THE STATE CORPORATION COMMISSION
OF THE STATE OF KANSAS

Before Commissioners: Shari Feist Albrecht, Chair
Jay Scott Emler
Pat Apple

In the Matter of the Complaint Against Kansas City Power & Light Company by Keith S. Carpenter.	)))	Docket No. 15-KCPE-474-COM
In the Matter of the Complaint Against KCP&L by Denese Roberts.	))	Docket No. 15- KCPE-265-COM
In the Matter of the Complaint Against Westar Energy by Jami Reihm.	))	Docket No. 15-WSEE-211-COM

ORDER ADOPTING STAFF'S MEMORANDUM

This matter comes before the State Corporation Commission of the State of Kansas (Commission). Having examined Litigation Staff's Memorandum submitted in this matter and being duly advised in the premises, the Commission finds as follows:

I. BACKGROUND

1. On April 13, 2015, Keith S. Carpenter (Complainant) filed a Formal Complaint against Kansas City Power & Light Company (KCP&L) with the Commission.[1]

2. On April 27, 2015, Litigation Staff for the Commission prepared a Memorandum analyzing the Formal Complaint for compliance with the Commission regulations and recommended to the Commission that the Formal Complaint does not satisfy the procedural requirements of K.A.R. 82-1-220. Litigation Staff further recommended the Commission grant the Complainant thirty (30) days to correct the procedural deficiencies and file an amended formal complaint.

[1] Complaint Against Kansas City Power & Light Company by Keith S. Carpenter (Apr. 13, 2015) (Formal Complaint).

3. On April 30, 2015, the Commission issued an Order Adopting Staff's Memorandum.

4. On May 18, 2015, Complainant filed an Amended Formal Complaint, attached hereto as "Attachment A", citing to the 4th and 5th Amendments of the U.S. Constitution as laws being violated by KCP&L for attempting to install an AMI meter at Complainant's residence.[2] The Complaint also alleges that smart meters create a serious health risk due to EMF radiation.[3]

5. On August 5, 2015, Litigation Staff for the Commission prepared a Memorandum analyzing the Amended Complaint for compliance with Commission regulations.[4]

Invasion of Privacy Argument

6. Litigation Staff recommends the Commission find that the Complainant's privacy arguments based upon alleged violations of the 4th and 5th amendment should be dismissed for lack of jurisdiction.[5]

Health and Safety Argument

7. Litigation Staff recommends the Commission find that the Complainant's health and safety argument substantially complies with the procedural requirements of K.A.R. 82-1-220 and establishes a *prima facie* case for Commission action.[6] Staff notes that the Amended Complaint does not specifically cite to any violation of law, rule or order in support of its argument and is thus not in compliance with K.A.R. 82-1-220(b)(1).[7] However, Staff recommends the Commission waive K.A.R. 82-1-200(b)(1) for good cause.[8]

II. FINDINGS AND CONCLUSIONS

[2] Amended Complaint Against Kansas City Power & Light Company by Keith S. Carpenter, May 18, 2015 (Amended Complaint).
[3] Id.
[4] Legal Staff's Memorandum, August 5, 2015.
[5] Id. at p. 2.
[6] Id.
[7] Id. at pp. 2-3.
[8] Id. at p. 3.

8. The Commission is satisfied that jurisdiction to conduct the requested investigation exists pursuant to K.S.A. 66-101 *et seq.*[9] Specifically, the Commission may investigate formal complaints regarding rates, rules, regulations, or practices of gas and electric public utilities. Furthermore, the Commission is granted authority over each electric public utility's equipment, manner of conduct, and management to protect public safety.[10] However, the Commission lacks the jurisdiction to issue rulings pertaining to the constitutional questions raised by the Complainant.[11]

9. The Commission finds that Litigation Staff's Memorandum dated August 5, 2015, attached hereto as Attachment "B" is hereby adopted and incorporated by reference.

IT IS, THEREFORE, BY THE COMMISSION ORDERED THAT:

(A) The Complainant's privacy argument based upon alleged violations of the 4th and 5th amendment is dismissed for lack of jurisdiction.

(B) The Complainant's health and safety argument substantially complies with the procedural requirements of K.A.R. 82-1-220.

(C) K.A.R. 82-1-220(b)(1) is waived for good cause.

(D) The Amended Complaint establishes a *prima facie* case for Commission action.

(E) The Amended Complaint is to be served upon KCP&L.

---

[9] Specifically, the Commission is granted broad authority to review formal complaints. *See* K.S.A. 66-101e ("Upon a complaint in writing made against any electric public utility governed by this act that any of the rates or rules and regulations of such electric public utility are in any respect unreasonable, unfair, unjust, unjustly discriminatory or unduly preferential, or both, or that any regulations, practice or act whatsoever affecting or relating to any service performed or to be performed by such electric public utility for the public, is in any respect unreasonable, unfair, unjust, unreasonably inefficient or insufficient, unjustly discriminatory or unduly preferential, or that any service performed or to be performed by such electric public utility for the public is unreasonably inadequate, inefficient, unduly insufficient or cannot be obtained, the commission may proceed with or without notice, to make such investigation as it deems necessary.").

[10] K.S.A. 66-101h.

[11] *Kaufman v. State Dep't of Soc. & Rehabilitative Servs.*, 248 Kan. 951, 954, 811 P.2d 876, 879 (1991).

(F) Staff shall investigate this matter and submit a Report and Recommendation to the Commission.

(G) This docket shall be consolidated with Docket Nos. 15-KCPE-265-COM and 15-WSEE-211-COM.

(H) The parties have fifteen (15) days, plus three (3) days if service of this order is by mail, from the date this order was served in which to petition the Commission for reconsideration of any issue or issues decided herein.[12]

(I) The Commission retains jurisdiction over the subject matter and the parties for the purpose of entering such further orders as it may deem necessary and proper.

BY THE COMMISSION IT IS SO ORDERED.

Albrecht, Chair; Emler, Commissioner; Apple, Commissioner

Dated: AUG 13 2015

Amy L. Gilbert

ORDER MAILED AUG 14 2015

Amy L. Gilbert
Secretary

SRF

[12] K.S.A. 66-118b; K.S.A. 2014 Supp. 77-529(a)(1).

Attachment A

KANSAS CORPORATION COMMISSION
OFFICE OF PUBLIC AFFAIRS & CONSUMER PROTECTION

Formal Complaint
February 2015

FORMAL COMPLAINT

BEFORE THE STATE CORPORATION COMMISSION OF THE STATE OF KANSAS

IN THE MATTER OF THE COMPLAINT AGAINST

Kansas City Power + Light
(Respondent, name of utility company)

by

Keith S. Carpenter + Barbara D. Carpenter
(Complainant, your name)

For Commission use only

DOCKET NO.

Received on

MAY 18 2015

by State Corporation Commission of Kansas

Please provide complainant (your) contact information:

Full Name(s): Keith S. + Barbara D. Carpenter

Address: 7633 Colonial Dr., Prairie Village, KS 66208

Daytime Phone: 913-381-8417

E-mail Address *(optional)*: kbcarp@sbcglobal.net

FORMAL COMPLAINT

Keith S. Carpenter and Barbara D. Carpenter
(Your name)

states that the above-named respondent is a public utility providing service in Kansas and is subject to the jurisdiction of the State Corporation Commission.

The facts and circumstances surrounding the complaint are set out in detail below:
(Be specific and as brief as possible. If necessary, attach additional sheets.)

In addition to the circumstances and events set forth in my original complaint (15-KCPE-474-Com), I received a letter from KCP+L dated April 14, 2015 informing us that unless the company heard from us within 30 days, KCP+L has the right to terminate all services without further notice. We know that utility companies have easement to install meters and we would be happy to unlock

(Continued on the other side)

(See Attached sheets)

Formal Complaint *continued*

Complainant requests that the respondent utility be required to provide an answer to the complaint and requests the following action be ordered by the Commission. *(State action or result desired.)*

> KCP+L must allow customers who choose to opt out of having AMI (smart meters) on their homes to do so without any additional monthly or other charges.

> KCP+L will install only conventional non communicating analog meters for customers who choose to opt out.

> Customers who have already had an AMI (smart meter) placed on their homes may have it removed by KCP&L and have it replaced with a conventional non communicating analog meter without additional monthly or other charges.

note: These requests are not unreasonable as they are very similar to requests granted to customers in the State of Vermont.

and for such further order or orders as the Commission may deem necessary.

VERIFICATION: I do solemnly, sincerely, and truly declare and affirm that the statements made in this complaint form are true and accurate to the best of my knowledge, and I do this under the pains and penalties of perjury.

Keith A. Carpenter
Barbara D. Carpenter

Complainant's (your) signature

May 14, 2015

Date signed

FILING INSTRUCTIONS

This form may be filed in person at the Kansas Corporation Commission's Office or by mail. All formal complaints, whether filed by mail or delivered in person, must be directed to:

Acting Executive Secretary
Kansas Corporation Commission
1500 SW Arrowhead Road
Topeka, KS 66604

For more information about the formal complaint process please refer to the instructions provided with this form or visit the KCC website: **http://kcc.ks.gov/**, Consumer Assistance, Filing a Complaint. You may also contact our Consumer Assistance staff toll-free at 1-800-662-0027 or by e-mail at public.affairs@kcc.ks.gov.

the gate for an installer to install a conventional non transmitting analog meter. It is not that we don't want our meter replaced, we just do not want it replaced with a transmitting device that exposes everyone to high levels of radio frequency, invades the privacy of our home, exposes us to cyber security risks, and violates our property rights.

Documentation

Since submitting my first complaint, we have discovered some compelling documentation concerning the potential threat of privacy and cyber security violations:

1. Department of Energy Data Access and Privacy Issues Related to Smart Grid Technologies report of October 5, 2010 (See especially page 2, last paragraph.)
2. Before the Public Utilities Commission (Comments of EPIC on EISA)
3. Smart Meter Data: Privacy and Cyber Security report to Congress by CRS

I am enclosing other documentation that will verify that smart meters can create a serious health risk:

4 Statement by American Academy of Environmental Medicine
5. Letter from Dr. David Carpenter to Baltimore Gas and Electric
6. Reducing Exposure to Dirty Electricity

Five other documents and pieces of information are inclosed:

7. What Does it Mean to Accept a Wireless Smart Meter on Your Homer or Business? by Ronald M. Powell, Ph.D., a retired U.S. Government scientist
8. Is Your Home's Energy Meter Spying on You? from Fox News
9. Smart Grid Information Clearinghouse
10. Federal Energy Act 2005
11. United States - IEEE Smart Grid
12. Federal Smart Grid Task Force | Department of Energy

Violations and/or possible Violations of any Laws,
Statutes, Regulations or the US and Kansas Constitutions

1). 4th Amendment to the Constitution of the United States of America * and Kansas Bill of Rights #15

See **document 3, page 10** "If, for example, the government requested the utility to record larger quantities of data than was customary this would likely warrant Fourth Amendment scrutiny. "

See **document 3, page 16** "However, there are three overarching considerations embodied in the use of smart meters that might weigh against the application of traditional third-party analysis. These include (a) a person's expectation of privacy while at home; (b) the breadth and granularity of private information conveyed by smart meters; (c) the lack of a voluntary assumption of the risk or consent to release of this data."

"In the case of smart meters, the information is generated in the home, an area accorded specific textual protection in the Fourth Amendment, and one the Supreme Court has persistently safeguarded. In no uncertain terms the court has asserted that "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion."

See **document 3, pages 19-21** "The mosaic theory is grounded in the idea that surveillance of the whole of one's activities over a prolonged period is substantially more invasive than a look at each item in isolation. In the case of smart meters, this is the difference between knowing a person's monthly energy usage and being able to discern a person's daily activities with considerable accuracy. This theory

intersects with the dragnet-styled law enforcement techniques in which the police cast a wide surveillance net, taking in a wealth of personal information with the goal of finding criminal activity among the stream of data...Additionally, the dragnet theory may apply to collection of energy usage data. This theory states that surveillance normally permitted under the Fourth Amendment--such as monitoring a person's movements on a public street--becomes an impermissible invasion of privacy when conducted on a prolonged 24-hour basis."

See **document 2, pages 4-5** "... the Supreme Court in *Kyllo v. United States* addressed the privacy implications of the monitoring of electricity 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

The Court found that even the minutest 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 government eyes.' Thus, the Court held that the police could not use thermal imaging equipment, which was not in general public use, 'to explore details of the home that would previously have been unknowable without physical intrusion,' without first obtaining a search warrant."

2.) 5th Amendment to the Constitution of the United States of America - last clause

See **document 7, page 1** "... to use your home or business to mount their wireless equipment ... without informing you fully of the implications... your home is no longer your castle, but instead is now the castle of your utility companies."

See **document 8** "They [power utilities] would say that 'they have easement,' but does this easement include the right to broadcast an FCC - regulated microwave transmitter on your home, taking your private property to do so, for their benefit, and without your consent?"

3.) Electronic Communications Privacy Act

See **Document 3, page 23** "ECPA, enacted in 1986, 'addresses the interception of wire, oral and electronic communications.' the statue defines electronic communications as 'any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...' Based on the description of the smart meter network, provided above, the envisioned transmission of customers' energy usage data by smart meters would seem to fall squarely within the definition of electronic communications under ECPA."

4.) Federal Energy Act 2005

See **document 10 Sec. 1252 (a), (14), (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." Nothing is said here about forcing a time-based meter on a customer.

F. A. C.

* The Congressional Research Service stated that "The Fourth Amendment applies only to acts by the government. But there are at least two exceptions to this rule. First, if a utility performs a function traditionally exercised by the government, it may be considered a state actor under the public function exception... The Fourth Amendment may also apply to a private utility if its acts were directed by the government." **(document 3, pages 8-9)**

KCP&L is regulated by the KCC. According to a 2007 order, "The Commission encouraged voluntary pilot programs as the best vehicle for deploying smart metering and TOU rates." According to the same order, "The commission **strongly encourages** the development and implementation of pilot programs introducing smart metering and time-based rates, and time-based technology." (emphasis mine) The words "strongly encourage" would qualify as direction by a state government agency. **(See document 9, page 1)**

"The United States' Smart Grid policy is primarily directed by the central federal government through the guidance and authority of various acts of congress which are implemented by the Federal Smart Grid Task Force led by the Department of Energy (DoE) and staffed by" several different agencies.

"In its key role as the implementer of national Smart Grid policy the DoE has created a partnership industry and quasi governmental professional electrical power organizations in an attempt to integrate a comprehensive set of subject matter experts in developing a roadmap and vision for the Smart Grid."

"Although the federal government is responsible for the nation's Smart Grid policy via its national energy policy some aspects of that policy fall outside of the federal government's jurisdictional boundaries and are the responsibility of a vast and complex web of state, regional, local and municipal governing authorities. Together these groups are pooling their resources to collaboratively develop the Smart Grid" **(document 11, page 1)**

The above three paragraphs from United States - IEEE Smart Grid web site confirm that KCP&L is acting as an agent of government at many if not all levels.

"The Federal Smart Grid Task Force was established under Title XIII of the Energy Independence and Security Act of 2007 (EISA)...The mission of the Task Force is to ensure awareness, coordination and integration of the diverse activities of the Federal Government related to smart grid technologies, practices, and services."
(document 12)

Keith A. Carpenter
Barbara A Carpenter May 14, 2015

Doc. 1

DEPARTMENT OF ENERGY

DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES

October 5, 2010

INTRODUCTION AND EXECUTIVE SUMMARY

This report by the Department of Energy (DOE) complements DOE's companion report, *Informing Federal Smart Grid Policy: The Communications Requirements of Electric Utilities.*[1] Both reports are also components of the federal government's much broader efforts to facilitate the adoption and deployment of various Smart Grid technologies. These ongoing broader efforts have encompassed many agencies including many operational units within DOE, the Federal Communications Commission (FCC), the Federal Energy Regulatory Commission (FERC), the National Institute of Standards and Technology (NIST), and the National Science and Technology Council Committee on Technology's Subcommittee on Smart Grid.

This report and its companion report also respond to recommendations directed toward DOE in the National Broadband Plan (the "NBP"), authored by the FCC at the direction of Congress.[2] The NBP seeks to ensure that every American has access to broadband capability. The NBP also includes a detailed strategy for achieving affordability and maximizing use of broadband to advance consumer welfare, civic participation, public safety and homeland security, health care delivery, energy independence and efficiency, education, entrepreneurial activity, job creation and economic growth, and other national purposes.[3] As part of this strategy, the NBP made recommendations to various Federal agencies, including DOE. In particular, the NBP recommended that DOE evaluate the overall communications needs of the Smart Grid, consider consumer-data-accessibility policies when evaluating Smart Grid grant applications, and report on the states' progress toward enacting consumer data accessibility and develop best practices guidance for states. This report implements the latter two recommendations, while the companion report implements the first recommendation.

Smart Grid technologies will be a critical long-term component of a more interactive, robust, and efficient electricity generation, transmission and usage system. Moreover, the advanced, state-of-the-art electrical grid that these technologies will create will be an important component of an overall national energy, economic, and security strategy predicated upon reasserting U.S. leadership in the race to develop cleaner, sustainable, and secure sources of energy—a race that Secretary of Energy Chu has called "a Second Industrial Revolution."

As DOE has emphasized, the promise of the Smart Grid is enormous and includes improved reliability, flexibility, and power quality, as well as a reduction in peak demand and transmission costs, environmental benefits, and increased security, energy efficiency, and durability and ease

---

[1] *See* Department of Energy, *Informing Federal Smart Grid Policy: The Communications Requirements of Electric Utilities*, October 5, 2010, available at http://www.gc.energy.gov/1592.htm. This complementary report provides a more detailed summary of both the operation of Smart Grid technologies like advanced metering and the federal government's multifaceted efforts to promote their adoption and deployment.

[2] The Plan, developed pursuant to the American Recovery and Reinvestment Act of 2009 (P.L. No. 111-5), was issued on March 16, 2010 and is available at http://www.broadband.gov/plan/.

[3] *Id.*

of repair in response to attacks or natural disasters. But DOE also recognizes that long-term success of Smart Grid technologies depends upon understanding and respecting consumers' reasonable expectations of privacy, security, and control over who has access to potentially revealing energy-usage data.

DOE believes that privacy and access, in the context of a Smart Grid, are complementary values rather than conflicting goals. The practical impact of a Smart Grid depends on its capacity to encourage and accommodate innovation while making usage data available to consumers and appropriate entities and respecting consumers' reasonable interests in choosing how to balance the benefits of access against the protection of personal privacy and security. This report seeks to assist both policymakers and private and public entities interested in understanding how legal and regulatory regimes are evolving to better accommodate innovation, privacy and data-security. To that end, this report surveys industry, state, and federal practices in this evolving area to alert industry leaders, state regulators, and federal policy makers to trends and practices that seem most likely to accommodate all of these values and maximize the value of Smart Grid technologies.

This Report consists of two main components. The next section, *Key Findings*, summarizes DOE's impressions of the information it collected in the spring and summer of 2010 during its proceeding on the data-privacy and data-security issues raised by Smart Grid technologies like advanced metering. In particular, this section provides a coherent summary of developing trends, consensuses, and potential best practices emerging as States use or adapt existing legal regimes to accommodate the deployment of Smart Grid technologies. The second section, *Summary of Public Comments and Information,* provides a more comprehensive summary of the comments, both written and transcribed, that DOE received in response to the Request for Information ("RFI") and during the public roundtable discussion conducted during the preparation of this report.

Overview of Data Access and Privacy Concerns

Recognizing and addressing the significant concerns with access to and privacy protection for energy usage data are critical to the development of U.S. Smart Grid policies because of the enormous potential of consumer and authorized third party access to energy consumption data through the use of Smart Grid technologies, and the continued importance of utility access to such data.

Advances in Smart Grid technology could significantly increase the amount of potentially available information about personal energy consumption. Such information could reveal personal details about the lives of consumers, such as their daily schedules (including times when they are at or away from home or asleep), whether their homes are equipped with alarm systems, whether they own expensive electronic equipment such as plasma TVs, and whether they use certain types of medical equipment. Consumers rightfully expect that the privacy of this information will be maintained. The proprietary business information of non-residential customers could also be revealed through the release of energy consumption data, resulting in competitive harm. Studies conducted by utilities and consumer advocates have consistently shown that privacy issues are of tremendous import to consumers of electricity.

Doc. 2

Before the Public Utility Commission

Utility Commission

Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System

Rulemaking 08-12-009
(Filed December 18, 2008)

Comments of the Electronic Privacy Information Center (EPIC) on Proposed Policies and Findings Pertaining to the EISA Standard Regarding Smart Grid and Customer Privacy

Lillie Coney, Associate Director, coney@epic.org
Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue, NW, Suite 200
Washington, DC 20009
202-483-1140

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment and constitutional values. EPIC has a long-standing interest in privacy and technology issues.[1] EPIC has a specialized area of expertise regarding digital communication technologies and privacy policy.[2] 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.[3] 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. see http://epic.org/.

EPIC appreciates this opportunity to submit comments before the California Public Utility Commission on the topic of Smart Grid and Privacy.[4] The term "Smart Grid" encompasses a host of inter-related technologies rapidly moving into public use to reduce or better manage electricity consumption. Smart Grid systems may be designed to allow electricity service providers, users, or third-party electricity usage management service providers to monitor and control electricity use.

---

[1] EPIC, Electronic Privacy Information Center, http://www.epic.org (last visited Dec. 1, 2009).
[2] EPIC, Privacy, http://www.epic.org/privacy/default.html (last visited Dec. 1, 2009).
[3] EPIC, The Smart Grid and Privacy, http://epic.org/privacy/smartgrid/smartgrid.html (last visited Dec. 1, 2009).
[4] California Public Utility Commission, Assigned Commissioners and Administrative Law Judge's Joint Ruling Amending Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid, Feb. 8, 2010 http://www.cpuc.ca.gov/EFILE/RULINGS/113482.pdf.

Privacy implications for Smart Grid technology deployment centers on the collection, retention, sharing, or reuse of electricity consumption information on individuals, homes, or offices. Fundamentally, Smart Grid systems will be multi-directional communication and energy transfer networks that enable electricity service providers, consumers, or third-party access to customer information.

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.

SMART GRID DEPLOYMENT PLANS AND PRIVACY

Fundamentally, Smart Grid systems will be multi-directional communications and energy transfer network that enables electricity service providers, consumers, or third-party use of data. The focus for protecting privacy of information stored on computers or exchanged on computing networks is whether data is or is not PII. This is information that can locate or identify a person, or can be used in conjunction with other information to uniquely identify an individual. Historically, PII would include name, Social Security Number, address, phone number, or date of birth. In the Internet Age, the list of PII has grown to include e-mail addresses, IP addresses, social networking pages, search engine requests, log records and passwords.

If privacy is not a core component of Smart Grid and related applications that collect, retain, use, or share PII, then broad adoption of the technology will be at

risk. Smart Grid planning and implementation must take an end-to-end approach to securing PII that enforces privacy rights of energy users.

California has taken steps to establish privacy protections for its residents in a number of areas, but has added the critical component of accountability and oversight.[5] The drafters of the California Constitution state that, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[6]

There is also a well-established federal interest in the right of privacy. The U.S. Supreme Court notes, the constitutional right of privacy protects two distinct interests: "one is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[7] Moreover, public opinion polls consistently find strong support among Americans for privacy rights in law to protect their personal information from government and commercial entities.[8]

More recently, the Supreme Court in *Kyllo v. United States*[9] addressed the privacy implications of the monitoring of electricity use in the home. After reviewing precedent, the Court found that a search warrant must be obtained before the

---

[5] California Office of Privacy Protection, Privacy Laws, http://www.privacy.ca.gov/privacy_laws.htm

[6] California State Constitution, Article1, Section 1, http://www.leginfo.ca.gov/.const/.article_1.

[7] *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977) and *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977).

[8] *See generally* EPIC, Public Opinion on Privacy, http://epic.org/privacy/survey (last visited Dec. 1, 2009).

[9] 533 U.S. 27 (2001).

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.[10]

The Court found that even the minutest 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 government eyes."[11] Thus, the Court held that the police could not use thermal imaging equipment, which was not in general public use, "to explore details of the home that would previously have been unknowable without physical intrusion," without first obtaining a search warrant.[12]

The well-established interest in privacy of power consumption in the home begins the discussion. There are documented instances in this decade where California residents have come under suspicion because of their electricity usage. For example, in 2004 a Carlsbad California family faced police investigation due to higher electricity consumption than their neighbors.[13]

Smart Grid PII data collection should begin with "fair information practices" or FIPs, which set out the essential framework for the collection and use of personal information. FIPs creates the foundation for service provision and is critical to state and federal privacy law. This approach to privacy protection, which places obligations on those entities that collect personal information and provides rights to

---

[10] *Id.* at 34.
[11] *Id.* at 37.
[12] *Id.* at 40.
[13] Privacy.org, "A Suspicious Electric Utility Bill?," March 29, 2004.

individuals whose personal data is collected, undergirds most of modern privacy law. In fact, it provides the framework for the Privacy Act of 1974[14] and dozens of state and federal laws.[15]

In the area of Smart Grid, the issues will not just arise when utilities are directly involved in the collection, retention, and use of PII, but will extend to third parties who have access to this data. Utilities have used contractors or third-party service providers to manage discrete components of electricity delivery, billing, or service provision. The question before the CPUC ultimately is the legitimacy of sharing consumer electricity consumption data with marketers, which could use the information to target sales for home improvements or new appliances. Business models for Smart Grid involve entities that have not established electric service relationships with consumers and therefore should be held to a higher standard for data use restrictions and security of consumer data.

TRANSPARENCY

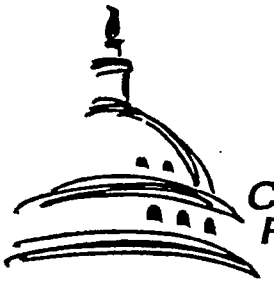
Energy consumers have expectations for privacy regarding their energy usage data that may run counter to data sharing and reuse by non-utility service providers. Some would argue that if consumers sign agreements allowing third parties to get access to their electric utility data that is sufficient. EPIC would strongly recommend that the CPUC not rely on the failed notice and consent models that have proven to be an unreliable means of assuring customer privacy rights.

---

[14] Privacy Act of 1974 , 5 U.S.C. § 552a (2008).

[15] *See, e.g.*, Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681u (2008); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-22 (2008); Fair Information Practices Act, Mass Ann. Laws ch. 66A §§ 1-3 (2008); Insurance Information and Privacy Protection Act, Me. Rev. Stat. Ann. tit. 24-A, §§ 2201-20 (2008).

Doc. 3



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

American Electric Reliability Corporation, which impose obligations on utilities that participate in the generation or transmission of electricity.[18]

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. Section 5 of the Federal Trade Commission Act (FTC Act) allows the Federal Trade Commission (FTC) to bring enforcement proceedings against electric utilities that violate their privacy policies or fail to protect meter data from unauthorized access, provided that the FTC has statutory jurisdiction over the utilities.

It is unclear how Fourth Amendment protection from unreasonable search and seizures would apply to smart meter data, due to the lack of cases on this issue. However, depending upon the manner in which smart meter services are presented to consumers, smart meter data may be protected from unauthorized disclosure or unauthorized access under the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), and the Electronic Communications Privacy Act (ECPA). If smart meter data is protected by these statutes, law enforcement would still appear to have the ability to access it for investigative purposes under procedures provided in the SCA, ECPA, and the Foreign Intelligence Surveillance Act (FISA).

Smart Meter Data: Privacy and Security Concerns

Residential smart meters present privacy and cybersecurity issues[19] that are likely to evolve with the technology.[20] In 2010, the National Institute of Standards and Technology (NIST) published a report identifying some of these issues, which fall into two main categories: (1) privacy concerns that smart meters will reveal the activities of people inside of a home by measuring their electricity usage frequently over time;[21] and (2) fears that inadequate cybersecurity measures surrounding the digital transmission of smart meter data will expose it to misuse by authorized and unauthorized users of the data.[22]

Detailed Information on Household Activities

Smart meters offer a significantly more detailed illustration of a consumer's energy usage than regular meters. Traditional meters display data on a consumer's *total* electricity usage and are typically read manually once per month.[23] In contrast, smart meters can provide *near real-time* usage data by measuring usage electronically at a much greater frequency, such as once every 15

[18] For additional information on the development of mandatory national smart grid privacy and cybersecurity standards by federal agencies, see MASS. INST. OF TECH., THE FUTURE OF THE ELECTRIC GRID 197-234 (2011) [hereinafter MIT GRID STUDY]; *see also* CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.

[19] According to the authors of the MIT study, cybersecurity "refers to all the approaches taken to protect data, systems, and networks from deliberate attack as well as accidental compromise, ranging from preparedness to recovery." MIT GRID STUDY, *supra* note 18, at 208. Closely related is the concept of "information privacy," which "deals with policy issues ranging from identification and collection to storage, access, and use of information." *Id.* at 219 n.viii.

[20] *See* NIST PRIVACY REPORT, *supra* note 11, at 1.

[21] *Id.* at 4, 11. Data that offers a high degree of detail is said to be "granular." *Id.*

[22] *See id.* at 4, 23-24, 29.

[23] *Id.* at 2, 9.

minutes.[24] Current smart meter technology allows utilities to measure usage as frequently as once every minute.[25] By examining smart meter data, it is possible to identify which appliances a consumer is using and at what times of the day, because each type of appliance generates a unique electric load "signature."[26] NIST wrote in 2010 that "research shows that analyzing 15-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances."[27] A report for the Colorado Public Utilities Commission discussed an Italian study that used "artificial neural networks" to identify individual "heavy-load appliance uses" with 90% accuracy using 15-minute interval data from a smart meter.[28] Similarly, software-based algorithms would likely allow a person to extract the unique signatures of individual appliances from meter data that has been collected less frequently and is therefore less detailed.[29]

By combining appliance usage patterns, an observer could discern the behavior of occupants in a home over a period of time.[30] For example, the data could show whether a residence is occupied, how many people live in it, and whether it is "occupied by more people than usual."[31] According to the Department of Energy, smart meters may be able to reveal occupants' "daily schedules (including times when they are at or away from home or asleep), whether their homes are equipped with alarm systems, whether they own expensive electronic equipment such as plasma TVs, and whether they use certain types of medical equipment."[32] **Figure 1**, which appears in NIST's report on smart grid cybersecurity, shows how smart meter data could be used to decipher the activities of a home's occupants by matching data on their electricity usage with known appliance load signatures.

---

[24] *Id.* at 13.

[25] COLORADO PRIVACY REPORT, *supra* note 6, at 2. Some utilities may elect to receive data at less frequent intervals because "backhauling real-time or near real-time data from the billions of devices that may eventually be connected to the Smart Grid would require not only tremendous bandwidth" but also greater data storage capacities that could make the effort "economically infeasible." DEP'T OF ENERGY COMMUNICATIONS REPORT, *supra* note 3, at 20. However, the "trend" is for utilities to collect data more frequently. *See* COLORADO PRIVACY REPORT, *supra* note 6, at A-1 n.111.

[26] NIST PRIVACY REPORT, *supra* note 11, at 2, 14.

[27] *Id.* at 14. *But see* DEP'T OF ENERGY PRIVACY REPORT, *supra* note 6, at 9 (claiming, in 2010, that smart meter technology "cannot yet identify individual appliances and devices in the home in detail, but this will certainly be within the capabilities of subsequent generations of Smart Grid technologies").

[28] COLORADO PRIVACY REPORT, *supra* note 6, at 3 n.7, A-8.

[29] *Id.* at A-9.

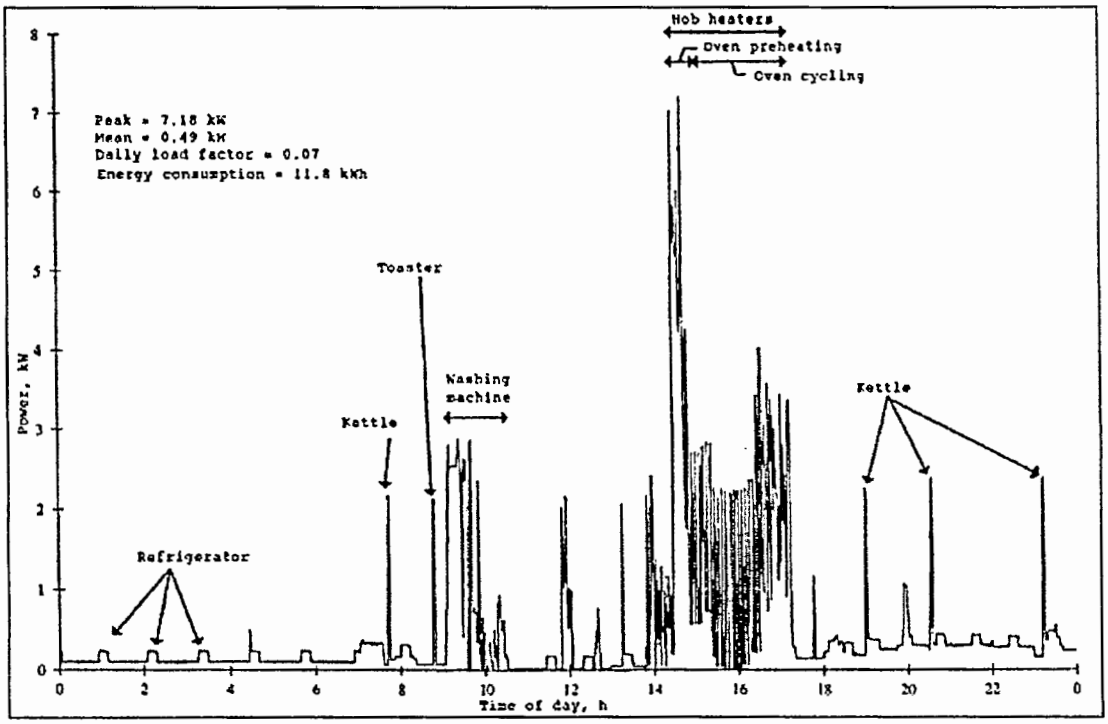
[30] NIST PRIVACY REPORT, *supra* note 11, at 6 & n.9.

[31] *Id.* at 11.

[32] DEP'T OF ENERGY PRIVACY REPORT, *supra* note 6, at 2.

Figure 1. Identification of Household Activities from Electricity Usage Data

Unique Electric Load Signatures of Common Household Appliances



Source: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 13 (2010), *available at* http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

Note: Researchers constructed this picture from electricity usage data collected at one-minute intervals using a nonintrusive appliance load monitoring (NALM) device, which is similar to a smart meter in the way that it records usage data. For a comparison of the technologies, see COLORADO PRIVACY REPORT, *supra* note 6, at A-1 to A-9.

Smart meter data that reveals which appliances a consumer is using has potential value for third parties, including the government. In the past, law enforcement agents have examined *monthly* electricity usage data from *traditional* meters in investigations of people they suspected of illegally growing marijuana.[33] For example, in *United States v. Kyllo*, a federal agent subpoenaed the suspect's electricity usage records from the utility and "compared the records to a spreadsheet for estimating average electrical use and concluded that Kyllo's electrical usage was abnormally high, indicating a possible indoor marijuana grow operation."[34] If law enforcement officers obtained near-real time data on a consumer's electricity usage from the utility company, their ability to monitor household activities would be amplified significantly.[35] For example, by observing when occupants use the most electricity, it may be possible to discern their daily schedules.[36]

[33] NIST PRIVACY REPORT, *supra* note 11, at 11, 29; *see also* United States v. Kyllo, 190 F.3d 1041, 1043 (9th Cir. 1999), *rev'd on other grounds*, 533 U.S. 27 (2001).

[34] *Kyllo*, 190 F.3d at 1043.

[35] *See supra* notes 26-32 and accompanying text.

[36] *See supra* note 32 and accompanying text.

contravene this protection. Although there is no Fourth Amendment case on point, analogous cases may provide guidance.[63]

To assess whether there has been a Fourth Amendment violation, two primary questions must be asked: (1) whether there was state action; that is, was there sufficient government involvement in the alleged wrongdoing to trigger the Fourth Amendment; and (2) whether the person had an expectation of privacy that society is prepared to deem reasonable.[64] If the first question is answered in the affirmative, then the analysis moves to the second question. But if no state action is found, the analysis ends there and the Fourth Amendment does not apply. This subpart will first determine whether access to smart meter data by police, or by privately and publicly owned utilities, satisfies the state action doctrine, thereby warranting further Fourth Amendment review.

State Action: Privately Versus Publicly Owned Utilities

Most of the safeguards for civil liberties and individual rights contained in the U.S. Constitution apply only to actions by state and federal governments.[65] This rule, known as the state action doctrine, arises when a victim claims his constitutional rights have been violated, and therefore must prove the wrongdoer had sufficient connections with the government to warrant a remedy.[66] Applying the state action test is intended to determine whether a utility's collection and dissemination of smart meter data is governed by the Fourth Amendment, and if so, to what extent. Although there are many variations in the governance and ownership of utilities—some are privately owned, others publicly owned, some federally operated, and still others nonprofit cooperatives—they generally fall into two broad categories: public and private.[67] This section will analyze the constitutional differences between privately and publicly owned utilities under the state action doctrine and a public records theory.

Privately Owned and Operated Utilities

It is broadly said that the Fourth Amendment applies only to acts by the government.[68] But there are at least two exceptions to this rule. First, if a utility performs a function traditionally exercised by the government, it may be considered a state actor under the public function exception. Second, the Fourth Amendment may apply when a private utility acts as an instrument or agent of the police.[69]

---

[63] For additional analyses of smart meters under the Fourth Amendment, see Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161 (2011); *see also* QUINN, *supra* note 6, at 28 ("[I]nterval data of electricity consumption appears to be in something of a no-man's-land under Supreme Court Fourth Amendment jurisprudence.").

[64] California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

[65] Civil Rights Cases, 109 U.S. 3, 11 (1883) ("It is State action of a particular character that is prohibited. Individual invasion of individual rights is not the subject-matter of the [Fourteenth] amendment."); *see* JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW §12.1(a)(i) (8th ed. 2010).

[66] NOWAK & ROTUNDA, *supra* note 65.

[67] Determining whether a private actor is sufficiently "public" is not clear-cut. Then Justice Rehnquist noted, "[t]he true nature of the State's involvement may not be immediately obvious, and detailed inquiry may be required in order to determine whether the test is met." Jackson v. Metropolitan Edison Co., 419 U.S. 345, 351 (1974).

[68] Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

[69] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

Under the public function exception, a nominally private entity is treated as a state actor when it assumes a role traditionally played by the government.[70] Determining when this exception applies has not proved easy,[71] but it is reasonably clear that private utilities do not, in most instances, satisfy it. In *Jackson v. Metropolitan Edison Co.*, a customer sued a privately owned utility under the Civil Rights Act of 1871 for improperly shutting off her service without providing her notice or a hearing.[72] The Supreme Court asked whether there was a close enough nexus between the state and the utility for the acts of the latter to be treated as those of the former.[73] Although the utility was heavily regulated by the state, it was held not to be a state actor.[74] The Court reasoned that the provision of utility service is not generally an "exclusive prerogative of the State."[75] Also absent was the symbiotic relationship between the utility and the state found in previous cases.[76] Though its holding was broad, the Court did not foreclose the possibility that a privately owned utility could be a state actor under different circumstances.[77] This possibility, however, appears narrow.

The Fourth Amendment may also apply to a private utility if its acts were directed by the government. Generally, searches performed by private actors without police participation or encouragement are not governed by the Fourth Amendment.[78] A search by a private insurance investigator, for instance, was not a "search" in the constitutional sense, though the evidence was ultimately used by the government at trial.[79] This result differs, however, if there is sufficient government involvement. If the search has been ordered or requested by the government, the private actor will become an "instrument or agent of the state" and must abide by Fourth Amendment strictures.[80] For example, the Fourth Amendment does not apply when a telephone company installs a pen register on its own initiative.[81] The same action constitutes a search, however, if requested by the government.[82]

This theory applies not only to direct instigation, but also on a broad, programmatic level. In the 1960s and 1970s the federal government required privately owned and operated airlines to institute new security measures to combat airline hijacking.[83] In *United States v. Davis*, the airline

[70] Marsh v. Alabama, 326 U.S. 501 (1946) (holding that privately owned property was equivalent to "community shopping center" thus private party was subject to the First and Fourteenth Amendments).

[71] *See* NOWAK & ROTUNDA, *supra* note 65, §12.2.

[72] *Jackson*, 419 U.S. at 347; *see also* Mays v. Buckeye Rural Elec. Coop., Inc., 277 F.3d 873, 880-81 (6th Cir. 2002) (holding that nonprofit cooperative utility was not a state actor under the federal constitution); Spickler v. Lee, No. 02-1954, 2003 U.S. App. LEXIS 6227, at *2 (1st Cir. March 31, 2003) (holding that private electric utility company was not a state actor).

[73] *Jackson*, 419 U.S. at 351.

[74] *Id.* at 358-59.

[75] *Id.* at 353.

[76] *Id.* at 357.

[77] *Id.* at 351.

[78] 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE §1.8, at 255 (4th ed. 2004).

[79] United States v. Howard, 752 F.2d 220, 227-28 (6th Cir. 1985).

[80] Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (internal quotation marks omitted); *see* LAFAVE, *supra* note 78, §1.8(b).

[81] United States v. Manning, 542 F.2d 685, 686 (6th Cir. 1976).

[82] People of Dearborn Heights v. Hayes, 82 Mich. App. 253, 258 (1978).

[83] United States v. Davis, 482 F.2d 893, 897-903 (9th Cir. 1973).

searched a passenger based on these requirements and found a loaded gun.[84] The Ninth Circuit held that it made no difference whether the search was conducted by a private or public official: "the search was part of the overall, nation-wide anti-hijacking effort, and constituted 'state action' for purposes of the Fourth Amendment."[85] Thus, if a private party is required to perform a search or collect data under federal or state laws or regulations, there will be sufficient state action for the Fourth Amendment to apply. Or, put another way, the government cannot circumvent the Fourth Amendment by requiring a private party to initiate a search or implement an investigative program.

This agency theory might apply to the collection of smart meter data. If the utility is accessing this information "independent of the government's intent to collect evidence for use in a criminal prosecution,"[86] the utility will not be considered an agent of the government for Fourth Amendment purposes. But there might be instances when government instigation will trigger further analysis. If, for example, the government requested the utility to record larger quantities of data than was customary (e.g., increasing the intervals from sub-15 minute intervals to sub-five minute or sub-one minute intervals), this would likely warrant Fourth Amendment scrutiny. Also, if the police requested the utility to hand over customer data, say, for spikes in energy commensurate with a marijuana growing operation, this would likely be a sufficient instigation to trigger further constitutional review. Other situations may arise where the government establishes a dragnet-type law enforcement scheme in which all smart meter data is filtered through police computers. This could also implicate the agency theory and warrant a finding of state action.

Publicly Owned and Operated Utilities

Although the Fourth Amendment (with its warrant and probable cause requirement) typically applies to public actors, in certain instances their collection of information may not fall under the Fourth Amendment or may prompt a lower evidentiary standard. The Supreme Court has infrequently considered the scope of the Fourth Amendment "on the conduct of government officials in noncriminal investigations,"[87] and even less frequently as to "noncriminal *noninvestigatory* governmental conduct."[88] Nonetheless, there are two lines of cases that may apply to smart meters in which the Fourth Amendment may not apply at all (noncriminal noninvestigatory conduct) or may be reduced (noncriminal investigations). The key to this analysis is the government's purpose in collecting the data.

The Supreme Court has developed a line of cases dubbed the "special needs" doctrine that permits the government to perform suspicionless searches if the special needs supporting the program outweigh the intrusion on the individual's privacy.[89] It is premised on the notion that "'special needs,' beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[90] If, on the one hand, the objective of the search is not for law

[84] *Id.* at 895.

[85] *Id.* at 904.

[86] United States v. Howard, 752 F.2d 220, 228 (6th Cir. 1985).

[87] *The Supreme Court, 1986-Term—Leading Cases*, 101 HARV. L. REV. 119, 230 (1987).

[88] United States v. Attson, 900 F.2d 1427, 1430 (9th Cir. 1990) (emphasis in original).

[89] Ferguson v. City of Charleston, 532 U.S. 67, 77-78 (2001).

[90] Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 620 (1989) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)).

States v. Hamilton held that the means of obtaining power records from a third-party by way of administrative subpoena as opposed to "intrusion on the home by 'sense enhancing technology'" is "legally significant," removing this type of situation from the *Kyllo*-home privacy line of cases into the *Miller*-third-party line.[139]

It is difficult to predict whether a court would extend this traditional third-party analysis to smart meters. The courts may seek to ensure the predictability and stability of the third-party doctrine generally and administration of utility services specifically, thus requiring a bright-line rule for all third-party circumstances.[140] There is an advantage to a rule that is easy to apply, that allows utilities to better govern their affairs, and does not permit "savvy wrongdoers [to] use third-party services in a tactical way to enshroud the entirety of their crimes in zones of Fourth Amendment protection."[141] However, there are three overarching considerations embodied in the use of smart meters that might weigh against the application of traditional third-party analysis. These include (a) a person's expectation of privacy while at home; (b) the breadth and granularity of private information conveyed by smart meters; (c) the lack of a voluntary assumption of the risk or consent to release of this data.

Privacy in the Home

The location of the search mattered little in the traditional third-party cases, but it may take on constitutional significance with smart meters.[142] In the case of smart meters, the information is generated in the home, an area accorded specific textual protection in the Fourth Amendment, and one the Supreme Court has persistently safeguarded.[143] In no uncertain terms the Court has asserted that "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion."[144] Even as technology advances—whether a tracking or thermal-imaging device or something new—the Court has maintained this bulwark. Because of the significance of the home, access to smart

[139] United States v. Hamilton, 434 F. Supp. 2d 974, 980 (D. Or. 2006); Booker v. Dominion Va. Power, No. 3:09-759, 2010 U.S. Dist. LEXIS 44960, at *17 (E.D. Va. May 7, 2010); *see also* Samson v. State, 919 P.2d 171, 173 (Ala. App. 1996) (holding under state constitution that "utility records are maintained by the utility and do not constitute information in which society is prepared to recognize a reasonable expectation of privacy"); People v. Stanley, 86 Cal. Rptr. 2d 89, 94 (Cal. App. 1999) (same).

[140] *See* Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1687, 1710 (1976).

[141] Kerr, *Third-Party Doctrine*, *supra* note 115, at 564.

[142] In *Smith*, the "site of the call was immaterial for purposes of analysis" of that case. Smith v. Maryland, 442 U.S. 735, 743 (1979). Whether a person dials a telephone number from his home, a telephone booth, or any other location does not alter the nature of the activity, and thus does not affect the Fourth Amendment analysis. The privacy interests implicated are the same no matter where the call is placed. The same theory applies to bank records. It matters not where someone writes a check, or fills out a deposit slip—the privacy interest is the same.

[143] Payton v. New York, 445 U.S. 573, 589 ("The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home—a zone that finds its roots in clear and specific constitutional terms: 'The right of the people to be secure in their ... houses ... shall not be violated.'") (quoting U.S. CONST. amend IV); Minnesota v. Carter, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring) ("[I]t is beyond dispute that the home is entitled to special protection as the center of the private lives of our people. Security of the home must be guarded by law in a world where privacy is diminished by enhanced surveillance and sophisticated communication systems.").

[144] Silverman v. United States, 365 U.S. 505, 511 (1961).

meter data may prompt a doctrinal shift away from the third-party doctrine. Several home privacy cases shed light on this possible approach.[145]

In *Kyllo v. United States*, the Court had to decide whether the use of a thermal-imaging device from the outside of a home that detected the amount of heat coming from inside the home was a violation of the Fourth Amendment.[146] In *Kyllo*, an agent of the Department of the Interior suspected Danny Kyllo was growing marijuana in his home with the use of high-intensity lamps.[147] The agent used a thermal imager to scan the outside of Kyllo's apartment to determine if he was using these "grow" lamps.[148] Thermal imagers can detect energy emitting from the outside surface of an object.[149] When scanning the home, the thermal imager produced an image with various shades of black, white, or gray—the shades darker or lighter depending on the warmth of the area being scanned.[150] From the passenger seat of his car, the agent scanned Kyllo's home for several minutes.[151] From his scan, he determined that the area over the garage and one side of his home were relatively hot compared to neighboring homes.[152] Based on utility bills, informant tips, and the results of thermal imaging, the agents obtained a warrant to search Kyllo's home.[153] As suspected, inside the home the agents found a marijuana growing operation, including over 100 plants.[154]

Justice Scalia first posited that "with very few exceptions, the question whether a warrantless search of the home is reasonable must be answered no."[155] Searches of the home were historically analyzed under the common law doctrine of trespass,[156] but during the mid-20th century the Court instead anchored the Fourth Amendment to a conception of privacy.[157] While this test may be difficult to apply in the context of automobiles, telephone booths, or other public areas, it is made easier when concerning the home:

> In 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 deep roots in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged

[145] In April 2012, the Supreme Court will hear oral arguments in its most recent home privacy case, Jardines v. Florida, 73 So. 3d 34 (Fla. 2011), *cert granted*, 2012 U.S. LEXIS 7 (Jan. 6, 2012) (No. 11-564), where it will decide whether a drug sniff at the front door of a suspect's house by a trained narcotics dog is a Fourth Amendment search requiring probable cause. This case should shed further light on the parameters of privacy surrounding the home.

[146] Kyllo v. United States, 533 U.S. 27, 29 (2001).

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] *Id.* at 29-30.

[151] *Id.* at 30.

[152] *Id.*

[153] *Id.*

[154] *Id.* The Ninth Circuit held that Kyllo had not exhibited a subjective expectation of privacy in the home because he did not attempt to prevent the heat emitting from the lamps from escaping his home. United States v. Kyllo, 190 F.3d 1041, 1046 (9th Cir. 1999). Further, the panel held that even if he had a subjective expectation of privacy, it was not a reasonable one since the imager "did not expose any intimate details of Kyllo's life." *Id.* at 1047.

[155] *Kyllo*, 533 U.S. at 31.

[156] *See* Olmstead v. United States, 277 U.S. 438 (1928).

[157] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The modern formulation of the reasonable expectation of privacy test derives not from the majority opinion but from Justice Harlan's concurrence.

police merely obtained the relative temperatures of a house,[170] and in *Karo* the police only generally located the beeper in the house.[171] Although this information was limited, the Court nonetheless prohibited such investigatory techniques. Smart meters have the potential to produce significantly more information than that derived in *Kyllo* and *Karo*, including what individual appliances we are using; whether our house is empty or occupied; and when we take our daily shower or bath.[172] Further, a look at **Figure 1**, *supra*, makes it clear that this level of information is much more intimate than prior technologies used by law enforcement. This depth of intrusion suggests that customers may have a reasonable expectation of privacy in smart meter data.

There is also a question whether smart meters are in "general public use." (The police must use technology not in general public use for *Kyllo* to apply.)[173] Unfortunately, the Court provided no criterion for making this determination.[174] Several courts applying this test have held that night vision goggles were in general public use.[175] One federal district court reasoned that the goggles were regularly used by the military and police and could be found on the Internet, so were considered in general public use.[176] In 2009, the Department of Energy estimated that 4.75% of all electric meters were smart meters.[177] The department projects that by 2012 approximately 52 million more meters will be installed.[178] With little guidance on this issue, it is uncertain whether this jump in numbers would elevate smart meters into the general public use category.

The means by which data is gathered also differentiates the thermal-imaging in *Kyllo* from smart meters. In *Kyllo*, the police independently gathered the information using the thermal imager; an agent went outside Kyllo's house and used the thermal imager himself.[179] With smart meters, the utility company compiles the information and the police subpoena the company for the data. This difference in means was material in one lower court analyzing access to traditional utility data.[180] It is not clear whether this difference advises against application of *Kyllo* here.

Mosaic and Dragnet Theories

The second factor guiding against the application of the third-party doctrine is composed of two interconnected theories: the mosaic and dragnet theories. The mosaic theory is grounded in the idea that surveillance of the whole of one's activities over a prolonged period is substantially

[170] United States v. Kyllo, 533 U.S. 27, 30 (2001).

[171] *Karo*, 468 U.S. at 705, 709-10.

[172] NIST PRIVACY REPORT, *supra* note 11, at 14 & n.35. It is unclear whether the specificity of the data from the smart meter will directly affect the constitutional analysis. *Kyllo*, 533 U.S. at 37 ("The *Fourth Amendment's* protection of the home has never been tied to measurement of the quality or quantity of information obtained."). With that said, the NIST report maintains that sufficient information about the activities inside of the home are presented to implicate a *Kyllo*, home search analysis.

[173] *Kyllo*, 533 U.S. at 34.

[174] *See* Douglas Adkins, *The Supreme Court Announces a Fourth Amendment "General Public Use" Standard for Emerging Technologies but Fails to Define It:* Kyllo v. United States, 27 DAYTON L. REV. 245 (2002).

[175] *See* United States v. Dellas, 355 F. Supp. 2d 1095, 1107 (N.D. Cal. 2005).

[176] United States v. Vela, 486 F. Supp. 2d 587, 590 (W.D. Tex. 2005).

[177] DEP'T OF ENERGY, SMART GRID SYSTEM REPORT vi (2009), *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SGSRMain_090707_lowres.pdf.

[178] *Id.*

[179] United States v. Kyllo, 533 U.S. 27, 29 (2001).

[180] United States v. McIntyre, 646 F.3d 1107, 1111-12 (8th Cir. 2011).

more invasive than a look at each item in isolation.[181] In the case of smart meters, this is the difference between knowing a person's monthly energy usage, and being able to discern a person's daily activities with considerable accuracy. This theory intersects with dragnet-styled law enforcement techniques in which the police cast a wide surveillance net, taking in a wealth of personal information with the goal of finding criminal activity among the stream of data.

Although the Supreme Court has never formally adopted the mosaic theory, there seems to be a ready-made majority potentially willing to consider it.[182] In *United States v. Jones*, the police used a GPS tracking device to track Jones's movements for almost a month.[183] The majority, led by Justice Scalia, held that attaching a GPS device on a vehicle for the purpose of collecting information constituted a "search" under the Fourth Amendment.[184] The physical intrusion, rather than a *Katz*-type invasion of privacy, was the lynchpin of the decision.[185] Justices Alito and Sotomayor both agreed that this was a search, but on different grounds. Both discussed an adaptation of the mosaic theory as prohibiting police from tracking a person for an extended period of time. Justice Alito, joined by Justices Breyer, Ginsburg, and Kagan, assumed that a short-term search would not violate the Fourth Amendment, but that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[186] Likewise, Justice Sotomayor agreed with this "incisive" observation, noting that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about familial, political, professional, religious, and sexual associations."[187] Both of these comments closely mirror those of the opinion below, which relied on the mosaic theory: "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[188]

Although the *Jones* majority did not embrace the mosaic theory, the concurrences demonstrate that five justices are flirting with the idea. These arguments resemble those made against the unfettered use of smart meter data. With smart meters, police would have a rich source of personal data that reveals far more about a person than traditional analog meters. Understanding a person's daily activities, including what appliances he is using, is a far leap from knowing his monthly energy usage. This is the difference between knowing about a single trip a person took and monitoring his movements over a month-long period. The breadth and granularity of the smart meter data may be seen as warranting application of the mosaic theory and may perhaps find receptive ears on the Court.

Additionally, the dragnet theory may apply to collection of energy usage data. This theory states that surveillance normally permitted under the Fourth Amendment—such as monitoring a person's movements on a public street—becomes an impermissible invasion of privacy when

---

[181] *See* Cent. Intelligence Agency v. Sims, 471 U.S. 159, 178 (1985).

[182] *See* Orin Kerr, VOLOKH CONSPIRACY, What's the Status of the Mosaic Theory After Jones?, http://volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/.

[183] United States v. Jones, 565 U.S. ___, 2 (2012).

[184] *Id.* at 3.

[185] *Id.* at 4.

[186] *Id.* at 13 (Alito, J., concurring in the judgment).

[187] *Id.* at 3 (Sotomayor, J., concurring in the judgment and the opinion).

[188] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

conducted on a prolonged, 24-hour basis.[189] "If such dragnet-type law enforcement practices as respondent envisions should eventually occur," Justice Rehnquist asserted earlier in *United States v. Knotts*, "there will be time enough then to determine whether different constitutional principles may be applicable."[190] Twenty-four hour access to our intimate daily activities, including what appliances we use, when we take our daily shower or bath, eat, and sleep, may push smart meters into the dragnet category.

Coinciding with the mosaic and dragnet theories is the difference in sophistication and the quantity of the data revealed between traditional third-party cases and smart meters. Comparing *Smith* with *Katz* provides insight into this distinction. Pen registers, as used in *Smith*, have "limited capabilities"—they can only record the numbers dialed from a phone.[191] In comparison, in *Katz* the police listened to the contents of Katz's phone call—the actual words spoken.[192] In noting this distinction, it seems the *Smith* Court, in permitting the use of pen registers, intentionally limited its holding to the discrete set of data conveyed—the telephone numbers dialed. Smart meters, to the contrary, have the potential to collect and aggregate precise detail about the activities inside the home. It is more than one packet of data, but reveals minute-by-minute activity, something far more revealing, and arguably more like *Katz* than *Smith*.

Assumption of the Risk—Consent

The third difference between traditional third-party cases and smart meters is the nature of services involved and whether the customer actually assumes the risk or consents to this information being shared with others. Assumption of the risk and consent are the two leading theories supporting the third-party doctrine. In *United States v. Miller*, the customer "assumed the risk" that the bank would turn over the bank records to government authorities.[193] That was a risk he took in doing business with the bank. As to the consent theory, one commentator asked and answered the question as follows: "When does a person's choice to disclose information to a third-party constitute consent to a search? So long as a person knows that they are disclosing information to a third-party, their choice to do so is voluntary and the consent valid."[194]

With banking or telephone services, a customer has the option of transferring his business to another bank or another telephone carrier.[195] To the contrary, because electric utilities are essentially monopolies, the customer cannot simply switch services. The only way to avoid the recordation of his electric usage is to terminate his utility service altogether, an impracticable option in modern society. As one state court has noted:

> Electricity, even more than telephone service, is a "necessary component" of modern life, pervading every aspect of an individual's business and personal life: it heats our homes,

[189] *Id.* at 558.

[190] United States v. Knotts, 460 U.S. 276, 283-84 (1983). Because this statement was not essential to the holding, it was dictum: persuasive, but not binding.

[191] *Smith*, 442 U.S at 741 (citing Katz v. United States, 389 U.S. 347 (1967)).

[192] *Katz*, 389 U.S. at 348.

[193] *Smith*, 442 U.S. at 744 (citing United States v. Miller, 425 U.S. 435 (1976)).

[194] Kerr, *Third-Party Doctrine*, *supra* note 115, at 588.

[195] *Contra Smith*, 442 U.S. at 750 (Marshall, J., dissenting) ("[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of "assuming" the risk in contexts where, as a practical matter, individuals have no realistic alternative.").

> powers our appliances, and lights our nights. A requirement of receiving this service is the disclosure to the power company (and in this case an agent of the state) of one's identity and the amount of electricity being used. The nature of electrical service requires the disclosure of this information, but that disclosure is only for the limited business purpose of obtaining the service.[196]

It is not clear whether assumption of the risk or consent should apply to smart meters. It is reasonable to assume that customers understand utility companies must collect usage data to bill the customer for that usage. Customers receive their statement each month demonstrating this fact. However, most customers are probably not familiar with the sophistication of smart meters and the detailed data sets that can be derived from them. Even if customers are aware their utility usage can be recorded in sub-fifteen minute intervals, a reasonable customer would probably be surprised, if not shocked, to know that data from smart meters can potentially be used to pinpoint the usage of specific appliances. If knowledge of the sophistication of the data is a prerequisite to assumption of the risk or consent, it is difficult to say whether a reasonable customer would understand the privacy implications with this new technology.[197]

Because smart meters are an emerging technology not yet judicially tested, it is difficult to conclude with certainty how they would be handled under the Fourth Amendment. Further, beyond the possible constitutional implications of smart meters, federal communication and privacy statutes may also apply. As noted by Professor Kerr, "in recent decades, legislative privacy rules governing new technologies have proven roughly as privacy protective, and quite often more protective than, parallel Fourth Amendment rules."[198]

Statutory Protection of Smart Meter Data

This section discusses federal statutory protections that may be applicable to the contents of communications sent by a smart meter, independent of the Fourth Amendment, while they are either stored within the smart meter prior to transmission, during transmission, or after they have been delivered to the utility. Three federal laws, the Electronic Communications Privacy Act (ECPA),[199] the Stored Communications Act (SCA),[200] and the Computer Fraud and Abuse Act (CFAA)[201] may be applicable to these situations and are discussed in more detail below.

---

[196] *In re* Restraint of Maxfield, 133 Wn.2d 332, 341 (Wash. 1997); *see also* Balough, *supra* note 63, at 185.

[197] *Cf.* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("*Miller* involved simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue here.").

[198] Kerr, *Fourth Amendment and New Technologies*, *supra* note 114, at 806.

[199] For more detailed information on ECPA, *see* CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

[200] For a more detailed discussion of the SCA, *see* CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

[201] For more detailed information on the CFAA, *see* CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle.

The Electronic Communications Privacy Act (ECPA)

ECPA, enacted in 1986, "addresses the interception of wire, oral and electronic communications."[202] The statute defines electronic communications as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...."[203] Based on the description of the smart meter network provided above,[204] the envisioned transmission of customers' energy usage data by smart meters would seem to fall squarely within the definition of electronic communications under ECPA.

ECPA generally prohibits the interception of electronic communications, but also provides a mechanism for government entities to conduct such surveillance, and a number of other exceptions.[205] Additionally, the statute provides that interception under the procedures and exceptions set forth in ECPA, or pursuant to the Foreign Intelligence Surveillance Act, are the exclusive means for intercepting electronic communications.[206] The unlawful interception of electronic communications in violation of ECPA is generally punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 for individuals and not more than $500,000 for organizations.[207]

Of particular relevance to the immediate discussion is the fact that ECPA permits interception of an electronic communication where a party to the communication has consented to such interception.[208] In the context of a smart meter network that is the subject of this report, it appears that the utility would be a party to all of the communication sent by the smart meters, since it is primarily receiving that information for its own billing purposes. Therefore, if the utility consents to law enforcement's interception of the traffic which is addressed to it, that surveillance would not appear to violate the prohibitions in ECPA.

ECPA also provides a procedural mechanism for law enforcement to conduct surveillance activities for investigative purposes without the consent of any party to the communication. The statute limits the types of criminal cases in which electronic surveillance may be used[209] and requires court orders authorizing electronic surveillance to be supported by probable cause to believe that the target is engaged in criminal activities, that normal investigative techniques are

---

[202] S.Rept. 99-541 at 3.

[203] 18 U.S.C. §2510(12).

[204] *See supra* note 47 and accompanying text (noting that smart meters may use a variety of communications technologies, including fiber optics, wireless networks, satellite, and broadband over power line).

[205] 18 U.S.C. §2516. Exceptions cover things such as interception with the consent of a party to the communication and interception by communication service providers as an incident to providing service.

[206] 18 U.S.C. §2511(2)(f). FISA defines electronic surveillance to include more than the interception of wire, oral, or electronic communications, 50 U.S.C. §1801(f), but places limitations on its definition based upon the location or identity of some or all of the parties to the communications involved.

[207] "Except as provided in (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both." 18 U.S.C. §2511(4)(a).

[208] 18 U.S.C. §2511(2)(c).

[209] The list of covered criminal provisions can be found at 18 U.S.C. §2516(1), and includes offenses such as violence at international airports; animal enterprise terrorism; arson; bribery of public officials and witnesses; unlawful use of explosives; fraud by wire, radio, or television; terrorist attacks against mass transportation; sexual exploitation of children; narcotics production and trafficking; and many others.

The Electronic Communications Privacy Act (ECPA)

ECPA, enacted in 1986, "addresses the interception of wire, oral and electronic communications."[202] The statute defines electronic communications as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...."[203] Based on the description of the smart meter network provided above,[204] the envisioned transmission of customers' energy usage data by smart meters would seem to fall squarely within the definition of electronic communications under ECPA.

ECPA generally prohibits the interception of electronic communications, but also provides a mechanism for government entities to conduct such surveillance, and a number of other exceptions.[205] Additionally, the statute provides that interception under the procedures and exceptions set forth in ECPA, or pursuant to the Foreign Intelligence Surveillance Act, are the exclusive means for intercepting electronic communications.[206] The unlawful interception of electronic communications in violation of ECPA is generally punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 for individuals and not more than $500,000 for organizations.[207]

Of particular relevance to the immediate discussion is the fact that ECPA permits interception of an electronic communication where a party to the communication has consented to such interception.[208] In the context of a smart meter network that is the subject of this report, it appears that the utility would be a party to all of the communication sent by the smart meters, since it is primarily receiving that information for its own billing purposes. Therefore, if the utility consents to law enforcement's interception of the traffic which is addressed to it, that surveillance would not appear to violate the prohibitions in ECPA.

ECPA also provides a procedural mechanism for law enforcement to conduct surveillance activities for investigative purposes without the consent of any party to the communication. The statute limits the types of criminal cases in which electronic surveillance may be used[209] and requires court orders authorizing electronic surveillance to be supported by probable cause to believe that the target is engaged in criminal activities, that normal investigative techniques are

---

[202] S.Rept. 99-541 at 3.

[203] 18 U.S.C. §2510(12).

[204] *See supra* note 47 and accompanying text (noting that smart meters may use a variety of communications technologies, including fiber optics, wireless networks, satellite, and broadband over power line).

[205] 18 U.S.C. §2516. Exceptions cover things such as interception with the consent of a party to the communication and interception by communication service providers as an incident to providing service.

[206] 18 U.S.C. §2511(2)(f). FISA defines electronic surveillance to include more than the interception of wire, oral, or electronic communications, 50 U.S.C. §1801(f), but places limitations on its definition based upon the location or identity of some or all of the parties to the communications involved.

[207] "Except as provided in (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both." 18 U.S.C. §2511(4)(a).

[208] 18 U.S.C. §2511(2)(c).

[209] The list of covered criminal provisions can be found at 18 U.S.C. §2516(1), and includes offenses such as violence at international airports; animal enterprise terrorism; arson; bribery of public officials and witnesses; unlawful use of explosives; fraud by wire, radio, or television; terrorist attacks against mass transportation; sexual exploitation of children; narcotics production and trafficking; and many others.

insufficient, and that the facilities that are the subject of surveillance will be used by the target.[210] It also limits the use and dissemination of information intercepted.[211] In addition, when an interception order expires, authorities must notify those whose communications have been intercepted.[212] Law enforcement may also conduct electronic surveillance when acting in an emergency situation pending issuance of a court order.[213]

The government may also conduct electronic surveillance under the authority of the Foreign Intelligence Surveillance Act (FISA). FISA governs the gathering of information about foreign powers, including international terrorist organizations, and agents of foreign powers.[214] Although it is often discussed in relation to the prevention of terrorism, it applies to the gathering of foreign intelligence information for other purposes.[215] Although some exceptions apply, such as for emergency situations,[216] the government typically must obtain a court order, supported by probable cause, from the Foreign Intelligence Surveillance Court (FISC), a neutral judicial decision maker, in order to conduct electronic surveillance pursuant to FISA.[217]

The Stored Communications Act (SCA)

The SCA was enacted in 1986 as Title II of the Electronic Communications Privacy Act (ECPA),[218] to "address[] access to stored wire and electronic communications and transactional records."[219] The SCA prohibits unauthorized persons from accessing a facility through which an *electronic communication service* (ECS) is provided; or obtaining, altering, or preventing access to an electronic communication while it is in *electronic storage* in an ECS.[220] The SCA also limits the circumstances in which providers of ECS or a *remote computing service* (RCS) may disclose information that they carry or maintain.[221] The SCA also provides a mechanism by which law enforcement may compel the disclosure of stored communications.[222]

The terms "electronic communication service," "remote computing services," and "electronic storage" are all specifically defined by the SCA. As described above, the SCA applies only to providers of either an ECS or an RCS; stored communications held by other types of entities are not protected by the SCA. Therefore, in order to determine whether the SCA would protect stored information collected by a smart meter, this report will first examine whether a utility's deployment of a smart meter network falls within the definition of an ECS or an RCS and then

[210] 18 U.S.C. §§2516, 2518(3).

[211] 18 U.S.C. §2517.

[212] 18 U.S.C. §2518(8).

[213] 18 U.S.C. §2518(7).

[214] *See* 50 U.S.C. §1801(a) (definition of "foreign power").

[215] For example, it extends to the collection of information necessary for the conduct of foreign affairs. *See* 50 U.S.C. §1801(e) (definition of "foreign intelligence information").

[216] 50 U.S.C. §1805(e).

[217] 50 U.S.C. §§1801-1808. FISA authorizes electronic surveillance without a FISA order in specified instances involving communications between foreign powers. 50 U.S.C. §1802.

[218] P.L. 99-508.

[219] S.Rept. 99-541 at 3.

[220] 18 U.S.C. §2701(a). Unauthorized access includes exceeding an authorization to use the facility. *Id.*

[221] 18 U.S.C. §2702.

[222] 18 U.S.C. §2703.

Doc. 4

American Academy of Environmental Medicine

6505 E Central • Ste 296 • Wichita, KS 67206
Tel: (316) 684-5500 • Fax: (316) 684-5709
www.aaemonline.org

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

Doc. 5

MSMA Maryland Smart Meter Awareness

education and advocacy working to protect public health

Dr. David Carpenter's Letter to BG&E

by Mary on February 21, 2012 in General Info, Health

21 February 2012

Re: Smart Meters and Baltimore Gas & Electric

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 (www.bioinitiative.org), a comprehensive review of the literature on this subject. The public health chapter from this report was subsequently published in a peer reviewed journal. 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.

The statement released by BG&E that "Many studies conducted across the country have found that smart meters do not pose a health risk" is totally false. There have been no studies of the health effects of smart meters to my knowledge. The statements about the Food and Drug Administration and World Health Organization are equally untrue. 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 in a state that already has too much.
2. When a 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, until more is know about health consequences of chronic RF exposure. 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. The BG&E letters states "The meter that we will install at customers' homes will transmit for less than 15 minutes each day on average." This is probably true, but is a deceptive statement, because while transmission of data to the utility occurs for short periods of time, 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. Their use 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.

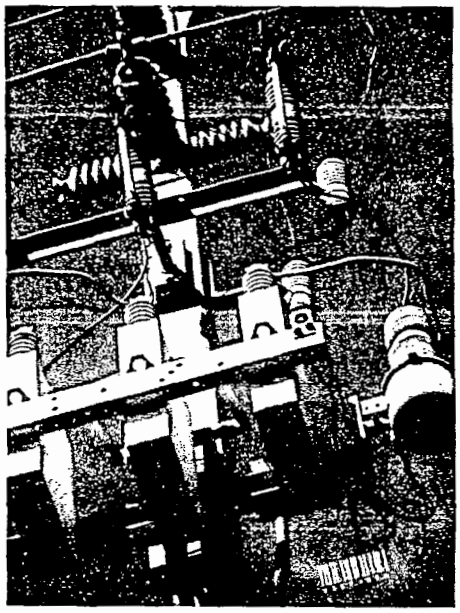
Yours sincerely,

Doc. 6

Ways to Reduce Exposure to Dirty Electricity

GREEN LIVING, HEALTHY LIVING

by Sarah TheHealthyHomeEconomist March 23, 2014



Electricity was originally intended as a "clean" and safe source of power for homes and businesses through standard usage of the steady electrical frequency of 60 oscillations per second, or 60 Hertz (Hz).

Modern energy efficient devices, electronics, and other reasons such as earth currents can cause significant deviance from the 60 Hz frequency, however, and this pulsed exposure to spiking and unsafe frequencies of electromagnetic radiation (EMFs) on overloaded wires is what has become known as **"dirty electricity".**

Exposure to dirty electricity has the potential to cause and exacerbate existing health problems in some people. It is not something that can be smelled, touched, seen, or felt and yet it is very real and very problematic for those who experience it on a daily basis.

The health effects of dirty electricity were first identified as early as the 1950's in rural areas when the behavior and feeding patterns of animals were negatively affected by stray voltage caused by poor grounding and lack of utility infrastructure.

In humans, symptoms of exposure to dirty electricity can include:

Headaches
Difficulty sleeping
Body aches and pains
Ringing in the ears (tinnitus)
Chronic Fatigue Syndrome
Worsening of symptoms from multiple sclerosis or ALS (Lou Gehrig's Disease)

In Sweden, sensitivity to dirty electricity is a recognized disability affecting approximately 3% of the population. In Switzerland, a survey of doctors concluded that 5% of symptoms in patients could be traced to dirty electricity exposure.

Ways To Reduce Your Exposure Today

While the concept of dirty electricity is a complex one that practically requires a degree in Physics to fully understand, ways to reduce your exposure are simple and easy to implement.

1. **Get rid of all the fluorescent light bulbs.** Compact fluorescent light bulbs or CFLs, as they are known, have a very large EMF field compared with simple incandescent light bulbs. CFLs also produce a lot of dirty electricity. Getting rid of them and all sources of fluorescent lighting in your home and business will reduce your exposure to dirty electricity immediately.

2. **Replace all dimmer switches with simple on/off switches.** Dimmer switches produce a lot of dirty electricity! Replace them with simple on/off switches or if that is not in the budget, just leave them off all the time.
3. **Turn off your wireless router at night**. While getting rid of exposure to all wireless communications is futile in this day and age when it is literally everywhere, you can at least give your body a rest at night while you sleep by turning them off in your home.
4. **Make sure your home does not use a Smart Meter.** Power companies all over the United States are installing smart meters to simplify the meter reading process. Call your local power company and find out if you have already gotten one and if so, make sure to opt out and go back to the analog meters.

I initially thought our home had a Smart Meter, but after investigating, discovered to my great relief that the automated meters in our area were not Smart Meters and were one way communication devices which allowed meter readers to drive down our street and pick up a weak radio signal and thereby read the meter without entering a person's property. They were not two-way Smart Meters constantly pulsing and sending information to the power company about our electrical usage.

> The American Academy of Environmental Medicine recently adopted a resolution which formally opposes the installation of Smart Meters in homes and schools "***based on a scientific assessment of the current medical literature. Chronic exposure to wireless radiofrequency radiation is a preventable environmental hazard that is sufficiently well documented to warrant immediate preventative public health action.***"

Dirty electricity was identified as a possible carcinogen in 1999 by the US National Toxicology Program. What's more, existing safety limited for pulsing radio frequency are insufficient to maintain public health according to the Radiofrequency Interagency Working Group.

More Ways to Protect Youself From Dirty Electricity

If you feel that dirty electricity is seriously impacting your health and want to know more, please **click here** to investigate information on a line of Earthing products that can protect you in your home or business.

Sarah, The Healthy Home Economist

More Information

Harvard Medical Doctor Warns Against Smart Meters

The Health Hazards of Wireless Baby Monitors

Sources:

Wise Traditions 2011 Conference, *Dirty Electricity*, Jules Klapper

Swiss EMF Study

What Causes Dirty Electricity?

Picture Credit

March 16, 2015 Doc. 7 Ronald M. Powell, Ph.D.

What does it mean to accept a Wireless Smart Meter on your home or business?

For Your Property Rights

- It means that you accept the right of your electric power company to mount, on or inside your home or your business, a meter that acts much like a compact cell tower, without informing you in advance of its full capabilities and associated risks, without your prior approval, and without compensating you for using your property for purposes well beyond metering your electricity.

  A Wireless Smart Meter measures the electrical energy consumed by your home or business with very fine time resolution, determined by your electric power company, and broadcasts your data over the air using a radiofrequency/microwave transmitter/receiver. The Wireless Smart Meters, in your neighborhood, form a wireless Mesh Network. Each meter not only transmits its own data, but also receives and retransmits (relays) the data of other meters, much like cell towers do. The purpose is to assure that all data reach a community-based transmitter/receiver, called a Collection Point, which then relays the data back to the electric power company. According to a document ordered by a California Court, each Wireless Smart Meter broadcasts an average of 10,000 bursts of radiation per day, up to a maximum of 190,000 bursts of radiation per day. Together, the Wireless Smart Meters in a community blanket that community with millions to billions of bursts of radiation every day, leaving no location unexposed. Each Wireless Smart Meter also contains a second radiofrequency/microwave transmitter/receiver. It forms a Home Area Network with your Wireless Smart Appliances (just now emerging) so that their identity and your use of them can be monitored by the company.

- It means that you accept that other utilities may claim a similar right, based on equal treatment with the electric utilities, to use your home or business to mount their wireless equipment under the same terms, that is, without informing you fully of the implications, etc. Those utilities include the gas, water, telephone, and internet service companies. In sum, you accept the fact that your home is no longer your castle, but instead is now the castle of your utility companies.

For Your Costs

- It means that the benefits that you are currently receiving, or expect to receive, from the Wireless Smart Meter System are so obvious and so great that you agree to pay for the cost of the Wireless Smart Meter System without even knowing what that cost is. And you may never know what that cost is because there is no requirement in place that the cost be revealed to you. Rather, that cost may be buried obscurely in other charges on your bill.

- It means that you have such trust in the integrity and the technical capability of your electric power company that you are willing to forfeit your ability to verify the accuracy of your monthly bill. Instead of insisting on the traditional analog mechanical meter, which cannot be interfered with by anyone, you agree to accept a Wireless Smart Meter that can be reprogrammed remotely and invisibly by wireless signals sent by your electric power company, without informing you and with unknown consequences for your monthly bill.

For Your Health

- It means that you accept the assurances of your electric power company that the Wireless Smart Meter System is safe for your health. That is, you trust your power company to know more about your health than your doctor, and more about the impact of radiofrequency/microwave radiation on your health than the entire international biomedical research community. That community has published thousands of journal articles on this subject and has been sounding the alarm.

- It means that you agree to volunteer yourself and your family for an uncontrolled medical experiment, mandated by the Maryland State Government through the Maryland Public Service Commission, to demonstrate what is already known to the international biomedical research community, that radiofrequency/microwave radiation is harmful to human health.

- In sum, it means that the benefits to you from your Wireless Smart Meter are so obvious and so great that they are more important to you than your own health, the health of your spouse, the health of your children, and the health of your friends, your colleagues, and your community.

For Your Privacy

- It means that you freely relinquish your right to privacy, because you believe the claims of your electric power company, that it must have, not just the one reading per month required to bill you for electricity, but rather as much information as it can gather, every day --

  - about the activities in your home or your business, as revealed by your detailed patterns of electricity consumption, such as when you get up, when you go to bed, when your children get home from school, and when you are away from your home or business

  - about the identity of every Wireless Smart Appliance in your home or business, and what use you make of all of them.

    As noted above, each Wireless Smart Meter contains a second radiofrequency/microwave transmitter/receiver that forms a Home Area Network (HAN) with your Wireless Smart Appliances (just now emerging). You have no control over either of the two transmitters/receivers in a Wireless Smart Meter.

- In sum, you accept that your electric power company has the right to install a surveillance device of unprecedented nature on, or inside, your home or business and to use that device for any purposes that it wishes, without making those purposes known to you or gaining your approval.

For Your Cyber Security

- It means that you accept that the electrical power to your home or business can be interrupted, intentionally or accidentally, using a new capability – the inclusion in each Wireless Smart Meter of a shut-down switch. That switch can be triggered wirelessly and remotely, either by your electric power company or by successful hackers, to turn off your electrical power, without anyone having to appear on your property, and for any reason, including disciplining you over a billing dispute.

Doc. 8

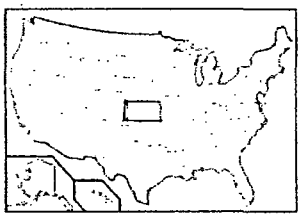
Is Your Home's Energy Meter Spying On You?

22 April 2014 at 3:57pm | 23,667 hits

"Imagine if AT&T set out to install FCC-regulated cell network repeaters on everyone's rooftops — all homes in the US — without permission or compensation. That they just went out and did it, in the interest of improving their network coverage, and improving their for-profit bottom line," Josh del Sol, a researcher and director of a documentary titled "Take Back Your Power," said to FoxNews.com. "Pretty ridiculous, right? This is theft, and if they were a government agency it would be an obvious violation of the latter part of the Fifth Amendment in addition to the Fourth."

"How, pray tell, are utilities able to get away with what amounts to the exact same thing," he added. "They [power utilities] would say that 'they have easement,' but does this easement include the right to broadcast an FCC-regulated microwave transmitter on your home, taking your private property to do so, for their benefit, and without your consent?"

Doc. 9



Kansas

Legislative activities

While the Kansas Legislature has not yet approved any laws specific with smart grid they have allowed for solar easement provision that allow parties to voluntarily enter into solar easement contracts. In 2009 it also established net metering for customers of investor-owned utilities in Kansas. (HB 2369) [2, 3]

Regulatory activities

Kansas Corporation Commission worked with residential and business demand side management as early as 1991 and thermal storage as early as 1992 and dealt with real-time pricing in 1999 Time-of-Use rates by 2000 for business customers and 2007 for residential customers. Prior to 2010 interruptible accounts were available to business customers as an alternative method of load management. [4, 5]

"In August 2007, the Kansas Corporation Commission decided not to adopt PURPA Standard 14 ("Time-Based Metering and Communications") as enacted in EPACT 2005. The Commission said that it should not mandate smart metering as that would be a "one size fits all" approach and could, as a result, disadvantage some utilities. Instead, the Commission encouraged voluntary pilot programs as the best vehicle for deploying smarting metering and TOU rates. Nonetheless, according to the August 2007 Order, "The Commission strongly encourages the development and implementation of pilot programs introducing smart metering and time-based rates, and time-based technology."" [1]

Demand side management consists of load control of air conditioning systems that can receive the companies signal to cycle off during periods of peak usage.

Thermal storage is determined on a case by case basis by the company.

The real-time pricing is based on the company's marginal cost-based prices and provided to the customer eight hours in advance of the day the power flows.

Time-of-use or time of day rates break the cost for electricity into periods on a seasonal basis and sections within on-peak and off-peak for pricing.

Load management includes interruptible service schedules which offer a reduced cost for a company's ability to shed load for up to 4 hours a from June through August.

Utilities and Rate Schedules

Empire District Electric Company
- Empire District Electric Company Rates

Kansas City Power & Light
- Kansas City Power & Light Tariffs

Midwest Energy, Inc.
- Midwest Energy, Inc. Rates

See the National Rural Electric Cooperative Association (NRECA) for information on consumer-owned Cooperatives: http://www.nreca.org/members/MemberDirectory/Pages/default.aspx

State-Level Incentives

Kansas has a renewable energy property tax exemption. Kansas City Power & Light also has an energy optimizer program to install a free Honeywell programmable thermostat capable of receiving signals to reduce air conditioning loads during high

Virginia
Washington
West Virginia
Wisconsin
Wyoming

demand periods.

More information can be found in the Database of State Incentives for Renewables & Efficiency (DSIRE):
http://www.dsireusa.org/incentives/index.cfm?re=1&ee=1&spv=0&st=0&srp=1&state=KS

Additional Resources

State Energy Office:
- Kansas Corporation Commission State Energy Office

State Authority Dealing with Energy Regulation:
- Kansas Corporation Commission
- Docket Search: http://www.kcc.state.ks.us/docket/docket.htm

Kansas Statutes

Database of State Incentives for Renewables & Efficiency (DSIRE): http://www.dsireusa.org/incentives/index.cfm?re=1&ee=1&spv=0&st=0&srp=1&state=KS

References

[1] Demand Response and Smart Metering Policy Actions Since the Energy Policy Act of 2005: A Summary for State Officials,

Prepared by the U.S. Demand Response Coordinating Committee for The National Council on Electricity Policy, Fall 2008.
URL: http://www.oe.energy.gov/DocumentsandMedia/NCEP_Demand_Response_1208.pdf
[2] Database of State Incentives for Renewables & Efficiency, Kansas – Net metering, 05/11/2010. URL:
http://www.dsireusa.org/incentives/incentive.cfm?Incentive_Code=KS08R&re=1&ee=1
[3] Database of State Incentives for Renewables & Efficiency, Kansas Solar Easements, 12/14/2009. URL:
http://www.dsireusa.org/incentives/incentive.cfm?Incentive_Code=KS01R&re=1&ee=1
[4] Midwest Energy, Inc., Electric Terms, Conditions and Rates filed with the Kansas Corporation Commission. URL:
http://www.mwenergy.com/elecrate.aspx
[5] KCP&L, Kansas Tariffs. URL: http://www.kcpl.com/my-bill/for-home/rate-information/ks/detailed-tariffs

Doc. 10

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).".

Doc. 11

United States

Overview

The United States' Smart Grid policy is primarily directed by the central federal government through the guidance and authority of various acts of congress which are implemented by the Federal Smart Grid Task Force led by the Department of Energy (DoE) and staffed by:

- The Department of Energy
- The Federal Energy Regulatory Commission
- The Department of Commerce
- The Environmental Protection Agency
- The Department of Homeland Security
- The Department of Agriculture
- The Department of Defense
- The Federal Communications Commission
- The Department of State

Governmental/Industry Energy Organizations

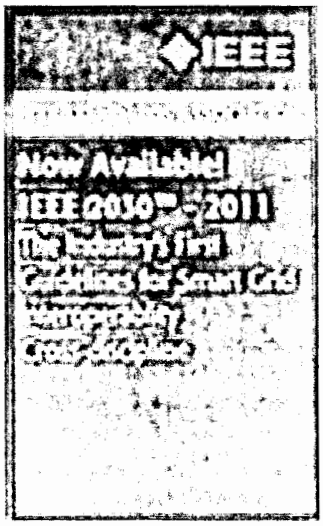
In its key role as the implementer of national Smart Grid policy the DoE has created a partnership industry and quasi governmental professional electrical power organizations in an attempt to integrate a comprehensive set of subject matter experts in developing a roadmap and vision for the Smart Grid. This group includes the GridWise Alliance, The Electric Power Research Institute (EPRI), The Galvin Electricity Initiative, The Institute of Electrical and Electronics Engineers (IEEE), Federal Energy Regulatory Commission (FERC), as well as a host of others

Although the federal government is responsible for the nation's Smart Grid policy via its national energy policy some aspects of that policy fall outside of the federal government's jurisdictional boundaries and are the responsibility of a vast and complex web of state, regional, local and municipal governing authorities. Together these groups are pooling their resources to collaboratively develop the Smart Grid.

Key Legislation

The Energy Independence Act of 2007 (EISA)

The first of the Federal government laws concerning the Smart grid was enacted by Congress in 2007 and is entitled **The Energy Independence Act of 2007**, or (EISA). EISA's primary focus from a Smart Grid perspective is found in Title 13 of the law which is directed towards the goal of modernizing the nation's electricity transmission and distribution system. To this goal 10 topic areas are addressed in the law, they include:



1. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
2. The dynamic optimization of grid operations and resources, with full cyber-security.
3. The Deployment and integration of distributed resources and generation, including renewable resources.
4. Development and incorporation of demand response, demand-side resources, and energy-efficiency resources.
5. Deployment of "smart" technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.
6. Integration of "smart" appliances and consumer devices.
7. Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning.
8. Provision to consumers of timely information and control options.
9. Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.
0. The Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices and services.

In 2008, in support of EISA, the DoE through its Office of Electricity Delivery and Energy Reliability (OE) produced a visionary report entitled **Smart Grid: an introduction**. This report outlines a national vision of the Smart Grid and the positioning of the Smart Grid's primary stakeholder groups. One of the key phrases from the report describes the Smart Grid in a futuristic perspective when it states "Think of the Smart Grid as the internet brought to our electric system" . The report goes onto to outlines 6 Key objectives for Smart Grid development as:

1. Ensuring the Electrical Grid's reliability to degrees never before possible.
2. Maintaining the Electrical Grid's affordability.
3. Reinforcing the United State's global competitiveness.
4. Fully accommodating renewable and traditional energy sources.
5. Potentially reducing the United State's carbon footprint and Green House Gases (GHG).
6. Introducing advancements and efficiencies to the Electrical Grid yet to be envisioned.

Finally the OE Smart Grid report identifies 6 strategic opportunities from which the United States wishes to use the Smart Grid to realize:

1. Enablement of nationwide use of plug-in hybrid electric vehicles
2. Deployment of large-scale energy storage
3. Seamless integration of renewable energy sources
4. Flexible consumer choice regarding electrical energy source and consumption
5. Exploit the use of green building standards to help lessen electrical load requirements
6. Making use of solar energy 24 hours a day

American Recovery and Reinvestment Act of 2009 (ARRA)
The next important piece of legislation containing funding and policy direction concerning the Smart Grid was passed by congress and enacted into law in 2009. Known as the **American Recovery and Reinvestment Act of 2009** (ARRA) the law extended Smart Grid efforts by funding activities such as:

1. **Smart Grid Investment Grants**which serves as catalyst and seed programs to enable commercial developments in Smart Grid technologies in the fields of:
   - Retail and Wholesale electrical markets
   - Central and Distributed electric generation and storage options
   - New products, services, and markets

- Power quality diversification to consumers
- Asset utilization and operating efficiency of the electric power system
- System disturbance prediction and analysis
- Resiliency preparedness to attack and natural disasters

2. The Smart Grid Demonstration Program funding initiative of ARRA was designed to enable the validation and verification of Smart Grid technologies in respect to cost versus benefits, the ability to be replicated, the ability to be piloted and implemented, and the ability to produce new business models. Demonstration program funding is focused on Smart Grid technologies which:
   - Enable customers, electricity distributors, and electricity generators to change their behavior in order to reduce electric power system demands and costs
   - Increase energy efficiency
   - Match electricity demand and resources
   - Increase grid reliability.

   The demonstration program is particularly interested in funding those projects that are focused on energy storage on a macro or grid-scale; especially those that can:
   - Enable renewable energy resources to be controlled by grid operators in more manageable ways.
   - Balance microgrids to achieve a good match between generation and load.
   - Provide frequency regulation to maintain the balance between the network's load and power generation.
   - Enable deferment of transmission and distribution investments.
   - Provide a more reliable power supply for high-tech industrial facilities.
3. **The Smart Grid Workforce Training and Development program** is another important part of the ARRA Act funding of the Smart Grid as it helps provide for the training and education of a new generation of electrical power professionals directly associated with Smart Grid technologies. Through universities, community colleges, manufacturers and utilities this program shall provide funding to train 30,000 people by: developing and enhancing workforce training programs for the electrical power sector and by helping the development of a series of Smart Grid workforce training programs.
4. **The Smart Grid Maturity Model**- As part of the ARRA funding of the Smart Grid the federal government is funding the building of a management model to help utilities track progress towards Smart Grid technologies implementation through the analysis of 8 main criteria:
   - Strategy, management, and regulatory
   - Organization and structure
   - Grid operations
   - Work and asset management
   - Technology
   - Customer
   - Value chain integration
   - Societal and environmental

Other Notable laws or Actions

American Clean Energy and Security Act of 2009 H.R.2454

- Section 121 - Requires utilities to develop plans to support electric vehicle infrastructure and establish protocols for integration with smart grid systems.
- Sections 142 and 143 - Provides for assessment and inclusion of Smart Grid capability in Energy Star and Energy Guide Ratings
- Section 144 - Requires the FERC to coordinate a national program to reduce peak electric

demand for load-serving electric utilities with peak loads in excess of 250 megawatts

- Section 145 - Reauthorize the joint DOE/EPA efficiency public information initiative and expands the initiative to include information on smart grid technologies, practices, and benefits.
- Section 146 - Inclusion of Smart Grid Features in Appliance Rebate Program

Current Major Projects

Listed below are sites which contain listing of major projects underway within discreet category headings

Advanced Metering Infrastructure- Various projects nation wide
Customer Systems- Various projects nation wide
Electric Distributions Systems- Various projects nation wide
Electric Transmission Systems- Various projects nation wide
Equipment Manufacturing- Various projects nation wide
Integrated and Crosscutting Systems- Various projects nation wide
Energy Storage Demonstration Projects- Various projects nation wide
Regional Demonstration Projects- Various projects nation wide

Perfect Power- Microgrid Technologies
Perfect Power is a research project being conducted at Illinois Institute of Technology (ITT) in conjunction with the Galvin Electricity Initiative and the United States Department of Energy (DOE) to develop a comprehensive solution to the loss in time and money lost to power outages. In collaboration with S&C Electric, Endurant Energy, and ComEd, the Perfect Power System project will incorporate smart microgrid technologies into a loop system to produce redundant electricity in an effort to eliminate costly outages, minimize power disturbances, moderate an ever-growing demand, and curb greenhouse gas emissions.

The Perfect Power System will include the following elements:

- Self-sustaining electricity infrastructure
- An intelligent distribution system and system controllers
- Onsite electricity production
- Demand-response capability
- Sustainable energy systems and green buildings/complexes
- Technology-ready infrastructure

Distribution Management System (DMS) - Management of Distributed Generation (DG), Energy Storage and Demand Response technologies

Project's objective is to develop and demonstrate a Distribution Management System (DMS) that aggregates distributed generation (DG), energy storage, and demand response technologies in a distribution system to achieve both distribution and transmission level benefits. Ideally, the application of these technologies would increase system reliability and improve power quality along with reducing costs to both the utility and its customers.

An integrated distribution system control and communications architecture that combines and coordinates the following:

- Advanced metering infrastructure (AMI) as a home portal for direct demand response signals, as well as structured electricity rates
- Building automation to implement energy conservation and demand response
- Meter information gathering, mining, and reporting functions in the distribution system control platform
- Energy management, implementing optimal dispatch of DG, storage, and loads on the feeder
- Tieline dispatch controls, allowing tight dynamic control of the power exchange between the

distribution system and the transmission grid

- Integrated voltage/VAR control to minimize losses and control the voltage profile

Contact
IEEE Smart Grid
445 Hoes Lane
Piscataway, New Jersey 08854
Contact Program Manager
Feedback

Home
Smart Grid Brand Toolkit
Smart Grid Clearinghouse
Smart Grid Jobs
Spectrum Magazine
Tech Nav

Doc. 12

OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

FEDERAL SMART GRID TASK FORCE

Electricity Advisory Committee
Technology Development
Smart Grid
Demand Response
Federal Smart Grid Task Force
Distributed Energy
Microgrids
Recovery Act Interoperability
Recovery Act SGDP
Recovery Act SGIG
Recovery Act Workforce Training
Interactive Grid
Smart Grid Primer
Smart Grid Request for Information and Public Comments
Energy Delivery Systems Cybersecurity
Energy Storage
Power Electronics

TASK FORCE BACKGROUND

The Federal Smart Grid Task Force was established under Title XIII of the Energy Independence and Security Act of 2007 (EISA) and includes experts from eleven Federal agencies. The Department of Energy is represented by the Office of Electricity Delivery and Energy Reliability which is the Task Force lead, as well as the Office of Energy Efficiency and Renewable Energy and the National Energy Technology Laboratory.

TASK FORCE MISSION

The mission of the Task Force is to ensure awareness, coordination and integration of the diverse activities of the Federal Government related to smart grid technologies, practices, and services. The Task Force will collaborate with DOE's Electricity Advisory Committee and other relevant Federal agencies and programs.

TASK FORCE MEMBERS

- Department of Energy (DOE)
  - Office of Electricity Delivery and Energy Reliability
  - Office of Energy Efficiency and Renewable Energy (EERE)
  - National Energy Technology Laboratory (NETL)
- U.S. Department of Commerce (DOC)
- International Trade Administration (ITA)
- National Institute of Standards and Technology (NIST)
- Federal Energy Regulatory Commission (FERC)
- U.S. Department of Homeland Security (DHS) – Science and Technology Directorate
- U.S. Department of State
- U.S. Environmental Protection Agency (EPA)
- U.S. Department of Agriculture (USDA) – Rural Utility Service (RUS)
- Department of Defense (DOD)
- Federal Communications Commission (FCC)
- National Oceanic and Atmospheric Administration (NOAA)
- U.S. Trade and Development Agency (USTDA)

RELATED LINKS

Energy Independence and Security Act of 2007 Title XIII - Smart Grid

1500 SW Arrowhead Road
Topeka, KS 66604-4027

Kansas
Corporation Commission

Phone: 785-271-3100
Fax: 785-271-3354
http://kcc.ks.gov/

Shari Feist Albrecht, Chair
Jay Scott Emler, Commissioner
Pat Apple, Commissioner

Sam Brownback, Governor

MEMORANDUM
LEGAL DIVISION

TO: Chair Shari Feist Albrecht
Commissioner Jay Scott Emler
Commissioner Pat Apple

FROM: Samuel Feather, Litigation Counsel

DATE: August 5, 2015

SUBJECT: 15-KCPE-474-COM
In the Matter of the Complaint Against Kansas City Power & Light Company by Keith S. Carpenter

EXECUTIVE SUMMARY:

Keith S. Carpenter (Complainant) filed a Formal Complaint[1] on April 13, 2015. On April 30, 2015, the Kansas Corporation Commission entered an Order Adopting Staff's Memorandum (Order), finding that the Complainant has not satisfied the procedural requirements for filing formal complaints as detailed in K.A.R. 82-1-220. The Order gave Complainant 30 days to correct the procedural deficiencies and submit an amended complaint. On May 18, 2015, Complainant filed an Amended Formal Complaint[2] wherein Complainant cites to the 4th and 5th Amendments of the U.S. Constitution. The Kansas Corporation Commission lacks the jurisdiction to rule on issues relating to the U.S. Constitution. Therefore, Legal Staff recommends the Commission dismiss the Amended Complaint as it relates to the Complainant's Constitutional arguments. However, Legal Staff recommends the Commission accept the Amended Complaint as it relates to the Complainant's health and safety argument and forward the Complaint to KCP&L. Furthermore, Legal Staff notes that the Commission currently has an open investigation regarding the health risks posed by smart meters and recommends the Commission join the Amended Complaint to its ongoing investigation.

BACKGROUND & ANALYSIS:

On May 18, 2015, the Complainant filed an Amended Formal Complaint against KCP&L due to KCP&L's attempted installation of an AMI meter at Complainant's address.[3] The Amended Complaint raises two arguments. First, the Complainant alleges that the installation of the smart meter is an invasion of the Complainant's privacy and is thusly

[1] Complaint Against Kansas City Power & Light by Keith S. Carpenter, April 13, 2015 (Formal Complaint).
[2] Amended Formal Complaint Against Kansas City Power & Light by Keith S. Carpenter, May 18, 2015 (Amended Complaint).
[3] *See Amended Complaint.*

an unlawful violation of the Complainant's 4th and 5th amendment rights as granted by the U.S. Constitution. Second, the Complaint alleges that smart meters create a serious health risk due to EMF radiation. Upon the filing of a formal complaint, the Commission must determine "whether or not the allegations, if true, would establish a prime [sic] facie case for action by the commission and whether or not the formal complaint conforms to [the Commission's] regulations."[4]

K.A.R. 82-1-220(b) requires formal complaints to satisfy three procedural requirements:

> (1) Fully and completely advise each respondent and the commission as to the provisions of law or the regulations or orders of the commission that have been or are being violated by the acts or omissions complained of, or that will be violated by a continuance of acts or omissions;
>
> (2) set forth concisely and in plain language the facts claimed by the complainant to constitute the violations; and
>
> (3) state the relief sought by the complainant.

Invasion of Privacy Argument
The Amended Complaint cites to the 4th and 5th Amendments of the U.S. Constitution, in support of the invasion of privacy complaint. The Kansas Corporation Commission lacks the jurisdiction to issue rulings pertaining to the constitutional questions[5] and thus lacks the jurisdiction to hear the privacy aspect of the Complaint. Thus this argument in the Amended Complaint should be dismissed.

Health and Safety Argument
The Amended Complaint states, "... that smart meters can create a serious health risk" and provides attached documentation on the health impacts of EMF. The concise narrative and attached documentation provide notice to KCP&L and the Commission that the Complaint is alleging that KCP&L's installation of smart meters creates a risk to public safety and thus complies with procedural requirement (2).

The Amended Complaint requests that KCP&L 1) allow customers to opt out of having smart meters with no additional charges, 2) install only conventional non communicating analog meters for customers who choose to opt out of receiving smart meters.[6] The Amended Complaint clearly states the relief sought and thus complies with procedural requirement (3).

The Amended Complaint does not expressly cite to any law, regulation, or order in support of its health and safety argument and thus does not comply with procedural requirement (1). However, the Commission has the discretion to waive its regulations for

---

[4] K.A.R. 82-1-220(c).
[5] *Kaufman v. State Dep't of Soc. & Rehabilitative Servs.*, 248 Kan. 951, 954, 811 P.2d 876, 879 (1991).
[6] The relief sought by the Amended Complaint would broadly apply to customers who have already had a smart meter installed on their home and those who have not yet had a smart meter installed.

good cause if it is in the public interest to do so unless otherwise required by law.[7] The detailed requirements of the Commission's regulation are more restrictive than that ordinarily required by law.[8]

The Commission has been given full power, authority and jurisdiction to supervise and control the electric public utilities doing business in Kansas.[9] Furthermore, the Commission is granted authority over each electric public utility's equipment, manner of conduct, and management to protect public safety.[10] Legal Staff believes that the Amended Complaint provides sufficient detail to notify KCP&L and the Commission that the Complainant is asking the Commission to exercise its authority to protect public safety from the alleged harm of EMF. The Commission's Technical Staff currently is investigating this issue in the consolidated Docket Nos. 15-KCPE-265-COM and 15-WSEE-211-COM.

The public interest is not served by dismissing the complaints of customers without legal representation for deficiencies of procedural requirements that are more stringent than that required by Kansas law.[11] Thus the Amended Complaint substantially complies with the procedural requirements of K.A.R. 82-1-220 and the Commission should waive K.A.R. 82-1-220(b)(1) for good cause.

This memorandum makes no recommendation regarding the *validity or veracity* of the Complainant's claims.

RECOMMENDATION:

Legal Staff recommends the Commission find:

- The Complainant's privacy argument based upon alleged violations of the 4th and 5th amendment should be dismissed for lack of jurisdiction;
- The Complainant's health and safety argument substantially complies with the procedural requirements of K.A.R. 82-1-220;
- K.A.R. 82-1-220(b)(1) should be waived for good cause.
- The Amended Complaint establishes a *prima facie* case for Commission action;
- The Amended Complaint should be served upon KCP&L;
- Staff should be directed to investigate this matter and submit a Report and Recommendation to the Commission;

---

[7] K.A.R. 82-1-202.

[8] *See,* K.S.A. 66-101e, (the specific language of the statute allows for a complaint based solely on an unreasonable practice, K.A.R. 82-1-220(b) places the additional burden of alleging a specific violation of law, tariff or order which is not required by statute and may place an undue burden on complainants not represented by legal counsel); *See also, Boydston v. Bd. of Regents for State of Kan.*, 242 Kan. 94, 99, 744 P.2d 806, 811 (1987) (as long as the opponent is apprised of the facts that entitle the plaintiff to relief, it is not necessary to spell out a legal theory of relief in the pleadings).

[9] K.S.A. 66-101.

[10] K.S.A. 66-101h.

[11] K.S.A. 66-155 obligates Legal Staff with the duty to prosecute suits on behalf of parties complaining of unjust discriminations by a public utility or other violations of the public utility act. Legal Staff believes full representation of the Complainant in this case would be an unnecessary use of Commission resources and is evidence of further good cause for the Commission to waive K.A.R. 82-1-220(b)(1).

- This docket should be consolidated with Docket Nos. 15-KCPE-265-COM and 15-WSEE-211-COM.[12]

[12] K.A.R. 82-1-224

IN RE: DOCKET NO. **15-WSEE-211-COM** DATE **AUG 1 3 2015**

PLEASE FORWARD THE ATTACHED DOCUMENT (S) ISSUED IN THE ABOVE-REFERENCED DOCKET TO THE FOLLOWING:

NAME AND ADDRESS	NO. CERT. COPIES	NO. PLAIN COPIES

DENESE M. ROBERTS
8915 CHEROKEE LANE
LEAWOOD, KS 66206

JAMI RIEHM
711 ROCKLEDGE RD #1N
LAWRENCE, KS 66049

ROGER W. STEINER, CORPORATE COUNSEL
KANSAS CITY POWER & LIGHT COMPANY
ONE KANSAS CITY PL, 1200 MAIN ST (64105)
PO BOX 418679
KANSAS CITY, MO 64141-9679

MARY TURNER, COMPLAINTS
KANSAS CITY POWER & LIGHT COMPANY
ONE KANSAS CITY PL, 1200 MAIN ST (64105)
PO BOX 418679
KANSAS CITY, MO 64141-9679

SAMUEL FEATHER, LITIGATION COUNSEL
KANSAS CORPORATION COMMISSION
1500 SW ARROWHEAD RD
TOPEKA, KS 66604-4027
*****Hand Delivered*****

DUSTIN KIRK, ASSISTANT GENERAL COUNSEL
KANSAS CORPORATION COMMISSION
1500 SW ARROWHEAD RD
TOPEKA, KS 66604-4027
*****Hand Delivered*****

KEITH S. CARPENTER, COMPLAINANT
7633 COLONIAL DR
PRAIRIE VILLAGE, KS 66208

CATHRYN J. DINGES, SENIOR CORPORATE COUNSEL
WESTAR ENERGY, INC.
818 S KANSAS AVE
PO BOX 889
TOPEKA, KS 66601-0889

ORDER MAILED AUG 1 4 2015

The Docket Room hereby certified that on this ___ day of _____ , 20____, it caused a true and correct copy of the attached ORDER to be deposited in the United States Mail, postage prepaid, and addressed to the above persons.

IN RE: DOCKET NO. **15-WSEE-211-COM** DATE AUG 1 3 2015

PLEASE FORWARD THE ATTACHED DOCUMENT (S) ISSUED IN THE ABOVE-REFERENCED DOCKET TO THE FOLLOWING:

NAME AND ADDRESS	NO. CERT. COPIES	NO. PLAIN COPIES
JEFFREY L. MARTIN, VICE PRESIDENT, REGULATORY AFFAIRS WESTAR ENERGY, INC. 818 S KANSAS AVE PO BOX 889 TOPEKA, KS 66601-0889		

ORDER MAILED AUG 1 4 2015

The Docket Room hereby certified that on this ___ day of _____ , 20_____, it caused a true and correct copy of the attached ORDER to be deposited in the United States Mail, postage prepaid, and addressed to the above persons.