildings, (2) the data showed energy usage over a longer time span such as a month and did not show usage by specific appliance, and (3) the utilities were not sharing this data in the ways that will now be possible with the Smart Grid. Public concerns for the related privacy impacts will likely change with implementation of the Smart Grid, because energy consumption data can reveal personal activities and the use of specific energy using or generating appliances, and because the data may be used or shared in ways that will impact privacy." [emphasis added]

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

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

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

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

There is no justifiable reason for a Utility to collect thousands of data points for incremental energy usage in order to bill each customer for monthly service." [emphasis added]

Essentially, a smart meter has the same attributes as a cell phone whereby data and information can be transmitted and received to determine behavioral patterns of an individual. In a general sense, analysis of granular smart meter energy data results in or may result in:

- Invasion of privacy and intrusion of solitude;
- Near real-time surveillance;
- Behavior profiling;
- Endangering the physical security of life, family, and property;
- Unwanted publicity and embarrassment (e.g., public disclosure of private facts or the publication of facts which place a person in a false light). More specifically, analysis of smart meter data or manipulation of smart meter data/firmware can be used for the following purposes:
- Determine how many people are home and at what times;
- Determine your sleeping routines;
- Determine your eating routines;
- Determine what appliances you use when, e.g., washer, dryer, toaster, furnace, A/C, microwave,

medical devices ... the list is almost endless;

- Determine when a home is vacant (for planning a burglary), who has high-priced appliances, and who has a security system;
- Law enforcement can obtain information to identify suspicious or illegal behavior or later determine whether you were home on the night of the alleged crime;
- Landlords can spy on tenants through an online utility account portal;
- For consumers with plug-in electric vehicles, charging data can be used to identify travel routines and history;
- Utilities can promote targeted energy management services and products;
- Marketers could obtain information for targeted advertising;
- Hackers could wirelessly update smart meter firmware and remotel disconnect users. This could also allow attackers to corrupt the smart meters of individual homes, running up bogus charges or cause an electrical system to malfunction, shut down, or surge (frying all of your outlets and anything connected to them). Cyber assaults could involve hackers causing networked thermostats and appliances to malfunction possibly causing physical harm, especially to vulnerable populations. [Reference: "The Future of Crime" article, dated May 14, 2014];

This is not an exhaustive list. There is a potential for more extensive invasion of privacy as technology is developed and evolves into the future.

The following chart was extracted from a study on issues concerning privacy and legitimate applications of smart meters.:

Summary of Privacy Concerns Related to Smart Meters

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

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

Because of the potential for the invasion of privacy with existing technology and the unknowns of future technology interfacing with smart meters, the Claimant believes Duke Energy Ohio should have strict limits on the implementation and installation of smart meters.

REMEDY

Claimant has not refused the installation of a smart meter, but has demanded written documentation

from Duke Energy Ohio limiting the technological design and use of its smart meter to accumulate and retrieve only monthly electric use. PUCO has unlawfully permitted Duke Energy Ohio to charge Claimant $30 per month fee on his electric bill. Claimant demands a refund of each of the months for the months he has been charged and for Duke to cease charging the unlawful fee. Claimant believes if software can be designed to invade the home, software can be designed to limit a smart meters unlawful capabilities.

Respectfully submitted,

Gregory Peck, sui juris
3268 US Highway 52
Felicity, Ohio

Certificate of Service

I hereby certify that a true, accurate and complete copy of the foregoing was sent to be delivered by U. S. mail (postage prepaid), personal delivery, or electronic mail on this 24th day of October, 2017, to the following parties:

Gregory Peck

Elizabeth H. Watts
Duke Energy Business Services
139 East Fourth Street, 1303-Main
Cincinnati, Ohio 45201-0960

Public Utility Commission of Ohio
180 Broad Street
Columbus, Ohio 43215
Attn: Dan Fullin