

-----Original Message-----

From: BPA <[BPA@puc.nv.gov](mailto:BPA@puc.nv.gov)>

To: ntefusa <[ntefusa@aol.com](mailto:ntefusa@aol.com)>

Cc: BPA <[BPA@puc.nv.gov](mailto:BPA@puc.nv.gov)>; rwhite <[rwhite@puc.nv.gov](mailto:rwhite@puc.nv.gov)>

Sent: Tue, Nov 20, 2012 1:28 pm

Subject: PUCN Electronic Filings Submittal

11/20/2012 1:27:49 PM 12-05003

Thank you for submitting your electronic filing.

This E-mail is your confirmation that the filing submittal has been received and electronically signed.

Please save and retain your E-mail acknowledgement of receipt for your records!

-----  
You have acknowledged that by filing documents in a Commission Docket you are placing yourself

on a service list and both the documents you filed and the contact information you provided for yourself will be publicly available.

-----  
Filings submitted outside of business hours will be date stamped as filed on the next business day.

The PUCN's business hours are 8:00 A.M. - 5:00 P.M. Monday through Friday excluding state holidays.

-----  
Filed For: NV Energy Stop Smart Meters

Filed By: Angel De Fazio

Filed By Phone Number: (702) 490-9677

Docket Number: 12-05003

Fee Submitted: \$0.00

Pertains To: As Docketed

DocType: Other filings in an Open Docket

EPay Confirmation Number: none

EPay Settlement Date: none

Epay Reference: none

PUCN Assigned Electronic Filing ID: ca31e529-0269-4bde-af38-4a1375fa8c47

Filer's Uploaded File Name: combo.pdf

Filer's Accounting Reference:

-----  
This message, including any attachments, is the property of the Public Utilities

Commission of Nevada and is solely for the use of the individual or entity intended to receive it. It may contain confidential and proprietary information and any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient(s) or if you have received this message in error, please contact the sender by reply email and permanently delete it.

NV Energy Stop Smart Meters  
POB 29194  
Las Vegas, NV 89126  
702.490.9677  
[Info@NVESmartMeters.Info](mailto:Info@NVESmartMeters.Info)

November 20, 2012

Re: Docket Number 12-05003

Dear Commissioners:

Since information provided during public comment sessions are not automatically incorporated in any pending open dockets, we wanted to make sure that there is a public record of what the Commission was made aware of regarding the smart meters and so called 'expert' testimony of NV Energy's PAID industry representatives. Along with notification of CFR violations.

To review, in Docket Number 11-10007, your reference number 13267, filed on December 2, 2011, by NVE, they retained Exponent to 'assist' the Commission in this Docket. NOTE that the Commission DID NOT request this company to appear, that their testimony WAS NOT under oath, nor did they REQUEST to appear as either a Commenter or Intervener, as required by the relevant NAC's. Which as USUAL the Commission allowed their 'favorite son' utility to circumvent the regulations.

On page 47/383 Testimony of Shkolnikov & Bailey.

Q. What is Exponent's role in the December 6, 2011 workshop?

A. NV Energy asked Exponent to be a technical resource to the Commission and to the public on health and safety issues relating to radiofrequency (RF) fields.

When Bailey and Shkolnikov 'testified', they 'cherry picked' references which they ACCUSED the public off. Also, the old man on the Commission asked 'leading' questions to 'reaffirm' their prevarications to the Hearing Master, at this time it was Wenzel, and the public in attendance. Especially since there is not a SINGLE person on the Commission or the others on the PUC panel that has science/health degrees/education. Not to forget the Commission panel had QUITE a few members engaged in communication with each other and were COMPLETELY IGNORING the public when they appeared.

When the public testified and provided REFUTED evidence of the PREVARICATIONS or SELECTED testimony of Exponent the Commission ignored it. Realize that the Commission only has a written transcript of the hearing, the video tape shows what comments warranted these 2 experts to start

taking notes. Their actions are more 'informative' than just typed characters on cellulose.

They testified that the Sensus Meters were "SAFE" etc.

At the same hearing date, De Fazio testified that a whistleblower filed a Qui Tam Complaint in Alabama. On May 25, 2010, a Qui Tam Complaint was filed in The United States District Court For the Northern District of Alabama Southern Division, Case No.: CV-10-CO-1337-S, *United States of America ex rel, Don Baker vs Sensus USA, Inc., Sensus Metering Systems, Inc., The Southern Company, and Alabama Power Company*, with allegations of fire safety concerns over their smart meters.

[2] <http://www.national-toxic-encephalopathy-foundation.org/wp-content/uploads/2012/02/SensusComplaint.pdf>

On October 11, 2012 at both the 1:30 and 6:00 p.m. consumer sessions, De Fazio provided the following information that REFUTES, NEGATES, DISCREDITS Exponent's and also NVE's so called ASSURITY of SAFETY issues with Sensus. EXHIBIT 1

Docket Number 12-07010, Docket ID Number 20549 were submitted and entered into the record for the consumer session. The SAME COMPANY that stated on December 6, 2011, that the meters WERE SAFE, were ALSO PAID to evaluate them and found them to be PROBLEMATIC in Pennsylvania.

Resulting in ALL INSTALLED SENSUS meters to be REMOVED and another company L&G meters to be installed.

These results were published in both public newspapers and industry publications.

*"Peco hired two independent consultants and Underwriters Laboratories (UL) to examine the meters after it suspended installations. The test results convinced the utility to swap out all the meters manufactured by Sensus Metering Systems Inc. of Raleigh, N.C., with those made by a Swiss vendor, Landis & Gyr AG... Officials earlier had indicated the meter problems were linked to faulty connections between the devices and the meter boards to which they are attached with four metal prongs. Experts suggested that poor connections caused electrical resistance and overheating in the meter sockets, which caused the devices to fail... Peco did not immediately release the results of its independent tests, which were conducted by Exponent Engineering and Scientific Consulting, of Menlo Park, Calif., and the National Electric Energy Testing Research and Applications Center (NEETRAC), which is affiliated with the Georgia Institute of Technology."*

[http://www.intelligentutility.com/article/12/10/after-tests-peco-resume-smart-meter-installations?quicktabs\\_11=1&quicktabs\\_4=2&quicktabs\\_6=1](http://www.intelligentutility.com/article/12/10/after-tests-peco-resume-smart-meter-installations?quicktabs_11=1&quicktabs_4=2&quicktabs_6=1)

The COMPLAINTS as asserted in these articles are MIRRORED in the QUI TAM Complaint filed in Alabama, by a HAND PICKED Sensus Project Manager.

Commissioners its time to extract the craniums from the SiO<sup>2</sup> and CaCO<sup>3</sup>. You have the SAME company testifying TWO times on the SAME COMPANY AND PRODUCT and they FOUND CONFLICITNG results.

In NVE's First Quarter 2012 Recovery.Gov filing they paid:

Exponent, Inc. - Award Number OE0000205 - Exponent, Inc.

|  |                                  |
|--|----------------------------------|
| <b>Award Number</b>                    | OE0000205                        |
| <b>Sub-Award Number</b>                | N/A                              |
| <b>Vendor DUNS Number</b>              | 168343346                        |
| <b>Vendor HQ Zip Code + 4</b>          | 77099-3465                       |
| <b>Vendor Name</b>                     | Exponent, Inc.                   |
| <b>Product and Service Description</b> | Consultation on RF Health Impact |
| <b>Payment Amount</b>                  | \$63,249                         |

<http://www.recovery.gov/Transparency/RecipientReportedData/Pages/RecipientProjectSummary508.aspx?AwardIDSUR=80621&vendorstart=1&qtr=2012Q1#vendorawards> Page 1 of 3. EXHIBIT 2

Also, they PAID to Cohbi Physicians, PC. out of Colorado for James Kornberg, MD's testimony

Award Number OE0000205 -

|                               |                           |
|-------------------------------|---------------------------|
| <b>Award Number</b>           | OE0000205                 |
| <b>Sub-Award Number</b>       | N/A                       |
| <b>Vendor DUNS Number</b>     | 960236649                 |
| <b>Vendor HQ Zip Code + 4</b> |                           |
| <b>Vendor Name</b>            |                           |
| <b>Product and Service</b>    | Consultation on RF Health |

|                       |          |
|-----------------------|----------|
| <b>Description</b>    | Impact   |
| <b>Payment Amount</b> | \$14,677 |

<http://www.recovery.gov/Transparency/RecipientReportedData/Pages/RecipientProjectSummary508.aspx?AwardIDSUR=80621&qtr=2012Q2#vendorawards>  
Page 1 EXHIBIT 2

NOW, you MUST keep in mind that NVE TESTIFIED that they COULD NOT allow a NON-FEE, as there was NO MONEY in their Smart Meter Budget for this. According to their submitted budget to the DOE, that they ALSO submitted to the PUC, there was NO ALLOCATION for the payment to Exponent or Cohbi Physicians, YET, they CHARGED these invoices to the "BUDGET". So where did this MYSTERIOUS funding come from?

Apparently, the PUC's highly, overstaffed department NEVER reviews expenditures against the so called DETAILED budget for these meters, that they agreed to when they approved this demon deployment of smart meters.

Can we say nonfeasance? Why should the consumers who are NOT BEING PAID, have to be doing the work of state employees who are REQUIRED to oversee the utilities? I am the FURTHEST from a CPA and even a former F/C bookkeeper can spot FRAUD and misappropriations of FEDERAL funds!

Commissioners you BETTER remember the following: On December 6, 2011, when Bailey testified he STATED that he **REVIEWS ALL** scientific reports and was CHALLENGED on the report from LSU done in JULY of 2011, that has now become a BENCHMARK for it's FLAWLESS STUDY DESIGN to PROVE the EXISTENCE of EHS. Which was published in a PEER REVIEWED SCIENTIFIC JOURNAL. Along with the Li study he INTENTIONALLY neglected to mention these QUANTIFIABLE proof of harm associated with EMF.

*International Journal of Neuroscience, 00, 1–7, 2011*  
Copyright©2011 Informa Healthcare USA, Inc.  
ISSN: 0020-7454 print / 1543-5245 online  
DOI: 10.3109/00207454.2011.608139

***Electromagnetic Hypersensitivity: Evidence for a Novel Neurological Syndrome***

<http://www.national-toxic-encephalopathy-foundation.org/lsustudy.pdf>

If the Commission had any medical/health knowledge they would KNOW that BREATHING is a NECESSITY to SUSTAIN life and is classified as a DISABILITY and protected under the ADA. These meters are giving off EMF's that are CAUSING DISABILITIES. Asthma is ON THE RISE and after THIRTEEN YEARS of follow up research it has been cited in *Arch Pediatr Adolesc Med.* 2011;165(10):945-950. doi:10.1001/archpediatrics.2011.135.

A PEER REVIEWED professional journal in OCTOBER of 2011. Maternal Exposure to Magnetic Fields During Pregnancy in Relation to the Risk of Asthma in Offspring by De-Kun Li, MD, PhD; Hong Chen, MPH; Roxana Odouli, MSPH

“Studies have shown that EMFs could adversely affect reproductive outcomes and the immune system.<sup>6-15</sup> A recent study also showed an EMF effect on brain cell activities.<sup>16-17</sup> Therefore, it is conceivable that exposure to high EMFs, especially during pregnancy (the period of fetal development), may have an impact on the risk of asthma in offspring. To examine this hypothesis, we conducted a prospective study based on a cohort of pregnant women whose daily exposure to magnetic fields (MFs) was captured objectively by a meter during their pregnancy and whose offspring from the index pregnancy were followed up for as long as 13 years for their asthma diagnosis.”  
<http://archpedi.jamanetwork.com/article.aspx?articleid=1107612>

One of the authors of this study sent this Response to California Council on Science and Technology (CCST) (Posted 3/31/11)  
<http://www.national-toxic-encephalopathy-foundation.org/LiCCST.pdf>

Lets look at the PUC's WANTON violations of both state and Federal laws.

PUC's March 2, 2012 Order states :

“Smart meters do not violate the ADA or the Fair Housing Act. Both the ADA and the Fair Housing Act require reasonable accommodations for the disabled individuals under certain circumstances. A disability is one that substantially limits one or more of the individual's major life functions. EHS is not a medical diagnosis, nor is it clear that the symptoms represent a single medical problem. Moreover, in 2005, the WHO indicated that no scientific basis currently exists for a connection between” EHS symptoms and Exposure to EMF. The accommodations suggested by several individuals including a moratorium on the installation of the smart meters, a rule proscribing the installations of smart meters in public facilities, and an opt-out provision, are not reasonable accommodations.

That conclusion is erroneous, myopic and factually incorrect, as they have selectively chosen one disability that has an association with EMF/RF. They neglected to incorporate all the other medical maladies/disabilities that are impacted by smart meters, such as increased cellular growth (cancer), muscular weakness, pacemakers, neurological and brain dysfunctions et al, that are directly tied into EMF/RF exposures.

De Fazio and others never utilized the term EHS and in testimony on December 6, 2011, acknowledged that EHS can possibly be perceived as “questionable”. All references to the ADA were associated with the recognized neurological

condition diagnosed as “Toxic Encephalopathy”, which has been accepted and defined by NIH and other agencies associated with them.

The WHO is not a US Federal Agency that is empowered to create rules and standards for citizens.

The Architectural and Transportation Barriers Compliance Board (Access Board) is an independent federal agency devoted to accessibility for people with disabilities. The Access Board is responsible for developing and maintaining accessibility guidelines to ensure that newly constructed and altered buildings and facilities covered by the Americans with Disabilities Act and the Architectural Barriers Act are accessible to and usable by people with disabilities.

*Federal Register*, Vol. 69, No. 141, July 23, 2004, page 44087,  
“The Board recognizes that multiple chemical sensitivities and electromagnetic sensitivities may be considered disabilities under the ADA if they so severely impair the neurological, respiratory, or other functions of an individual that it substantially limits one or more of the individual’s major life activities. The Board plans to closely examine needs of this population, and undertake activities that address accessibility issues for these individuals.”

Since the Access Board addressed electromagnetic sensitivities and said that it would be developing technical assistance materials on best practices for accommodating individuals with these disabilities, they have acknowledged that these are a protected demographic and warrant full protection under the ADA.

NVE must be ordered to refrain from violating these laws, thru the PUC in its supervisory and regulatory role and in implements its policies, practices and procedures which includes rulings and decisions.

The PUC’s authority extends to determining whether services or equipment of any public utility poses a danger or threat to the health and safety of the public and if so, prescribe corrective measures and order them into effect.

The PUC’s Rulings violate laws pertaining to commercial ratepayers and their customers, which prohibit barriers to access of services and programs to ‘qualified disabled customers’ and medical condition customers’ as described under federal and state constitutions and laws regarding their electric service. If removing or not installing the smart meter resolves the problem for the ‘qualified disabled customer/s’, the PUC is still deciding who much they will allow NVE to charge for those who want to opt out of the smart meters, in order to gain benefits of electric services where a healthy customer does not. This violates Title II of the ADA by putting the qualified disabled customer’ in the position of having no choice but to pay ordered fees to prevent harm and to also accept an alternative to the smart meter that has not been proven to be safe for them.



Moreover 'qualified disabled customers' whom are adversely affected by the EMF/RF emitted from the mesh network are discriminated against by the PUC and NVE's failure to make modifications to its policies, practices and procedures, to allow entitled accommodations.

The discrimination resulting, from the PUC and NVE failure to address the unique needs of qualified disabled customers in the smart meter deployment rulings, is by reason of their disabilities. Because the PUC failed to make modifications in its Rulings (policy, practices and procedures) qualified disabled customers and medical conditions customers are burdened "in a manner different and greater than it burdens others." Crowder v. Kitagawa 81 F.3d 1480, (1996) at 1484.

The Title II regulation Section 35.130 of the regulation lists several forms of conduct which constitute unlawful discrimination under Title II. Among them is the use of criteria or methods of administration "that have the effect of subjecting qualified individuals with disabilities to discrimination on the basis of disability." [12] 28 C.F.R. Section 35.130(b)(3)(i)(1993). The regulation's preamble explains that "the phrase 'criteria or methods of administration' refers to official written policy of the public entity and to the actual practices of the public entity. This paragraph prohibits both blatantly exclusionary policies or practices and nonessential policies and practices that are neutral on their face, but deny individuals with disabilities an effective opportunity to participate". [28 C.F.R. App. A. (1993).]

PUC violates Title II of the ADA, (and Rehab. Act of 1973 section 504) by not making modifications in its Rulings to accommodate qualified disabled customers and medical conditions customers.

Elsewhere is the same regulation specific forms of conduct are prohibited because they have a discriminatory effect upon individuals with disabilities. The use of criteria or methods of administration which "have the purpose or effect of defeating or substantially impairing accomplishment of the objects of the public entity's program with respect to individuals with disabilities" is prohibited. 28 C.F.R. section 35.130(b)(3)(ii)(1993). A public entities selection of a site for its services, programs or activities cannot "have the effect of" excluding individuals with disabilities from participation, denying them benefits, or otherwise subjecting them to discrimination, and cannot have the "purpose or effect" of defeating or substantially impairing the accomplishment of the objectives of the services, program, or activity, with respect to persons with disabilities. 28 C.F.R. section 35.130(b)(4)(i) and (ii)(1993). Finally, subsection 8 of the regulation says that a public entity "shall not impose eligibility criteria that screen out or tend to screen out an individual with a disability or any class of individuals with disabilities from fully and equally enjoying any service, program, or activity" unless the criteria are necessary for provision of the service, program, or activity. 28 C.F.R. section 35.130(b)(8)(1993).

*“A public entity shall make reasonable modifications in policies, practices, or procedures when the modifications are necessary to avoid discrimination on the basis of disability, unless the public entity can demonstrate that making the modifications would fundamentally alter the nature of the service, program or activity”.*

A ‘qualified disabled customer’ whose medical condition is exacerbated by the installation and operation of a smart meter and/or its mesh network, who requests a reasonable modification, by the installation of an analog meter and/or a ‘zone of safety’ would be requesting a reasonable modification to the policies, practices and procedures of the Commission in its regulation of the transmission and delivery of electrical service. For the Commission to fail to accommodate these reasonable modifications in the form of a request for an analog meters and/or ‘zone of safety’, based on a person’s disability, would violate section 35.130(b)(7). As the Commission has already acknowledge the implementation of an ALTERNATIVE to the smart meter, therefore, the retainment of the current analog meter is both financially neutral and feasible. As the current docket is seeking to determine rates for meter readers. Also, the OVERLOOK FACT that currently both the analog meters and smart meters are able to maintain both billing and readings thru NVE. NVE has DECIDED to PAD their EXPENSES by FEIGNING they need to alter their practices. IF that was the case, all those who are refusing the meters, would not be getting charged or having their accounts maintained by NVE. The computers and programs are already in use and there is no LOGICAL reason to have to REPROGRAM for meters that would be an ADDED expenses that is not justified.

The Commission’s failure to make reasonable modifications to it’s policies practices and procedures constitutes discrimination under Title II of the ADA. The prohibition against discrimination contained in the implementing regulations also requires a public entity to make reasonable modifications when the modifications are necessary to avoid discrimination on the basis of disability. This requirement is contained in 28 C.F.R. 35.130(b) (7) which provides:

PUC’s current docket that is to address charges/fees for opting out to a customer who opts out as a result of a disability is disability discrimination in violation of the ADA Title II and section 504 of the Rehab. Act as stated above.

Persons with disabilities are part of the “public” therefore the PUC must also consider, not just the danger to health and safety of the general healthy public, but also the dangers to health and safety of qualified persons with disabilities and those with protected medical conditions.

The PUC and the utilities are bound to comply with all federal and state laws pertaining to 'qualified disabled customers and 'medical condition customers'.

The PUC must afford equal benefits of service "qualified disabled customers". The regulations adopted by the U.S. Department of Justice to implement Title II of the ADA are contained in 28 C.F.R. parts 35. Imposing any opt-out fee on a person who opts-out on the basis of a qualifying condition and/or disability violates numerous provisions of the implementing regulations, which also are codified in numerous NRS.

An able bodied customer receiving electrical or gas service by way of a smart meter is afforded the full benefits of the electrical or gas service and is afforded the same benefit of such service provided to all others. On the other hand, a 'qualified disabled customer' who is adversely affected by the EMF/RF emitted by the smart meter/mesh network is not afforded the same benefit of such utility services provided to all others because the service exacerbates disabilities of of a customer as described supra.

The PUC and NVE can not rely upon 28 C.F.R. section 35.130(b)(8)(1993), to deny accommodations and modifications, as there is no federal requirement that every utility customer accept a smart meter and NVE's peers in other states, have provided accommodations for the retainment of the analog meters.

Modifications that the PUC should have enacted in their policies, practices and order utilities to comply with in order to accommodate the protected parties:

1. Retain the analog meter or replace an installed smart meter with an analog/electromechanical analog with no communication capabilities not any type of digital or non-transmitting meter at no charge; 2. Removal of smart meters in the area surrounding home of person with medical capabilities, at no charge to the customer, (distance to be determined by customers perceptions and symptoms); 3. Remove all wireless technology related to smart meters and smart grid within same circumference of home of person with covered medical condition; 4. Removal of any collector meter surrounding home of person with medical condition similar distance to "2 & 3".

Cases have been filed with numerous state regulatory agencies, state and federal courts, along with a vast number of cities, counties and entire states refusing to allow the meters to be installed. Or have ruled, allowing the customers the right to retain their analog meters.

Consumers have declared that radio frequencies have not been fully tested for health effects and the PUC should rule on the side of caution. That they should issue an immediate moratorium until 2014, when the federally funded study is complete. PUC was informed that John R. Bucher, Ph.D. Associate Director of the National Toxicology Program, National Institute of Environmental Health

Sciences, National Institutes of Health, U.S. Department of Health and Human Services “*The projected timeline is that pilot studies should be completed in November 2009. Subchronic toxicology studies then are expected to begin in early 2010, and the chronic toxicology and carcinogenicity studies are expected to start in late 2010, with an anticipated completion in 2012 and subsequent reporting and peer review of the data in 2013-2014.*”

*ED FRIEDMAN et al. v. PUBLIC UTILITIES COMMISSION et al.* ME Supreme Judicial Court, PUC-11-532, 2012 ME 90 [nor in the notices of the Opt-Out Investigation, nor in its other orders addressing this issue, did the Commission conclude that smart meter technology is not a credible threat to the health and safety of CMP’s customers. In fact, the Commission explicitly declined to decide this issue in the Opt-Out Investigation: “In initiating this investigation, we make no determination on the merits of health, safety, privacy or security concerns, the adequacy of existing studies or which federal or state agency has the jurisdiction to make these determinations and this investigation will not include such matters. Having never determined whether smart-meter technology is safe, the Commission is in no position to conclude in this proceeding that requiring customers who elect either of the opt-out alternatives to pay a fee is not “unreasonable or unjustly discriminatory,”

PUC Order dated March 2, 2011, referenced NVE’s comments:  
“Second, this alternative provides a non-standard metering arrangement that is most consistent with NVE’s obligations under the SGIG....Fourth, Alternative C is more consistent with the approach taken by other utility regulatory commissions.”

This was a factually incorrect statement provided to the PUC by NVE and they failed to verify the allegations of what other ‘utility regulatory commissions’ were doing.

PUC asked the utility what other states were doing and they neglected to affirm that there were opt out proposals to retain the analog meters. Defendant required NVE to submit proposals for four (4) options that mirrored the pending options in California. EXHIBIT 3

Michigan in July 2012, voted to allow opt out and retain their analogs.  
: Opt-out programs appear to be growing. Of the more than 100 utilities that participated in Chartwell’s 2012 Smart Grid survey, four reported that they are offering a “non-communicating wireless” meter opt-out choice and 14 reported considering such an option for their customers. Another six utilities reported that they now offer an analog meter as an opt-out option, and 10 utilities said they are considering the analog opt-out for their own customers.”  
<https://www.chartwellinc.com/another-state-joins-to-the-backward-moving-smart-meter-opt-out-train/>

Oregon The city of Ashland has dropped plans to charge utility customers who opt out on new smart meters to read their electricity use. Some residents are afraid that the radio waves transmitted by the smart meters could be harmful to their health.

The City Council has turned down a request from the city-owned Ashland Electric Department to charge customers \$120 plus \$20 a month to opt out of the new meters, which save money by transmitting the readings so meter readers don't have to drive down driveways and get out of cars. Instead, it adopted a budget that moved \$150,000 from reserves to cover the costs of customers who don't want smart meters, which so far number about 150.

When the PUC inquired if California adopted any specific meter, they were informed that the "recommended meter" as suggest from NVE, would be the choice for those who elected to opt out, but, it wasn't formalized yet. California has now designated the analog meter, to be the opt out choice. Page 18 has the formal Order on it. EXHIBIT 3

The PUC allowed NVE to inveigle them into believing that their DOE funding would be in jeopardy if they did not install all the smart meters, that they were federally mandated, that they must approve the installation of a pilot trial with non-transmitting meters with additional fees to those who request that smart meters not be installed and force the removal of the analog meters.

The PUC refused to entertain the legalities of that fallacious allegation of NVE. Numerous states who received the same type of funding as NV Energy such as Hawaii, California, Vermont, Maine, to reference a few, are offering their customers the option to keep their analog meters and their funding is not in jeopardy.

The PUC is only empowered to address public utilities such as energy, gas and telecommunications. They are not afforded any rights or privileges to make medical decisions, empower utilities to act in any medical capacity, supersede any federal or state statutes regarding the disabled, or deny any constitutional rights of the public.

NRS 703.150 General duties. The Commission shall supervise and regulate the operation and maintenance of public utilities and other persons named and defined in chapters 704, 704A and 708 of NRS pursuant to the provisions of those chapters.

NRS 703.151 Duties of Commission in adopting regulations relating to provision of electric service. In adopting regulations pursuant to this title relating to the provision of electric service, the Commission shall ensure that the regulations:

1. Protect, further and serve the public interest;
2. Provide effective protection for customers who depend upon electric service;

3. Provide for stability in rates and for the availability and reliability of electric service;
4. Encourage the development and use of renewable energy resources; and
5. Require providers of electric service to engage in prudent business management, effective long-term planning, responsible decision making, sound fiscal strategies and efficient operations.

On or about 2009/2010, NVE applied to the PUC to implement and deploy smart meters associated with a federal Department of Energy Grant they received on or about December 24, 2009, Grant Number OE0000205 in the amount of \$137,877,906.

The PUC freely elected to apply for federal stimulus monies under the American Recovery & Reinvestment Act. On November 17, 2009, under Grant Number DE-OE0000132, they were awarded a total of \$816,277.

Bringing both PUC and NVE actions under the federal Rehabilitation Act of 1973 section 504, which also prohibits discrimination by recipients of federal funds.

De Fazio has referenced numerous times, that these meters are not safe for service animals, as animals are more sensitive to environmental changes. The PUC has refused to require NVE to produce studies that service animals will not be impacted by the meters. Service animals that assist those with epileptic seizures are especially vulnerable to environmental disturbances, which will severely impact the animals ability to detect the onset of a seizure.

Please take note ANY HARM that comes upon my service animal I will be filing IMMEDIATELY and will FIND a WAY to go AFTER every Commissioner personally!

NRS 426.790 Unlawfully interfering with or allowing dog or other animal to interfere with use of service animal or service animal in training; unlawfully beating or killing service animal or service animal in training; penalties.

1. A person shall not:

Without legal justification, interfere with, or allow a dog or other animal the person owns, harbors or controls to interfere with, the use of a service animal or service animal in training by obstructing, intimidating or otherwise jeopardizing the safety of the service animal or service animal in training or the person using the service animal or service animal in training.

NRS 426.820 Civil liability for engaging in certain prohibited acts concerning service animals or service animals in training.

1. In addition to any criminal penalty that may be imposed, any person, including, without limitation, any firm, association or corporation, who violates the provisions of paragraph (a), (b) or (c) of subsection 1 of NRS 426.790 or

subsection 1 of NRS 426.810 is civilly liable to the person against whom the violation was committed for:

(a) Actual damages;

(b) Such punitive damages as may be determined by a jury, or by a court sitting without a jury, which must not be more than three times the amount of actual damages, except that in no case may the punitive damages be less than \$750; and

(c) Reasonable attorney's fees as determined by the court.

2. The remedies provided in this section are nonexclusive and are in addition to any other remedy provided by law, including, without limitation, any action for injunctive or other equitable relief available to the aggrieved person or brought in the name of the people of this State or the United States.

(Added to NRS by 2003, 2973; A 2005, 629)

The PUC as a state administrative agency created by the Nevada Constitution to regulate public utilities, the PUC is a public entity which pursuant to 42 U.S.C. section 12131, provides that Title II entities include "any department, agency...of a state..." As a public entity, the PUC is subject to Title II and the implementing regulations, The Rehabilitation Act of 1973 section 504 ("section 504") states that a violation of the ADA is a violation of section 504. The only additional requirement is receipt of federal funds. As noted, both the PUC and NVE were awarded federal funds, therefore is subject to section 504.

Section 504, as Spending Clause legislation, applies only to programs or activities that receive federal financial assistance. *See Koslow v. Pennsylvania*, 302 F.3d 161, 176 (3d Cir. 2002), *cert. denied*, 537 U.S. 1232 (2003). The plaintiffs' pleading here, while not a model of precision, is sufficient to state a claim under Section 504, as it includes "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009). Specifically, plaintiffs' allegation that the city receives federal funds "sufficient to invoke the coverage of Section 504," see Complaint 13 ¶ 31, permits this Court to draw the reasonable inference that the specific municipal programs responsible for the alleged discriminatory conduct receive such funds.

Consumers did request briefing of constitutional provision or state and federal laws that are applicable to these facts, which the PUC FAILED to address. This does not relieve the Commission or the utilities of duties under the law.

**Recipients of federal funds waive immunity for any conduct that is discriminatory toward, including by not limited to the disabled.**

[2]Quote from the DOE Application for Recovery Act Funds, signed by both Defendant and NVE states: "In accordance with the above laws and regulations issued pursuant thereto, the Applicant agrees to assure that no person in the United States shall, on the grounds of race, color, national origin, sex, age or

disability, be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program or activity in which the Applicant receives Federal Assistance from the DOE. Civil Rights Act of 1964 (Public Law 88-352); Section 16 of the Federal Energy Admin Act of 1974 (Pub. L. 93-275); Section 401 of the Energy Reorganization Act of 1974 (Pub. L. 93-438); Title IX of the Educational Amendments of 1972, as amended PL. 92-318; PL. 93-568; PL 94-482; Section 504 of the Rehabilitation Act of 1973 (PL. 93-112), the Age Discrimination Act of 1975 (PL. 94-135); Title VIII of the Civil Rights Act of 1968 (PL 90-284); the Dept of Energy Organization Act of 1977 (PL 95-91); and the Energy Conservation and Production Act of 1976, as amended (PL 94-385); Title 10 of Code of Federal Regulations Part 1040.

Consumers have been addressing AD NAUSEUM the privacy and constitutional aspects of these meters, which the Commission skirts over. Attached find the CONGRESSIONAL RESEARCH RECORD on this issue and how it is STILL NOT either black or white. EXHIBIT 4

Lets not FORGET that NVE has been stating that these are NO MORE HARMFUL than a cell phone. Will you BELIEVE YALE School of Medicine on the impact upon pregnant women? **YOU ARE NOT IMMUNE NOR ARE YOUR POTENTIAL GRANDKIDS!** EXHIBIT 5.

Fetal Radiofrequency Radiation Exposure From 800-1900 Mhz-Rated Cellular Telephones Affects Neurodevelopment and Behavior in Mice. Tamir S. Aldad, Geliang Gan<sup>2</sup>, Xiao-Bing Gao<sup>2,3</sup> & Hugh S. Taylor, published 15 March 2012. "We present the first experimental evidence of neuropathology due to in-utero cellular telephone radiation."

Remember this state is trying to attract businesses, are you actually that myopic that you think with all the hoopla of DENYING us analogs that OTHER STATES are PERMITTING, that people would want to come to a state with the SECOND HIGHEST power charges on the west coast?

Commissioners don't be stupid and side with the favorite son. Stupid decisions results in litigious consumers. You thought I wouldn't file the last time, NEVER underestimate a determined populous.

Do your homework, we are and apparently we seem to be amassing probable causation to look into malfeasance. When the time comes, you will have NO DEFENSE! As you can't FEIGN PLAUSIBLE DENIALBILITY!

I did confirm with the NV Bar in Las Vegas that even INACTIVE attorneys can have complaints filed against them.

Since you were NOMINATED, were you FULLY VETTED regarding NRS 703.04, if you have ANY mutual funds that have shares in NVE or SP? I THINK that's a



VIOLATION, don't you, if you didn't FULLY disclose all stocks held by any mutual fund?

**NRS 703.040 Commissioners: Additional qualifications; restrictions on other employment.**

2. No Commissioner may be **pecuniarily [sic]** interested in any public utility in this state or elsewhere.

Time for a full vetting of all financial interests, Commissioners?

Enjoy your Thanksgiving.

Respectfully submitted,

NV Energy Stop Smart Meters

/s/

Angel De Fazio, BSAT

Founder

The Laws of Ecology: "All things are interconnected. Everything goes somewhere. There's no such thing as a free lunch. Nature bats last." -Ernest Callenbach

# EXHIBIT 1

# THE ENERGY FIX

Purported smart meter fires: how power industry can get the facts, manage the risks

Written by theenergyfix on October 5, 2012

- Underwriters Lab (UL) has recently been engaged to do safety testing on these smart meters by some utilities. While presently there is not a specific meter safety test protocol by UL, they are modeling these tests after the electric vehicle charging specification (UL 2735).

**Testing Starts AFTER Houses Burn Down!**

**They admit they don't have a safety test for the Meters**



## The not so smart meter



**Norman Lambe**

LA Fire and Submarine Insurance Examiner

Subscribe

## Adjusters Admit Meters Are to Blame

For myself, as an adjuster, I believe the Smart Meters are a real a threat to the safety of your home, business and property. I have personally worked two large homeowner fires in which the Smart Meters were determined as responsible. Also, they have been responsible for several small fires in which appliances and computers have been destroyed.



Smart Meters

## Peco swaps meter makers, moves ahead with installations

Oct 9, 2012 [Talk Back](#) [Free Alerts](#) [More On This Topic](#) [SHARE](#) [f](#) [t](#) [e](#)

[<< Return to Page One](#)

### PECO Resumes Meter Installation Work

*Company continues support of PA Act 129*

PHILADELPHIA (October 9, 2012) – Following its own internal investigation and additional scientific analysis and testing by independent experts, PECO will resume meter installation work with Landis+Gyr (L+G) meters. PECO will replace the remaining previously installed 96,000 meters with L+G meters during the next 45 days. The company will then resume its meter installation work with L+G meters. As part of the project, Sensus is PECO's communications network provider.

"We have taken unprecedented steps to test our meters", said PECO President and CEO Craig Adams. "We are confident in the results of the scientific testing by independent experts. Based on our work, along with results of extensive independent testing, PECO has selected the Landis+Gyr (L+G) meter for use for our customers. And, UL (Underwriters Laboratories), a leading testing and certification company, has conducted safety performance tests using the UL safety requirements for utility meters and found that the L+G meter design we are using is fully compliant with these tests. We will continue to test and monitor our meters to ensure they meet the highest safety standards. Safety is always our top priority."

Customers will receive two letters and a telephone call beginning about six weeks prior to receiving a new meter. Customers with any questions or concerns can call 1-855-741-9011.

This project is part of PECO's continuing support of Pennsylvania's Act 129, requiring major utilities state-wide to install new metering technology for customers. The new meters will help PECO provide more information to customers to help them understand how they use energy, and how to save energy and money. The company also will be able to more quickly connect or disconnect service – providing faster, more convenient service for customers and assistance for emergency responders. And, PECO will be able to identify potentially dangerous situations like tampered meters and theft of electricity, detect problems faster – helping the company deploy field forces more effectively – and provide future new products and services to customers.

*Sponsored link:* Watch on-demand webinars from Structure. Topics include cyber security considerations when upgrading SCADA, optimizing business processes, GMS and more.

[<< Return to Page One](#)



### LATEST STORIES

**It's a wrap: 3 smart grid projects that are getting the job done**

[Synchrophasors in the Midwest to wind turbines in Oregon to demand response in Texas >>](#)

**Distributed energy: A hedge against lights out for Great Britain?**

[Regulator predicts energy shortage for Great Britain >>](#)

**A true smart grid contender: Aclara comes out swinging**

[Aclara succeeds in a slow market, but challenges lurk >>](#)



### HOT TOPICS

**Peco swaps meter makers, moves ahead with installations**

[Peco to swap smart meter vendors and resume installation >>](#)

**What a mess! ComEd puts brakes on smart grid rollout after rate dispute**

[Illinois regulators this week denied cost recovery on two key issues >>](#)

**Smart meter fire risks - a safe and sane approach**

**Talk Back to the Author** Current Comments (1) [Leave a Comment](#)

[Steps the industry can take to minimize potential risks >>](#)

**SMART METERS ARE FIRE STARTERS**

This is the technical analysis that the Peco resuming smart meter installations Philly article, did not tell you.  
<http://bcfreedom.wordpress.com/2012/10/10/smoking-gun-did-utilities-and-meter-makers-admit-responsibility-for-fires/>  
 The amazing thing to me is that the PECO talking Head , straight out told you that if Peco and Sensus do not come to terms as to who is responsible for the boondoggle. The PECO ratepayers will get left HOLDING the BAG! absorbing the costs of their screw-up!!  
 First they set your house on fire, and then charge you the expenses to put it out! (One has to start thinking , how much they really need electricity in the age of the cyborg!)  
 The BIG boys Play...The Little people PAY!  
 And the news reporting Investigative journalists and all, have developed the ability to hide behind their pen.  
 (Yes we know guys & gals, in the age of DIS-Information, you print what you are told by the politburo <http://www.thefreedictionary.com/Political+Bureau>)  
 Mr. Thiesen below says it exactly how it is and I concur with his analysis 100%

**George Karadimas - 10/10/2012 - 07:07**

[11 new smart grid solutions from names you know](#)

[Our latest roundup features new releases from industry stalwarts >>](#)

[Obama vs. Romney: Sizing up the electric industry's winners and losers](#)  
[Doug Houseman analyzes the candidates' energy policies >>](#)

[Leave a Comment](#)

[New to this Blog? Need some help?](#)

**Email:**

[?]

We will send you an email with an approval link you must click for your comment to appear.

**Full Real Name:**

[?]

Real comments need a real name.

**Subject:**

[?]

Please provide a short subject for your comment.

**Comment:** [?]

Do not post commercial/sales messages here. They will be deleted. Try: [pr@smartgridnews.com](mailto:pr@smartgridnews.com)

**PLEASE NOTE:** All HTML codes will be removed from your comment.

**CAPTCHA Security Code**



The numbers (0) and (1) are not used.

[?]

Please type the characters you see into the box above.

Remember my name? (Uncheck to forget.)

You can not edit or delete your comment once it is posted. Please check for spelling now.

Your IP Address is: 69.171.172.14

[HOME](#)

[Contact](#)  
[Advertise](#)  
[Privacy](#)

[NEWS](#)

[News](#)  
[Reviews](#)  
[Commentary](#)  
[Profiles](#)  
[Blogs](#)

[PROJECTS](#)

[Demos & Pilots](#)  
[R&D](#)  
[Stimulus](#)  
[Toolkits](#)  
[Updates](#)

[BUSINESS](#)

[Business Case](#)  
[Consumer Engagement](#)  
[Electronics](#)  
[Global](#)  
[Lessons Learned](#)  
[Markets & Pricing](#)  
[Policy & Regulation](#)  
[Smart Grid 101](#)  
[Strategy](#)

[T&D](#)

[Asset Management](#)  
[Distribution Automation](#)  
[DMS](#)  
[Microgrids](#)  
[Transmission](#)  
[Grid Optimization](#)

[END USE](#)

[Building Automation](#)  
[Demand Side](#)  
[Efficiency](#)

[TECHNOLOGIES](#)

[Communications](#)  
[Demand Response](#)  
[DG & Renewables](#)  
[Home Area Networks](#)  
[IT and Back Office](#)  
[MDM](#)  
[Metering](#)  
[SCADA](#)  
[Security](#)  
[Smart Water](#)  
[Standards](#)

[KEY PLAYERS](#)

[Associations](#)  
[Policy and Regulation](#)  
[Sponsors and Affiliates](#)  
[Utilities](#)  
[Vendors](#)

[STORE](#)

[SGN Research Marketplace](#)  
[Smart Grid Amazon](#)  
[IDC Reports](#)  
[Research and Markets](#)

[EXTRA](#)

[Events Calendar](#)  
[Hot Topics](#)  
[Newsletter Sign-up](#)  
[QuickPoll Archives](#)  
[RSS Feed](#)

**Electric Transportation**  
**Smart Homes**

**Storage**  
**Transmission**

**Videos**  
**Webinars**  
**© 2012 SmartGridNews**

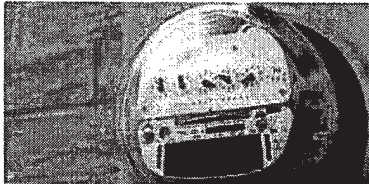


## Smart Meters

## Peco swaps meter makers, moves ahead with installations

Oct 9, 2012 [Talk Back](#) [Free Alerts](#) [More On This Topic](#) [SHARE](#) [f](#) [t](#) [e](#)

[Read the Peco news release on Page 2 >>](#)



Peco Energy announced Tuesday it will resume the smart meter installations it had stopped in August after several meters overheated and two caused fires at homes. Peco did not blame the Sensus meters it had installed for the fires, but said its own internal investigation and independent testing convinced utility officials to resume the installation project with meters from Swiss maker Landis+Gyr (L+G).

The Peco statement said in part: "Following its own internal investigation and additional scientific analysis and testing by independent experts, PECO will resume meter installation work with Landis+Gyr meters. PECO will replace the remaining previously installed 96,000 meters with L+G meters during the next 45 days. The company will then resume its meter installation work with L+G meters. As part of the project, Sensus is PECO's communications network provider."

A Sensus spokesman, quoted in the Philadelphia Inquirer, said the company was disappointed with the decision and added that the meters are safe. "All of the investigations we've seen have proven the Sensus meter is not a problem," said Randolph Wheatley, VP of corporate marketing for Sensus.

*Sponsored link:* Watch Accenture's video that features energy experts responding to children's questions about the importance of a smarter grid to a sustainable energy future.

A number of experts, including those at DNV KEMA, have said fire risks shouldn't be blamed on the meters, but on poor or degraded connections in the meter socket receptacles.

Peco had hired two independent firms and Underwriters Laboratories to examine and test the meters after it stopped the installations.

While Peco does not appear to have criticized the Sensus meters, "We determined that the L&G meter is the best solution for Peco customers, that it performed better in the field, and that was confirmed by testing," said Peco spokeswoman Cathy Engel Menendez, also quoted in the Inquirer.

Peco customers will receive mail and telephone notifications before receiving new meters.

A Pennsylvania Public Utility Commission investigation into the meter installations is continuing.

1

The issue is not just a problem for Sensus, but could give those groups opposed to smart meters more ammunition for their campaigns. And that would be unfortunate for the entire industry.

*You might also be interested in ...*

[House fire stalls smart meter deployment while Peco Energy investigates cause](#)



### LATEST STORIES

**It's a wrap: 3 smart grid projects that are getting the job done**

[Synchrophasors in the Midwest to wind turbines in Oregon to demand response in Texas >>](#)

**Distributed energy: A hedge against lights out for Great Britain?**

[Regulator predicts energy shortage for Great Britain >>](#)

**A true smart grid contender: Aclara comes out swinging**

[Aclara succeeds in a slow market, but challenges lurk >>](#)

LESSONS FROM THE REAL WORLD

## Customer Engagement with In-Home Displays

A FREE WEBINAR featuring Rakant Energy  
Wednesday, Oct. 17  
10:30 a.m. PT / 1:30 p.m. ET  
[Register](#)

### HOT TOPICS

**Peco swaps meter makers, moves ahead with installations**

[Peco to swap smart meter vendors and resume installation >>](#)

**What a mess! ComEd puts brakes on smart grid rollout after rate dispute**

[Illinois regulators this week denied cost recovery on two key issues >>](#)

**Smart meter fire risks - a safe and sane approach**

[Steps the industry can take to minimize potential](#)



Page 2: Peco news release >>

risks >>

11 new smart grid solutions from names you know

Our latest roundup features new releases from industry stalwarts >>

Obama vs. Romney: Sizing up the electric industry's winners and losers

Doug Houseman analyzes the candidates' energy policies >>

Talk Back to the Author Current Comments (1) Leave a Comment

**SMART METERS ARE FIRE STARTERS**

This is the technical analysis that the Peco resuming smart meter installations Philly article, did not tell you.  
<http://bcfreedom.wordpress.com/2012/10/10/smoking-gun-did-utilities-and-meter-makers-admit-responsibility-for-fires/>  
 The amazing thing to me is that the PECO talking Head , straight out told you that if Peco and Sensus do not come to terms as to who is responsible for the boondoggle. The PECO ratepayers will get left HOLDING the BAG! absorbing the costs of their screw-up!!  
 First they set your house on fire, and then charge you the expenses to put it out! (One has to start thinking , how much they really need electricity in the age of the cyborg!)  
 The BIG boys Play...The Little people PAY!  
 And the news reporting Investigative journalists and all, have developed the ability to hide behind their pen.  
 (Yes we know guys & gals, in the age of DIS-Information, you print what you are told by the politburo <http://www.thefreedictionary.com/Political+Bureau>)  
 Mr. Thiesen below says it exactly how it is and I concur with his analysis 100%

**George Karadimas - 10/10/2012 - 07:07**

Leave a Comment New to this Blog? Need some help?

**Email:**  [?]  
 We will send you an email with an approval link you must click for your comment to appear.


**Full Real Name:**  [?]  
 Real comments need a real name.

**Subject:**  [?]  
 Please provide a short subject for your comment.

**Comment:** [?]

Do not post commercial/sales messages here. They will be deleted. Try: [pr@smartgridnews.com](mailto:pr@smartgridnews.com)  
**PLEASE NOTE:** All HTML codes will be removed from your comment.

**CAPTCHA Security Code**

  
 The numbers (0) and (1) are not used.  
 [?]  
 Please type the characters you see into the box above.

Remember my name? (Uncheck to forget.)

**Post Comment**  
 You can not edit or delete your comment once it is posted. Please check for spelling now.  
 Your IP Address is: 69.171.172.14

|                           |                                    |                                     |   |                                     |   |  |
|---------------------------|------------------------------------|-------------------------------------|---|-------------------------------------|---|--|
| <a href="#">HOME</a>      | <a href="#">PROJECTS</a>           | <a href="#">BUSINESS</a>            | <a href="#">T&amp;D</a>                 | <a href="#">TECHNOLOGIES</a>        | <a href="#">KEY PLAYERS</a>             | <a href="#">STORE</a>                    |
| <a href="#">Contact</a>   | <a href="#">Demos &amp; Pilots</a> | <a href="#">Business Case</a>       | <a href="#">Asset Management</a>        | <a href="#">Communications</a>      | <a href="#">Associations</a>            | <a href="#">SGN Research Marketplace</a> |
| <a href="#">Advertise</a> | <a href="#">R&amp;D</a>            | <a href="#">Consumer Engagement</a> | <a href="#">Distribution Automation</a> | <a href="#">Demand Response</a>     | <a href="#">Policy and Regulation</a>   | <a href="#">Smart Grid Amazon</a>        |
| <a href="#">Privacy</a>   | <a href="#">Stimulus</a>           | <a href="#">Electronomics</a>       | <a href="#">DMS</a>                     | <a href="#">DG &amp; Renewables</a> | <a href="#">Sponsors and Affiliates</a> | <a href="#">IDC Reports</a>              |
|                           | <a href="#">Toolkits</a>           | <a href="#">Global</a>              | <a href="#">Microgrids</a>              | <a href="#">Home Area Networks</a>  | <a href="#">Utilities</a>               | <a href="#">Research and Markets</a>     |

**NEWS**  
**News**  
**Reviews**  
**Commentary**  
**Profiles**  
**Blogs**

**Updates**

**Lessons Learned**  
**Markets & Pricing**  
**Policy & Regulation**  
**Smart Grid 101**  
**Strategy**

**Transmission**  
**Grid Optimization**  
  
**END USE**  
**Building Automation**  
**Demand Side**  
**Efficiency**  
**Electric Transportation**  
**Smart Homes**

**IT and Back Office**  
**MDM**  
**Metering**  
**SCADA**  
**Security**  
**Smart Water**  
**Standards**  
**Storage**  
**Transmission**

**Vendors**

**EXTRA**  
**Events Calendar**  
**Hot Topics**  
**Newsletter Sign-up**  
**QuickPoll Archives**  
**RSS Feed**  
**Videos**  
**Webinars**  
**© 2012 SmartGridNews**

# 5

## *The Enronization of Science*

Lead...Hill and Knowlton. Vinyl chloride...Hill and Knowlton. Asbestos...Hill and Knowlton. Tobacco...Hill and Knowlton. Are we beginning to see a pattern here? Given where we are today, it is hard to believe that the cigarette manufacturers did not even have a trade association until 1953, when public relations guru John Hill warned the industry to get organized before it was too late and offered his firm's services for that dubious purpose. In 1966 Hill and Knowlton set up its Division of Scientific, Technical, and Environmental Affairs, which in later years would brag in solicitation brochures that this founding was "years before the first 'Earth Day' or the establishment of the Environmental Protection Agency."<sup>1</sup> Regarding the vinyl chloride story, the firm boasted that it assisted the producers of this carcinogen "to help fight and finally bring under control one of the most violent media and government regulatory firestorms ever experienced by a single industry," with the result that the final OSHA standards "were significantly less onerous than had been originally proposed."<sup>2</sup> When three scientists linked chlorofluorocarbon gas—Freon—to the destruction of the ozone layer<sup>3</sup> and users of the chemicals began to look for alternatives, Hill and Knowlton went into action. On behalf of the Freon manufacturers, the firm attacked the science as uncertain and later boasted that its work helped DuPont gain "two or three years before the government took action to ban fluorocarbons."<sup>4</sup> In fact, the science was of the highest quality: The three researchers subsequently won a Nobel Prize.

While Hill and Knowlton continues to provide public relations services to polluters, since the 1970s the sophistication of the “product defense industry” has grown apace with the federal regulatory apparatus established by Congress. For thirty years, therefore, it has been pretty much smooth sailing—that is, lots of lucrative work—for the key players in the new industry who specialize in helping corporations fight regulation. Ironically, more work is assured them with every advance in our ability to identify the deleterious health effects of toxic exposures. Only in the last few decades have we perfected the techniques that allow us to recognize and measure the illness and premature death toll associated with specific components of air pollution. New laboratory techniques have enabled scientists to examine the endocrine-disrupting properties of chemicals at almost unthinkably low levels of concentration. As a general rule, the more we know, the more regulation is required. Industry and free-market ideologues despise this logic, but what is the alternative? *Ignore* the health impact of these toxins? Yes, or better yet, let’s debate the impact!

As the product defense work has gotten more and more specialized, the makeup of the business has changed; generic public relations operations like Hill and Knowlton have been eclipsed by product defense firms, specialty boutiques run by scientists. Having cut their teeth manufacturing uncertainty for Big Tobacco, scientists at ChemRisk, the Weinberg Group, Exponent, Inc., and other consulting firms now battle the regulatory agencies on behalf of the manufacturers of benzene, beryllium, chromium, MTBE (methyl tertiary-butyl ether), perchlorates, phthalates, and virtually every other toxic chemical in the news today. Their business model is straightforward. They profit by helping corporations minimize public health and environmental protection and fight claims of injury and illness. In field after field, year after year, this same handful of individuals and companies comes up again and again.

The range of their work is impressive. They have on their payrolls (or can bring in on a moment’s notice) toxicologists, epidemiologists, biostatisticians, risk assessors, and any other professionally trained, media-savvy experts deemed necessary. They and the larger, wealthier industries for which they work go through the motions we expect of the scientific enterprise, salting the literature with their questionable reports and studies. Nevertheless, it is all a charade. The work has one overriding motivation: advocacy for the sponsor’s position in civil court, the court of public opinion, and the regulatory arena. Often tailored to address issues that arise in litigation, they are more like legal pleadings than scientific papers. In the regulatory arena, the studies are useful not because they are good work that the regulatory agencies have to take seriously but because they clog the machinery and slow down the process.

Public health interests are beside the point. Follow the science wherever it leads? Not quite. This is science for hire, period, and it is extremely lucrative. Court records show that the big three U.S. auto companies paid product defense scientists \$23 million between 2001 and 2006 to help defend them against disease claims by mechanics and other workers exposed to asbestos contained in automobile brakes.<sup>5</sup>

The coterie of consulting firms that specialize in product defense have done a great job—so great that manufacturing uncertainty has become a big business in itself. The scientific studies these firms do for their clients are like the accounting work that some Arthur Andersen Company accountants did for Enron (until both companies went bankrupt): They appear to play by the rules of the discipline, but their objective is to help corporations frustrate regulators and prevail in product liability litigation.

\* \* \*

Should the public lose all interest in its health, these product defense firms would be out of luck. Exponent, Inc., one of the premier firms in the product defense business, acknowledges as much in this filing with the Securities and Exchange Commission:

Public concern over health, safety and preservation of the environment has resulted in the enactment of a broad range of environmental and/or other laws and regulations by local, state and federal lawmakers and agencies. These laws and the implementing regulations affect nearly every industry, as well as the agencies of federal, state and local governments charged with their enforcement. To the extent changes in such laws, regulations and enforcement or other factors significantly reduce the exposures of manufacturers, owners, service providers and others to liability, the demand for our services may be significantly reduced.<sup>6</sup>

Exponent, Inc., began its existence as an engineering firm, calling itself Failure Analysis Associates and specializing in assisting the auto industry in defending itself in lawsuits involving crashes.<sup>7</sup> “Failure analysis” is a standard methodology for investigating the breakdown of a system or machine, but the firm must have realized that “Failure” in its name might not work well outside the engineering world and switched to the more palatable Exponent, Inc., when it went public in 1998.<sup>8</sup>

Exponent’s scientists are prolific writers of scientific reports and papers. While some may exist, I have yet to see an Exponent study that does not support the conclusion needed by the corporation or trade association that is paying the bill. Here are brief sketches of a few recent Exponent projects:

- The taste and smell of the gasoline additive MTBE are so foul that a tiny amount makes water undrinkable. This is bad because MTBE has contaminated drinking water sources across the country. (Moreover, it causes cancer in animals and may do so in people also, but this will be difficult to determine because the exposure levels are very low, exactly the sort of situation that epidemiology has the most difficulty addressing. The state of California has categorized MTBE as a possible human carcinogen.<sup>9</sup>) Communities across the country have sued the major oil companies and the MTBE manufacturers for the costs of cleaning up their water supplies. In response, a firm that provides the methanol used for making MTBE hired Exponent to produce a series of studies that concluded, not surprisingly, that MTBE is unlikely to pose a public health hazard and has not significantly impacted California's drinking water.<sup>10</sup> When the defendants in certain lawsuits tried to convince Congress to end the litigation by fiat and bail out the polluters, Exponent's economists produced a report for the American Petroleum Institute that concluded that the cost of the cleanup would be relatively low, which would make the proposed taxpayer bailout of the industry more acceptable to fiscal watchdogs.<sup>11</sup>
- An article in the *Annals of Emergency Medicine* suggested that the new generation of amusement park rides exposed thrill seekers to g-forces (a measure of acceleration) that exceed those experienced by astronauts and recommended that emergency physicians consider these rides as "a possible cause of unexplained neurologic events in healthy patients."<sup>12</sup> Six Flags Theme Parks, Inc., immediately commissioned Exponent to produce an "Investigation of Amusement Park Roller Coaster Injury Likelihood and Severity."<sup>13</sup> The press release on the report was headlined "Roller Coasters, Theme Parks Extraordinarily Safe."<sup>14</sup>
- Given the skyrocketing obesity rates among teenagers, many school systems and even some states have considered banning soda machines from high schools in order to discourage teenagers from consuming the empty calories. In 2005 an Exponent scientist conducted a study on behalf of the American Beverage Association that concluded that the number of beverages consumed from school vending machines "does not appear to be excessive."<sup>15,16</sup> In this case, however, the public just could not be convinced. The soft drink industry jettisoned these findings and in 2006 agreed to stop selling soda in schools.<sup>17</sup>
- Defense giant Lockheed Martin turned to Exponent when faced with the huge potential cost of cleaning up underground water sources contaminated with perchlorate, a rocket fuel component that ac-

according to the National Academy of Sciences causes thyroid disease in infants.<sup>18</sup> Exponent's studies minimized the risk associated with perchlorate exposure.<sup>19,20</sup>

- When a study by consulting epidemiologists discovered a high rate of prostate cancer cases at a Syngenta plant that produced the pesticide atrazine,<sup>21</sup> Exponent's scientists produced a study that found no relationship between the chemical and the disease.<sup>22</sup>
- After numerous studies that linked pesticide exposure and Parkinson's disease appeared in prestigious scientific journals, Exponent's scientists produced a literature review for CropLife America, the trade association of pesticide producers, whose conclusion maintained that "the animal and epidemiologic data reviewed do not provide sufficient evidence to support a causal association between pesticide exposure and Parkinson's disease."<sup>23</sup>
- Exponent specializes in literature reviews that draw negative conclusions. The company's scientists have produced several reviews of the asbestos literature for use in litigation, all of which conclude that certain types of asbestos and certain types of asbestos exposure are far less dangerous than previously believed.<sup>24-26</sup>

Another major player is the Weinberg Group, which was founded in 1983 by Dr. Myron Weinberg, formerly of Booz, Allen, and Hamilton. "Asbestos, Tobacco, Pharmaceuticals—We're All Next!" shouts the PowerPoint presentation of one Weinberg executive. Here is his bottom line: "Without the science you cannot win, but having it carries no guarantee."<sup>27</sup> In one promotional brochure the firm touts its work for a company that was confronted with a Superfund problem. On behalf of this client Weinberg's scientists "analyzed existing studies to find any design flaws to support legal defense. . . . [B]y reanalyzing the raw data from this study, a biostatistician from THE WEINBERG GROUP helped to demonstrate the study's numerous design and analysis flaws."<sup>28</sup>

In 2003 DuPont hired the Weinberg Group to address "the threat of expanded litigation and additional regulation by the EPA" of perfluorooctanoic acid (PFOA),<sup>29</sup> a chemical used in the production of Teflon. (The majority of members on an EPA scientific advisory board have labeled PFOA a "likely" carcinogen.<sup>30</sup>) Paul Thacker, a reporter, uncovered a letter from Terry Gaffney, Weinberg's vice president for Product Defense, to a DuPont vice president, explaining that "DUPONT MUST SHAPE THE DEBATE AT ALL LEVELS." (This firm appears to favor uppercase exhortations.) Gaffney lays out a comprehensive strategy, including "analyzing existing data, and/or constructing a study to establish not only that

PFOA is safe . . . but that it offers real health benefits.”<sup>29,31</sup> At the time, Gaffney was also running the campaign of a major manufacturer of ephedra-based dietary supplements to stop the FDA from banning ephedra, a product that the agency had already linked to 164 deaths.<sup>32</sup>

In my work on beryllium, I first came across the work of Dr. H. Daniel Roth. This was a reanalysis by Dr. Roth and Dr. Paul Levy on behalf of the beryllium industry, and it yielded the usual result: By changing some of the parameters, the researchers had managed to demonstrate that the statistically significant elevation of lung cancer risk was no longer statistically significant.<sup>33</sup> Such reanalyses are a specialty of some of the product defense firms, whereby one epidemiologist reanalyzes another’s raw data in ways that almost always exonerate the chemical, toxin, or product in question. The studies are carefully designed to do just this. Statistically significant differences disappear; estimates of risk are reduced. Such alchemy is rather easily accomplished, whereas the opposite—turning insignificance into significance—is extremely difficult.

Intrigued by the work of Levy and Roth on behalf of the beryllium industry, I wanted to see whether the two had bestowed similar benefits on other industries, so I Googled them. Among the many exhibits I found were a number of tobacco documents showing how both men had worked for this industry. Dr. Levy was hired by R. J. Reynolds (RJR) to conduct a reanalysis of a study examining the link between lung cancer and workplace exposure to secondhand smoke; in 1998 he presented his findings to a National Toxicology Program panel that was considering whether to designate environmental tobacco smoke (ETS) as a carcinogen. No link existed, he concluded.<sup>34</sup> Dr. Roth’s work with tobacco was more extensive. In 1985 he was one of the experts hired by Philip Morris to assist with its litigation, especially to develop ways to attribute lung cancer among smoking asbestos workers to asbestos rather than to smoking.<sup>35</sup> In 1987 he applied for the position of executive director of the Center for Indoor Air Research (CIAR), a creation of the Tobacco Institute. The evaluation of Dr. Roth by CIAR’s executive search firm was very positive. “Simply put,” it concluded, he “believes in the mission of the Center and in his ability to achieve its objectives.”<sup>36</sup> The tobacco documents do not reveal whether he was offered the job, but it is clear he later played a key role in Big Tobacco’s efforts to stop OSHA’s proposed indoor air quality standard in 1994.<sup>37</sup>

The tobacco relationship did not surprise me, but the coal connection did. For the past thirty years Dr. Roth has worked for producers and users of coal, turning out reanalysis after reanalysis refuting studies of the health effects of airborne pollutants from coal-burning power plants. On behalf of the North Dakota Lignite Research Council, which represents companies that produce coal with a high mercury content, he reviewed the literature on



the effects of human exposure to mercury and, taking a page from the tobacco playbook, told the coal producers that most of the studies were “highly questionable” and that the overall picture was inconclusive. Even so, he recommended that “it would be valuable to reanalyze the raw data.”<sup>38</sup>

In 1977 Dr. Roth produced a report for the electrical power industry that attacked the EPA’s research on the relationship between exposure to fine particles in the air and the risk of asthma attacks. This reanalysis was required, he wrote, because the acceptance by the public and policy makers of the original EPA study was “making it most difficult to generate wise policy decisions on such matters as the rapid expansion of the use of coal.”<sup>39</sup> Interestingly, both of Dr. Roth’s coauthors on this study went on to become key scientists in Big Tobacco’s campaign to manufacture uncertainty about the health effects of secondhand smoke. One of them, Dr. Anthony Colucci, was appointed director of RJR’s Scientific Litigation Support Division.<sup>40</sup>

A jack of all trades within the product defense business, Dr. Roth also turned up in a book, *The Expert Witness Scam*, written by Leon Robertson, a retired professor of epidemiology from Yale and one of the two or three leading injury epidemiologists of the twentieth century. Dr. Robertson was appalled that for at least a decade Dr. Roth had been presented as an expert in vehicle rollovers although, according to Robertson, Roth had never published a research paper on any aspect of motor vehicle injuries.<sup>7</sup>

Dr. Roth also collaborated with Dr. Levy in refuting the risks associated with liquor; the Distilled Spirits Council of the United States hired them to critique the studies on alcohol consumption and breast cancer.<sup>41,42</sup>

Yet another major product defense consultant is ChemRisk, founded in the 1980s by Dennis Paustenbach, perhaps the leading figure in the field. Dr. Paustenbach has an unassailable scientific background. He is the author of two textbooks on risk assessment and hundreds of scientific articles and book chapters. At first, ChemRisk was part of a larger consulting firm, McLaren/Hart Environmental Engineering Corporation, of which Dr. Paustenbach eventually became president and chief executive officer. In 1998, when McLaren/Hart was facing bankruptcy, Dr. Paustenbach and several ChemRisk colleagues moved to Exponent, Inc.

In 2003 Dr. Paustenbach left Exponent and revived the name ChemRisk for his firm, which has prospered, quickly opening six offices around the country. He and his colleagues are important players in this book and are featured in upcoming discussions of benzene, beryllium, and chromium. In each case they have developed arguments that could have the effect of delaying or weakening public health regulation of a powerful toxin. Paustenbach is a veteran of the Love Canal and Times Beach, Missouri, catastrophes, and has been a key participant in the attempted rehabilitation of dioxin.<sup>43</sup> He has worked for the initiative funded by the auto industry that

attempts to show that asbestos liberated from automobile brakes does not cause disease,<sup>44,45</sup> and he was also among the scientists used by the tobacco industry to question the EPA's risk assessment of secondhand tobacco smoke.<sup>46</sup>

According to a report in the *Wall Street Journal*, Dr. Paustenbach and his colleagues at ChemRisk pulled off a particularly audacious stunt on behalf of Pacific Gas and Electric (PG&E).<sup>47</sup> The California utility was fighting several lawsuits, including the one portrayed in the movie *Erin Brockovich*, in which chromium-contaminated groundwater was alleged to have caused a range of illnesses. In mounting its defense, PG&E turned to ChemRisk, which had already been working for the chromium industry in New Jersey (trying to convince that state's regulators that the metal was not so dangerous as to require cleaning up a massive toxic waste dump.<sup>48</sup>) According to a report in the *Wall Street Journal*, ChemRisk's product defense experts, through an affiliate in Shanghai, obtained the raw data of a 1987 study that had implicated chromium-polluted water in high cancer rates.<sup>49</sup> This study was a major problem for the defendants. The *Wall Street Journal* reported that ChemRisk paid Dr. Zhang JianDong, the lead author, two thousand dollars, reanalyzed his data, and obtained different results that appeared to exonerate chromium. The reanalysis was then published under the names of Dr. Zhang and a Chinese colleague, without any mention or acknowledgement of ChemRisk's role.<sup>47,50,51</sup>

This initiative was remarkably successful; for almost a decade, the fabricated study was promoted in courts and regulatory proceedings. Fortunately, the questionable history of the article is now public knowledge. After much uproar, the editor of the journal in which the paper was published withdrew the work,<sup>52</sup> and a California state epidemiologist has re-examined the original data and determined that Dr. Zhang's first analysis was the accurate one: Drinking chromium in your water increases your risk of stomach cancer.<sup>53</sup> (Paustenbach has said that his involvement in the paper was relatively minor and has defended the "underlying science." ChemRisk has also claimed that its scientists "wanted to be co-authors on the paper."<sup>54</sup> A year after the *Wall Street Journal* reported the story, the Chinese paper's second author claimed that the newspaper's coverage was inaccurate.<sup>55</sup> But the *Wall Street Journal* has not corrected or retracted its story.)

This episode was outrageous but not all that out of line with the standards of the industry. When product defense specialists cannot get the raw data required for a reanalysis, they have even been known to make them up. I learned this when I came across an abstract that described the reanalysis of the data of a study of older adults that had found reduced performance on neuropsychological tests associated with polychlorinated biphenyl (PCB) levels. The reanalysts did not have access to the raw data, so they came up

with a simulated data set based on the overall distribution of subjects in the original study. Not surprisingly, their results called into doubt the validity of the original findings.<sup>56</sup> My curiosity piqued, I called the author of the original study, toxicologist Susan Schantz of the University of Illinois. Dr. Schantz had never heard of the reanalysis. She had never been asked to provide her raw data, and when I read her the abstract, she laughed. Dr. Schantz told me the new work was simply wrong, as she could have explained to the reanalysts if they had asked her. (One of those reanalysts was the same scientist who would later defend the cause of selling soda in schools for the American Beverage Association.)

\* \* \*

Peer review is a complex issue, one that is widely misunderstood by the public and by some individuals in the regulatory and legal systems. Even rigorous peer review by honest scientists does *not* guarantee a study's accuracy or quality. Peer review is just one component of a larger quality control process through which scientific knowledge is developed and tested—a process that never ends. Nevertheless, it has been granted an important role in both the regulatory and legal systems. Some agencies, including the International Agency for Research on Cancer (IARC), will not consider using a paper in its deliberations if it has not undergone peer review.<sup>57</sup> Articles that have been published in peer-review journals are assumed, often mistakenly, to be of high quality. This is not necessarily so.

The credibility given peer-reviewed studies encourages product defense firms to manipulate and distort the process. They play the peer-review card beautifully. They understand that their studies and reanalyses need this imprimatur, but how do they get this seal of approval? Easy. They establish vanity journals that present themselves to the unwary as independent sources of information and science, but the peer reviewers are carefully chosen, like-minded corporate consultants sitting in friendly judgment on studies that are exquisitely structured to influence a regulatory proceeding or court case.

There is now a slew of these “captured” journals. The tobacco industry, for example, secretly financed the journal *Indoor and Built Environment* to promote (and position for legal purposes) the idea that indoor air pollution was a problem caused not by secondhand smoke but by inadequate ventilation.<sup>58</sup> The best-known of these publications is *Regulatory Toxicology and Pharmacology*, the official mouthpiece of the International Society for Regulatory Toxicology and Pharmacology (ISRTP)—an impressive name, but really just an association dominated by scientists who work for industry trade groups and consulting firms.<sup>59</sup> The sponsors of the ISRTP include many of the major tobacco, chemical, and drug manufacturing companies. Its leadership consists of corporate and product defense scientists and

attorneys, along with a small number of government scientists who have apparently bought in or who do not know better. The immediate past president was Terry Quill, an attorney who became senior vice president for product defense of the Weinberg Group.<sup>60</sup> Quill also has roots in the tobacco wars but not as a scientific expert. Rather, he served as outside counsel to Philip Morris in the secondhand-smoke litigation.<sup>61</sup>

The editor of *Regulatory Toxicology and Pharmacology* is Gio Gori, well known in the public health community as one of the tobacco industry's most prominent and long-standing defenders—after serving from 1968 to 1980 as director of the National Cancer Institute's highly regarded Smoking and Health Program. Then he changed sides and embarked on a lucrative career defending Big Tobacco on the secondhand smoke issue.<sup>62</sup>

Does the peer-review process at these journals play a role in improving the published papers or do studies of questionable validity move to publication unchallenged? Here is a recent story that speaks volumes. One well-known epidemiologist and corporate consultant recently conducted what is called a meta-analysis, in which several studies on the same exposure were combined into a single large study, theoretically at least more powerful than several smaller ones. The study, which was paid for by PG&E for use in the chromium-contaminated drinking water suits, concluded that, contrary to fifty years of epidemiologic studies, chromium was “only weakly carcinogenic for the lungs.”<sup>63</sup>

Published in *Regulatory Toxicology and Pharmacology*, the study makes the most basic (and fatal) mistake of combining all types of exposure and cancer rates and treating them as comparable. Heavy exposures to airborne chromium among the workers in pigment factories were combined with light exposures among residents of towns with contaminated water. Of course, there was no increased lung cancer risk among the community residents—they were not *breathing* chromium. However, since there were several times more community residents than workers, they were weighted more heavily in the analysis, thereby diluting the effects seen in the worker study and making it appear that chromium was “only weakly carcinogenic for the lungs.” That is an elementary error. The peer reviewers evidently did not mind, though, since the study achieved its product defense purpose for the industry.

Another story also illustrates how polluters use these journals-for-hire to impede public health measures. The International Agency for Research on Cancer is the branch of the World Health Organization devoted to cancer prevention. In February 2006 an IARC advisory panel met to consider whether carbon black, an important industrial chemical that is the foundation for many new “nanoproducts,” should be categorized as a carcinogen. One of the papers that the panel planned to consider was a study that had

found that workers who had been exposed to carbon black had twice the expected risk of lung cancer.<sup>64</sup> The weekend before IARC's meeting was to start, a scientist who was working for the International Carbon Black Association (ICBA) breathlessly delivered to the IARC panel three manuscripts<sup>65-67</sup> that reanalyzed data from that first study. All three of these papers had been first presented at a conference sponsored by the ICBA and held less than *one month* before the IARC meeting.<sup>68</sup> The three new re-analyses had been put into a fast-track (two week) peer review and accepted for publication in the *Journal of Occupational and Environmental Medicine (JOEM)*, whose work appears all too frequently in these pages. I should explain that peer review in a scientific journal generally takes at least several months, sometimes more than a year, and that authors generally revise articles based on reviewers' feedback. As we would surmise, the fast-track papers disputed the causal relationship between carbon black and lung cancer.

The IARC advisory panel voted that carbon black was "possibly carcinogenic" and concluded that, although sufficient evidence for carcinogenicity in animal studies existed, the human evidence was inadequate.<sup>69</sup> Did the three new reanalyses help shape the panel's conclusion? It is hard to say, but it is clear that most of the negative evidence from human studies was provided by the industry. No new independent studies have been undertaken, let alone fast-track peer-reviewed.

Skewed studies produced for the most mercenary of purposes are now accepted as part of the game. I saw this at the Department of Energy. Regarding the beryllium industry's advocacy briefs masquerading as scientific papers (they had been published in peer-review journals, after all), my career colleagues in the department shrugged. "It's all part of the game," they said. "We know what these papers are worth." The lack of outrage by honest scientists and regulators is distressing. The late senator Daniel Patrick Moynihan had a phrase for it—he called it "defining deviancy down."<sup>70</sup> Conduct that was once considered unacceptable and that *should* be considered unacceptable is no longer stigmatized or even acknowledged as being corrupt. Moreover, some scientists and certainly most nonscientists (including reporters, judges, juries, and members of Congress) do *not* know what those papers are worth. They are often fooled—which is the whole idea.

\* \* \*

Polluters and manufacturers of dangerous products also fund think tanks and other front groups that are well known for their antagonism toward regulation and devotion to "free enterprise" and "free markets." There are dozens of these organizations working on behalf of just about every significant industry in this country. Some of the ones leading the fight on behalf of corporate interests against public health and environmental regulation are familiar: the Heritage Foundation, Washington Legal Foundation, American

Enterprise Institute for Public Policy Research, Cato Institute, Competitive Enterprise Institute, Hudson Institute, Progress and Freedom Foundation, and Citizens for a Sound Economy, to name a few. Each year these think tanks, along with a host of smaller, lesser-known ones, collect millions of dollars from regulated companies to promote campaigns that weaken public health and environmental protections.

These broad public-policy groups rarely pretend to do science themselves; they generally focus on major regulatory issues. Therefore, the polluting corporations and their trade associations have also set up a different stratum of think tanks and front groups they can rely on to churn out predictable, authoritative-looking reports that cull the friendly science commissioned by the companies themselves. These reports are aimed at legislators, the press, and the public. They always question the science regarding specific hazards (generally those created by their funders). For example, the Council on Water Quality pretends to ensure that the “best available science drives government actions on setting standards for perchlorate in water.”<sup>71</sup> As previously mentioned, this rocket fuel additive is now contaminating groundwater supplies around the nation. Lockheed Martin and other polluters that are facing the huge cost of cleaning up contaminated aquifers provide the council’s funding.<sup>72</sup> The group is run by staff at APCO Worldwide, the public relations giant that has done similar work for Big Tobacco, so consider the source when judging the claim that “[s]cientific research shows low levels of perchlorate are harmless.”<sup>71</sup> In fact, an analysis by the National Academy of Sciences found that perchlorate causes thyroid damage, especially in infants, at fairly low exposure levels.<sup>18</sup>

The Center for Media and Democracy keeps tabs on these front groups on the web<sup>73</sup> and in a series of invaluable books written by Sheldon Rampton and John Stauber.<sup>74-75</sup> One of the groups they are following is the Center for Consumer Freedom, which uses funding from the food and restaurant industries to attack studies that link fat consumption to obesity.<sup>76</sup> The same group started FishScam to promote the idea that mercury in fish does not pose a danger to pregnant women.<sup>77</sup>

Another of these cleverly named organizations is the Foundation for Clean Air Progress. This group issues regular reports showing how pristine our environment is, questioning why anyone would want to strengthen the laws responsible for such excellent air. The organization is run by Burson-Marsteller, the PR firm, using funds provided by the petroleum, trucking, and other polluting industries.<sup>78</sup>

The Annapolis Center for Science-Based Policy was started by a vice president of the National Association of Manufacturers for, among other purposes, fighting the EPA’s Clean Air standards.<sup>79</sup> It is heavily funded by ExxonMobil (\$688,575 between 1998 and 2005)<sup>80,81</sup> and large coal-burning

utilities like the Southern Co. (\$325,00 in 2003–2004).<sup>82,83</sup> A “key finding” of one Annapolis Center report states that “No one knows whether controlling [airborne particles] will actually yield net benefits to public health. Further regulation of PM is thus premature.”<sup>84</sup> This has become the mantra of the big coal-burning power companies as they oppose further regulation of these particulates.<sup>85,86</sup> It is an indefensible assertion. While we cannot ethically set up a study in which we expose some people to high levels of these particulates (called PM, or particulate matter), the equivalent natural experiment happens all of the time. One of the most famous was studied by Arden Pope, a researcher at Brigham Young University who was conducting a long-term study of air pollution in Provo, Utah, in the 1980s. As his luck would have it, his research period covered a full year in which the big steel mill in Provo, which accounted for 80 percent of the region’s airborne PM, was idled by a labor strike. In that year, the mortality rate and hospitalizations dramatically *decreased*. Once the strike was settled and the PM pollution from the steel mill resumed, mortality and hospitalization rates went back up.<sup>87</sup> The cause-effect relationship could not have been clearer.

So many studies have linked exposure to airborne PM levels and increased risk of death, hospitalization, and emergency room and clinic visits that the editor of the journal *Epidemiology*, Dr. Jonathan Samet, a distinguished scientist and chairman of the Department of Epidemiology at the Johns Hopkins Bloomberg School of Public Health, told scientists to stop submitting new studies on this topic. So many had already been published that new ones would add little of value to the scientific literature; the pages of Dr. Samet’s journal could better be devoted to other topics.<sup>88</sup> We do not know everything about PM, but we know enough to be very confident that reducing the concentrations will prevent tens of thousands of deaths each year.<sup>89–91</sup>

\* \* \*

Let’s face it, the work product of the product defense industry is impressive. Carefully manicured reports and reanalyses, captured journals full of “peer-reviewed” articles, and captured think tanks hiring out their ad hoc advocacy sow uncertainty across a range of issues. Perhaps the sleaziest behavior of all, though, is their practice of denigrating scientists and studies whose findings do not serve the corporate cause. Today the most prominent and effective public face and front for this component of the attack on science is the “junk science” movement, whose sole purpose is to ridicule research that threatens powerful interests, irrespective of the quality of that research. Peter Huber, based at the Manhattan Institute, is often credited with coining the term, as I mentioned in the introduction. I would like to repeat Huber’s rough-and-ready description of junk science in his book *Galileo’s Revenge: Junk Science in the Courtroom*: “Junk science is the mirror image of real science, with much of

the same form but none of the substance. . . . It is a hodgepodge of biased data, spurious inference, and logical legerdemain. . . . It is a catalog of every conceivable kind of error: data dredging, wishful thinking, truculent dogmatism, and, now and again, outright fraud.”<sup>92</sup>

Orwellian indeed, as I stated in the introduction, but unquestionably the corporations and the product defense industry they fund have done a superb job in marketing the “sound science” slogan and thereby undermining the use of scientific evidence in public policy. The junkscience.com website lists a roster of “junk scientists,” including six elected members of the Institute of Medicine and four recipients of the highest honor bestowed by the American College of Epidemiology, so it appears that scientists who are asked to identify *their* most outstanding colleagues do not share the opinions of the promoters of the “junk science” label.<sup>93</sup>

The opposite of junk science is, of course, “sound science.” Rarely is the one invoked as bad without an immediate reference to the other as the ideal. The first entity to carry the official “sound science” flag was The Advancement of Sound Science Coalition (TASSC), which was “dedicated to ensuring the use of sound science in public policy decisions.”<sup>94,95</sup> This front organization was set up by APCO Associates, one of Philip Morris’s PR firms.<sup>96</sup> (Elisa Ong and Stanton Glantz described the founding role of tobacco in the sound science movement in the November 2001 issue of the *American Journal of Public Health*.<sup>97</sup>) Steven Milloy, the first executive director of TASSC, had formerly worked for Multinational Business Services, a firm run by Jim Tozzi, perhaps the premier antiregulatory tactician. Ultimately TASSC served its purpose and is now defunct, and Milloy has moved on to his own website, [www.junkscience.com](http://www.junkscience.com).

A representative “sound science” credo is this one from a TASSC press release, which quotes Dr. Margaret Maxey, director of the Clint W. Murchison Chair of Free Enterprise and professor of bioethics at the University of Texas: “More and more [science is] being used to justify preconceived agendas. Too often, public policy decisions that are based on inadequate science impose enormous economic costs and other hardships on consumers, businesses and government.”<sup>95</sup> The usual figure provided for the annual cost of “regulations” has been in excess of \$40 billion.<sup>98</sup> One of industry groups’ favorite examples of costly policy is the Clean Air Act. Another TASSC authority, Floy Lilley, also of the University of Texas, had this to say in denouncing that regulation: “The Clean Air Act is a perfect example of laboratory science being superficially applied to reality. If it were reflective of reality, based on current government studies, medical examiners would find evidence of effects in lungs that are irreversible and life-threatening. This simply has not happened. And now we must wonder if the cost of the Clean Air Act is justified by alleged health benefits.”<sup>95</sup>



In the fact-based world, the Clean Air Act has been one of the most successful modern public health regulations by preventing tens of thousands of illnesses and premature deaths and millions of asthma attacks.<sup>99</sup> Even the cost-benefit doyens of the second Bush administration, perhaps the most fervent opponents of regulation ever to occupy the White House, have estimated that its benefits outweigh its costs by somewhere between \$50 billion and \$400 billion.<sup>98</sup> But is anyone really surprised that it is subjected to ridiculous attacks? As comedian Lily Tomlin said, “No matter how cynical you become, it’s never enough to keep up.”<sup>100</sup>

# EXHIBIT 2

Text -A A +A Google Translate RSS Feeds

Con

Recovery.gov is the U.S. government's official website that provides easy access to data related to Recovery Act spending and allows for the reporting of potential fraud, waste, and abuse.

Looking For ? HOME ABOUT ACCOUNTABILITY WHERE IS THE MONEY GOING? OPPORTUNITIES NEWS F

Home > Where is The Money Going? > Recipient Data > Recipient Project Summary

Overview of Funding

Recipient Data

Projects Map

Recipient Profile

Quarterly Summary

State/Territory Summaries

Jobs Summary

State/Territory Totals by Award Type

State/Territory Totals by Agency

Changed Reports

Recovery Explorer

Map Gallery

Agency Data

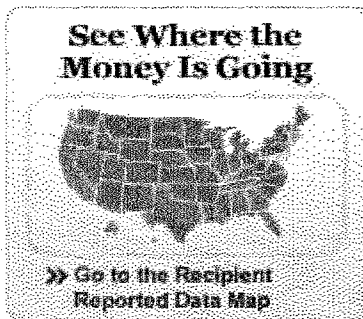
### GRANTS - AWARD SUMMARY

#### NV ENERGY, INC.

NV Energy's Smart Grid Investment Grant Program, initially called the Advanced Service Project (ASD) now referred to as the NVEnergize Project, is a large project in the Integrating Cross-Cutting Systems Topic Area that supports a major dynamic pricing trial, and will be implemented from 2010-2012, link 1.45 million electric and gas meters across square miles of service territory, and benefit 2.4 million Nevadans. From Nevada's north to its southern deserts, weather, customer types, and load factors are extremely diverse this challenge with an integrated, reliable, safe and scalable Smart Grid foundation. Creating streamlined operations, and reducing peak demand, ASD integrates dynamic pricing, communications, grid situational awareness, home area networks, demand response, distribution automation, distributed renewables, and electric vehicles. The secure and proven ASD includes the Advanced Metering Infrastructure, the Meter Data Management System, the Demand Response Management System, and the Demand Response Management System - including in-home and programmable controllable thermostats. NV Energy (NVE) will build a Smart Grid for an open model for the utility industry, sharing how customers take ownership of their energy. The entire State of Nevada will benefit as a result. The DOE approved additional funding above the previously approved \$137.8 million for work NV Energy will undertake for Confidentiality activities.

Choose a quarter and click "Go."

January 1 - March 31, 2012



#### AWARD OVERVIEW

|                    |               |                          |                      |
|--------------------|---------------|--------------------------|----------------------|
| Award Number       | OE0000205     | Funding Agency           | Department of Energy |
| Total Award Amount | \$138,877,906 | Project Location - City  | Las Vegas            |
| Award Date         | 12/24/2009    | Project Location - State | NV                   |

|                            |                         |                        |            |
|----------------------------|-------------------------|------------------------|------------|
| Project Status             | More than 50% Completed | Project Location - Zip | 89146-3060 |
| Jobs Reported              | 102.99                  | Congressional District | 03         |
| Project Location - Country | US                      |                        |            |

**RECIPIENT INFORMATION (GRANTS)**

|   |                   |
|---|-------------------|
| Recipient Name  | NV ENERGY, INC.   |
| Recipient DUNS Number                                 | 121809347         |
| Recipient Address                                     | 6226 W SAHARA AVE |
| Recipient City  | LAS VEGAS         |
| Recipient State                                       | Nevada            |
| Recipient Zip   | 89146-3060        |
| Recipient Congressional District                      | 03                |
| Recipient Country                                     | USA               |
| Required to Report Top 5 Highly Compensated Officials | No                |

**PROJECTS AND JOBS INFORMATION**

|  |   |
|--|---|
| Project Title                            | NV Energy, Smart Grid Investment Grant Program (EISA 1306), Advanced Service Delivery (a.k.a. NVEnergize), 2006000  |
| Project Status                           | More than 50% Completed   |
| Final Project Report Submitted           | No  |
| Project Activities Description           | Energy Resources  |
| Quarterly Activities/Project Description | First qtr 2012 activities: In January, the PUCN held its second workshop to discuss comments and recommendations to non-standard metering options. In February, the PUCN determined a trial opt-out program is warranted to determine the need for a permanent non-standard metering option. NV Energy (NVE) has 60 days to file a trial opt-out program. The program will include digital meters capable of drive-by meter reading. Customers who choose to opt-out will bear the full costs. The trial will have a 12-month test year. The PUCN concluded NVE's program has taken reasonable and appropriate steps to ensure the AMI network is safe, secure, private and accurate. During the qtr, System Release 7.7 was deployed adding Register Read Billing and Portal functionalities to NVE's northern service territory, enabling NVE to begin route cutover for operational benefits as meters are |

deployed. Sector Acceptance Testing continued in both service territories. Employee Acceptance Testing continued throughout the qtr in NVE's southern service territory of In-Home Display devices and Programmable Communicating Thermostats. 79,586 meters were deployed in the qtr in NVE's southern service territory; totaling 774,889 smart meters installed in southern Nevada as of Mar 31. Mass deployment of smart meters began in Jan in NVE's northern service territory resulting in 21,465 meters deployed during the qtr totaling 21,519 smart meters installed in northern Nevada as of Mar 31, 2012. No new Tower Gateway Base Stations (TGBs) were commissioned in NVE's southern service territory; therefore, no change to the total of 67 TGBs commissioned as of Mar 31; five sites are in various stages of construction and will be commissioned in the next several months. Additionally, four new TGBs were completed and commissioned in the qtr in NVE's northern service territory; totaling 17 as of Mar 31, 2012; 25 additional sites are in various stages of construction and will be commissioned in the next several months.

|                             |  |
|-----------------------------|--|
| Jobs Created                | 102.99   |
| Description of Jobs Created | During the first quarter of 2012, meter installation contractor, Scope Services, created 46 new positions. The 46 new positions were added to support smart meter deployment in NVE's northern Nevada service territory. |

**PURCHASER INFORMATION (GRANTS)**

|                           |               |
|---------------------------|---------------|
| Contracting Office ID     | Not Reported  |
| Contracting Office Name   | Not Available |
| Contracting Office Region | Not Available |
| TAS Major Program         | 89-0328       |

**AWARD INFORMATION**

|                     |                      |
|---------------------|----------------------|
| Award Date          | 12/24/2009           |
| Award Number        | OE0000205            |
| Order Number        |                      |
| Award Type          | Grants               |
| Funding Agency ID   | 89                   |
| Funding Agency Name | Department of Energy |
| Funding Office Name | Not Available        |
| Awarding Agency ID  | 89                   |

|   |                      |
|---|----------------------|
| Awarding Agency Name                    | Department of Energy |
| Amount of Award                         | \$138,877,906        |
| Funds Invoiced/Received                 | \$94,261,767         |
| Expenditure Amount                      | \$105,862,210        |
| Infrastructure Expenditure Amount       | \$0                  |
| Infrastructure Purpose and Rationale    | Not Reported         |
| Infrastructure Point of Contact Name    | Not Reported         |
| Infrastructure Point of Contact Email   | Not Reported         |
| Infrastructure Point of Contact Phone   | Not Reported         |
| Infrastructure Point of Contact Address | Not Reported         |
| Infrastructure Point of Contact City    | Not Reported         |
| Infrastructure Point of Contact State   | Not Reported         |
| Infrastructure Point of Contact Zip     | Not Reported         |

### PRODUCT OR SERVICE INFORMATION (GRANTS)

|                       |                  |
|-----------------------|------------------|
| Primary Activity Code | C05.02           |
| Activity Description  | Energy Resources |

### SUB-AWARDS INFORMATION

|   |              |
|---|--------------|
| Sub-awards to Organizations                                     | 0            |
| Sub-award Amounts to Organizations                              | \$0          |
| Sub-Awards to Individuals                                       | 0            |
| Sub-Award Amounts to Individuals                                | \$0          |
| Number of Sub-awards less than \$25,000/award                   | 0            |
| Amount of Sub-awards less than \$25,000/award                   | \$0          |
| Number of payments to vendors greater than \$25,000             | 46           |
| Total Amount of payments to vendors greater than \$25,000/award | \$33,843,418 |
| Number of payments to vendors less than \$25,000/award          | 1587         |
| Total Amount of payments to vendors less than \$25,000/award    | \$3,307,766  |

### VENDOR TRANSACTIONS

- Award Number OE0000205 -

Award Number OE0000205  
 Sub-Award Number N/A  
 Vendor DUNS Number 960236649  
 Vendor HQ Zip Code + 4  
 Vendor Name  
 Product and Service Description Consultation on RF Health Impact  
 Payment Amount \$14,677

- Award Number OE0000205 -

Award Number OE0000205  
 Sub-Award Number N/A  
 Vendor DUNS Number 033211457  
 Vendor HQ Zip Code + 4  
 Vendor Name  
 Product and Service Description HAN Implementation  
 Payment Amount \$15,103

- Award Number OE0000205 -

Award Number OE0000205  
 Sub-Award Number N/A  
 Vendor DUNS Number 015837996  
 Vendor HQ Zip Code + 4  
 Vendor Name  
 Product and Service Description Research and Development Services for Dynamic Pricing Trial  
 Payment Amount \$13,590

- Award Number OE0000205 -

Award Number OE0000205  
 Sub-Award Number N/A  
 Vendor DUNS Number 021471241  
 Vendor HQ Zip Code + 4  
 Vendor Name  
 Product and Service Description Battery Backup Systems  
 Payment Amount \$45,831

- Award Number OE0000205 -

Award Number OE0000205  
 Sub-Award Number N/A  
 Vendor DUNS Number 025916679  
 Vendor HQ Zip Code + 4  
 Vendor Name  
 Product and Service Description Networking Equipment  
 Payment Amount \$76,264

## - Award Number OE0000205 -

|  |                                     |
|--|-------------------------------------|
| <b>Award Number</b>                    | OE0000205                           |
| <b>Sub-Award Number</b>                | N/A                                 |
| <b>Vendor DUNS Number</b>              | 045659394                           |
| <b>Vendor HQ Zip Code + 4</b>          |                                     |
| <b>Vendor Name</b>                     |                                     |
| <b>Product and Service Description</b> | Review of Benefits Realized to Date |
| <b>Payment Amount</b>                  | \$108,548                           |

## - Award Number OE0000205 -

|  |                            |
|--|----------------------------|
| <b>Award Number</b>                    | OE0000205                  |
| <b>Sub-Award Number</b>                | N/A                        |
| <b>Vendor DUNS Number</b>              | 041054348                  |
| <b>Vendor HQ Zip Code + 4</b>          |                            |
| <b>Vendor Name</b>                     |                            |
| <b>Product and Service Description</b> | Network Equipment Hardware |
| <b>Payment Amount</b>                  | \$140,627                  |

## - Award Number OE0000205 -

|  |                           |
|--|---------------------------|
| <b>Award Number</b>                    | OE0000205                 |
| <b>Sub-Award Number</b>                | N/A                       |
| <b>Vendor DUNS Number</b>              | 202484981                 |
| <b>Vendor HQ Zip Code + 4</b>          |                           |
| <b>Vendor Name</b>                     |                           |
| <b>Product and Service Description</b> | Cyber Security Consulting |
| <b>Payment Amount</b>                  | \$155,063                 |

## - Award Number OE0000205 -

|  |  |
|--|--|
| <b>Award Number</b>                    | OE0000205                                |
| <b>Sub-Award Number</b>                | N/A                                      |
| <b>Vendor DUNS Number</b>              | 029092131                                |
| <b>Vendor HQ Zip Code + 4</b>          |  |
| <b>Vendor Name</b>                     |  |
| <b>Product and Service Description</b> | Portal Software and Integration Services |
| <b>Payment Amount</b>                  | \$174,575                                |

## - Award Number OE0000205 -

|  |  |
|--|--|
| <b>Award Number</b>                    | OE0000205  |
| <b>Sub-Award Number</b>                | N/A  |
| <b>Vendor DUNS Number</b>              | 961609760  |
| <b>Vendor HQ Zip Code + 4</b>          |  |
| <b>Vendor Name</b>                     |  |
| <b>Product and Service Description</b> | Integration Services for Demand Response Management System |
| <b>Payment Amount</b>                  | \$192,422  |



- Award Number OE0000205 -

**Award Number** OE0000205  
**Sub-Award Number** N/A  
**Vendor DUNS Number** 241785666  
**Vendor HQ Zip Code + 4**  
**Vendor Name**  
**Product and Service Description** Specialized system implementation resources and systems integration support  
**Payment Amount** \$4,056,858

Ballard Spahr Andrews & Ingersoll LLP - Award Number OE0000205 - Ballard Spahr Andrews & Ingersoll LLP

**Award Number** OE0000205  
**Sub-Award Number** N/A  
**Vendor DUNS Number** 858682644  
**Vendor HQ Zip Code + 4** 84111-2212  
**Vendor Name** Ballard Spahr Andrews & Ingersoll LLP  
**Product and Service Description** Legal Services  
**Payment Amount** \$810,511

Board Of Regents Of The University Of Nevada - Award Number OE0000205 - Board Of Regents Of The University Of Nevada

**Award Number** OE0000205  
**Sub-Award Number** N/A  
**Vendor DUNS Number** 785962689  
**Vendor HQ Zip Code + 4** 89512-1666  
**Vendor Name** Board of Regents of The University of Nevada  
**Product and Service Description** Market research services for NV Energy's Dynamic Pricing Trial  
**Payment Amount** \$47,073

Boice Dunham Group Inc - Award Number OE0000205 - Boice Dunham Group Inc

**Award Number** OE0000205  
**Sub-Award Number** N/A  
**Vendor DUNS Number** 112993720  
**Vendor HQ Zip Code + 4** 10011-7912  
**Vendor Name** Boice Dunham Group Inc  
**Product and Service Description** Program design and market research services for NV Energy's Dynamic Pricing Trial  
**Payment Amount** \$372,206

Comverge, Inc - Award Number OE0000205 - Comverge, Inc

**Award Number** OE0000205  
**Sub-Award Number** N/A  
**Vendor DUNS Number** 014998479

**Vendor HQ Zip Code + 4** 94560-5355  
**Vendor Name** Comverge, Inc  
**Product and Service Description** Program Integration and Management Resources  
**Payment Amount** \$175,000

Dell Marketing L.P. - Award Number OE0000205 - Dell Marketing L.P.

**Award Number** OE0000205  
**Sub-Award Number** N/A  
**Vendor DUNS Number** 078626715  
**Vendor HQ Zip Code + 4** 91185  
**Vendor Name** Dell Marketing L.P.  
**Product and Service Description** Computer Cabinets, SQL Server Licenses  
**Payment Amount** \$258,118

Deloitte & Touche L.L.P. - Award Number OE0000205 - Deloitte & Touche L.L.P.

**Award Number** OE0000205  
**Sub-Award Number** N/A  
**Vendor DUNS Number** 152155065  
**Vendor HQ Zip Code + 4** 89501-1949  
**Vendor Name** Deloitte & Touche L.L.P.  
**Product and Service Description** A-133 Audit, Smart Grid Investment Grant  
**Payment Amount** \$32,663

Digital Prototype Systems Inc - Award Number OE0000205 - Digital Prototype Systems Inc

**Award Number** OE0000205  
**Sub-Award Number** N/A  
**Vendor DUNS Number** 173818949  
**Vendor HQ Zip Code + 4** 93727-1523  
**Vendor Name** Digital Prototype Systems Inc  
**Product and Service Description** Networking Security Equipment  
**Payment Amount** \$26,037

Enspira Solutions, Inc - Award Number OE0000205 - Enspira Solutions, Inc

**Award Number** OE0000205  
**Sub-Award Number** N/A  
**Vendor DUNS Number** 861469526  
**Vendor HQ Zip Code + 4** 80111-4980  
**Vendor Name** Enspira Solutions, Inc  
**Product and Service Description** Overall program integration and program management resources  
**Payment Amount** \$4,576,600

Exponent, Inc. - Award Number OE0000205 - Exponent, Inc.

**Award Number** OE0000205  
**Sub-Award Number** N/A

|                                 |                                  |
|---------------------------------|----------------------------------|
| Vendor DUNS Number              | 168343346                        |
| Vendor HQ Zip Code + 4          | 77099-3465                       |
| Vendor Name                     | Exponent, Inc.                   |
| Product and Service Description | Consultation on RF Health Impact |
| Payment Amount                  | \$63,249                         |

<< < 1 2 3 > >>

**PROJECT LOCATION DETAIL**

|                        |                           |
|------------------------|---------------------------|
| Latitude, Longitude    | 36° 8' 39", -115° 13' 40" |
| Congressional District | 03                        |
| Address 1              | 6226 West Sahara Avenue   |
| Address 2              |                           |
| City                   | Las Vegas                 |
| County                 | Clark                     |
| State                  | NV                        |
| Zip                    | 89146-3060                |

**RECOVERY.GOV & THE BOARD**

- Read The Recovery Act
- What Is The Recovery Board?
- What Does The Recovery Board Do?
- What Is Recovery.gov?
- Inspectors General Reports

**LOOKING FOR...**

- Projects In My Neighborhood
- Opportunities & Benefits
- Job Information
- Details About A Recipient
- Funding By Program / Category

**I AM...**

- An Interested Citizen
- A Data User
- A Member Of The Media
- A Recipient

**SPECIAL FEATURES**

- Edward Tufte Lights On Map
- Comparison Maps
- Recovery Data Explorer
- Map Gallery

**SITE INDEX**

**REPORT FRAUD, WASTE OR ABUSE**

**SUBSCRIBE TO MONTH-IN-REVIEW EMAIL**

**LOOK CLOSER AT RECOVERY DATA**

- Create Charts And
- Search All Recover
- Find Details About
- Use Recovery Widg
- Get The Recovery i
- iPad App

# EXHIBIT 3



California  
Public Utilities  
Commission



[CPUC Home](#)

[Word Document](#) [PDF Document](#)

COM/MP1/avs **DRAFT Agenda ID #10870 (Rev. 3)**

**Ratesetting**

**2/1/2012 Item 28**

Decision **PROPOSED DECISION OF COMMISSIONER PEEVEY**

**(Mailed 11/22/2011)**

**BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA**

Application of Pacific Gas and Electric Company for Approval of Modifications to its SmartMeter™ Program and Increased Revenue Requirements to Recover the Costs of the Modifications. (U39M)

Application 11-03-014

(Filed March 24, 2011)

**DECISION MODIFYING PACIFIC GAS AND ELECTRIC COMPANY'S SMARTMETER PROGRAM TO INCLUDE AN OPT-OUT OPTION**

**TABLE OF CONTENTS**

**Title Page**

**DECISION MODIFYING PACIFIC GAS AND ELECTRIC COMPANY'S 22**

**SMARTMETER PROGRAM TO INCLUDE AN OPT-OUT OPTION 22**

**1. Summary 22**

**2. Background 33**

**3. PG&E's Application 66**

**4. Opt-Out Plan 77**

**4.1. Parties' Positions 99**

**4.2. Discussion 1111**

**5. Cost of Opt-Out Plan 2121**

**5.1. Parties' Comments 2323**

**5.2. Discussion 2424**

**6. Cost Recovery for the Opt-Out Plan and Rate Structure 2626**

**6.1. Parties' Comments 2828**

## 6.2. Discussion 2929

## 7. Next Steps 3333

## 8. Comments on Proposed Decision 3636

### Findings of Fact 3636

### Conclusions of Law 3737

### ORDER 3939

## **DECISION MODIFYING PACIFIC GAS AND ELECTRIC COMPANY'S SMARTMETER PROGRAM TO INCLUDE AN OPT-OUT OPTION**

### **1. Summary**

This decision modifies Pacific Gas and Electric Company's (PG&E) SmartMeter Program to include an option for residential customers who do not wish to have a wireless SmartMeter installed at their location. The opt-out option shall be an analog electric and/or gas meter.

This new opt-out option is a service that we are adopting with this decision. This opt-out option is a service because the standard for metering has been transitioned throughout the country and for the most part the world from the older technology, analog meters, to today's technology, SmartMeters. In this decision we are not reversing that transition, however, we do approve an option for those customers who, for whatever reason, would prefer an analog meter. This option to move away from the standard will require PG&E to incur costs such as purchasing a new meter, going back to the customer location to install and service the meter, and monthly cost of reading the meter. These are some of the examples of the additional costs required to opt-out of the standard wireless SmartMeters. As a result, this decision further finds that customers electing the opt-option shall be responsible for costs associated with providing the option. Issues concerning the actual costs associated with offering the analog opt-out option and whether some portion of these costs should also be allocated to all ratepayers or PG&E shareholders will be addressed in a separate phase of this proceeding.

To allow residential customers to begin selecting the opt-out option immediately, this decision adopts interim fees and charges, which will be subject to adjustment upon conclusion of the second phase of this proceeding. A Non-CARE customer electing the opt-out option shall be assessed an initial fee of \$75.00 and a monthly charge of \$10.00. A CARE customer electing the opt-out option shall be assessed an initial fee of \$10.00 and a monthly charge of \$5.00.

This decision also authorizes PG&E to establish new two-way electric and gas Modified SmartMeter Memorandum Accounts to track revenues and costs associated with providing the opt-out option until a final decision on recoverable costs and cost allocation is adopted.

This decision further directs PG&E to file a Tier 1 Advice Letter implementing the opt-out option and to establish a SmartMeter Opt-Out Tariff within 15 days of the effective date of this decision. Finally, the September 21, 2011 Assigned Commissioner's Ruling directing PG&E to establish a delay list shall no longer be in effect and all customers currently on the delay list shall be transitioned to a wireless SmartMeter unless they elect to participate in the opt-out option. This proceeding remains open to address cost issues associated with the opt-out option.

### **2. Background**

On March 24, 2011, Pacific Gas and Electric Company (PG&E) filed Application (A.) 11-03-014 seeking Commission approval of modifications to its SmartMeter Program, and an increase in revenue requirements to recover the costs of implementing the modifications. PG&E's application was filed in response to a directive by Commissioner Peevey to submit a proposal that would allow some form of opt-out for PG&E customers who did not wish to have a SmartMeter with radio frequency (RF) transmission. This is referred to in this proceeding as "opting out."

PG&E proposes that the SmartMeter Program be modified to provide residential customers the choice to request that PG&E "turn-off"/disable the radio inside their gas and/or electric SmartMeters, thus eliminating the RF communications from the SmartMeters. This has been referred to as the "radio off" option. It further proposes that it be allowed to recover

the associated costs from customers electing to opt out through an up-front fee, monthly charges, and an "exit" charge when a customer leaves the premises. The revenue requirements to recover these costs are estimated to be \$113.4 million for the two-year period of 2012-2013.

Timely protests were filed by the Ecological Options Network (EON), County of Lake (Lake), County of Mendocino (Mendocino), Aglet Consumer Alliance (Aglet), EMF Safety Network (Network), The Utility Reform Network (TURN), jointly by the Town of Fairfax, the Alliance for Human and Environmental Health and the County of Marin (jointly, Fairfax), Wilner and Associates (Wilner), and Alameda County Residents Concerned About Smart Meters (Alameda). The Division of Ratepayer Advocates (DRA) filed a timely response to PG&E's application.

A prehearing conference (PHC) was held on May 6, 2011. Shortly thereafter, an Assigned Commissioner Ruling and Scoping Memo (Scoping Memo) was issued on May 25, 2011. As identified in the Scoping Memo, the issues to be considered are:<sup>1</sup>

1. Whether PG&E's proposed radio-off option is reasonable.
2. Whether the proposed costs for PG&E's opt-out proposal are reasonable.
3. Whether PG&E's proposed cost recovery is reasonable.

A second PHC was held on July 27, 2011. Based on discussion at this second PHC, a combined workshop was scheduled to discuss the possible opt-out options for PG&E, Southern California Edison Company (SCE), San Diego Gas & Electric Company (SDG&E) and Southern California Gas Company (SoCalGas).

The combined workshop was held on September 14, 2011. At the workshop, parties discussed the following possible options, in addition to the radio off option, that might be offered to customers wishing to opt out of having a wireless SmartMeter installed:

1. Install a digital meter with no communication capability (referred to as 'radio out' option).
2. Analog meters - retention where a wireless SmartMeter has not been installed or installation of analog meters to replace a wireless SmartMeter.
3. Install a digital meter with wired (e.g., copper wire, fiber optic) transmission capability.

This discussion included the estimated costs and the technological feasibility of offering each of the different options.

In response to comments made at the workshop, the assigned Administrative Law Judge (ALJ) issued rulings directing PG&E to provide additional information concerning costs and RF emissions.<sup>2</sup> Additionally, the Assigned Commissioner issued a ruling on September 21, 2011 specifying the minimum requirements that PG&E, SCE and SDG&E must follow in response to customer requests to delay the installation of a wireless SmartMeter.<sup>3</sup>

### **3. PG&E's Application**

PG&E's electric SmartMeters include two low-power radios embedded in the meter that are capable of both transmitting and receiving a signal through the radio. One radio is used to communicate with PG&E over its SmartMeter electric mesh network. This radio communicates to local collectors called Access Points (AP) which communicate that information back to PG&E's system. The second radio is currently off and would be used only if the customer affirmatively decides to implement an integrated Home Area Network (HAN). PG&E's gas SmartMeters have a single radio, which is used to transmit a low power radio frequency signal to a Distribution Collection Unit (DCU) The DCU collects data from local meters and then communicates back to PG&E's systems.

PG&E proposes to offer the following opt-out options to customers:<sup>4</sup>

1. Radio off - Residential electric and gas customers would be eligible to request that the wireless radios embedded in the SmartMeter be "turned off"

(deactivated).

**2. Relocation - Electric customers may request that PG&E relocate the electric SmartMeter to a different location on the customer's property.<sup>5</sup>**

PG&E estimates the costs to implement the radio off option to be \$113.4 million for the years 2012 and 2013, assuming 148,500 customers will elect to opt out.<sup>6</sup> It proposes that these costs be recovered from those customers choosing to opt-out of a wireless SmartMeter through the assessment of an up-front fee covering all or a portion of PG&E's immediate costs of implementing the opt-out option, monthly fees covering ongoing monthly expenses and an "exit fee" upon termination of participation in the opt-out option.

**4. Opt-Out Plan**

PG&E states that it had evaluated various opt-out alternatives, and determined that the radio-off alternative was the most feasible and could be offered at a reasonable cost.<sup>7</sup> It further states that other alternatives evaluated were a wired meter and a legacy (analog) meter.

A combined workshop to consider opt-out alternatives for all of the investor owned utilities was held on September 14, 2011.<sup>8</sup> The following opt-out alternatives were considered:

- 1. Analog meter - Under this option, an electromechanical (analog) meter would be used in place of the wireless SmartMeter. This option would require the meter to be read manually every month.**
- 2. Digital meter with no radio installed - Under this option, a digital meter, with no radio communications ability, would be used in place of the wireless SmartMeter. Some of these meters may be able to store interval energy consumption data. This option would require the meter to be read manually every month.**
- 3. SmartMeter with radio transmission turned off - PG&E's proposed alternative, this option would retain the existing SmartMeter, but have the radio communications ability turned off. Under this option, the meter would need to be read manually every month.**
- 4. Wired smart meter - Under this option, interval energy consumption data would be transmitted to the utility through a traditional telephone line, fiber optic, a power line carrier or other wired technologies. Since this option would allow the meter to communicate with the utility, the meters would not need to be read manually every month. This option is not available for gas meters.**

PG&E states that the radio off option will not affect the accuracy of electric usage measurement. However, under this option, certain electric SmartMeter functions would be disabled. These would include:<sup>9</sup>

- 1. Hourly interval data of electric energy usage or daily gas usage.**
- 2. Any tariff or demand response program which requires interval data.**
- 3. Customer account internet presentment of interval data.**
- 4. Remote service connect/disconnect capability.**



5. Real-time meter diagnostic alarms and health assessment checks.
6. Real-time monitoring for security events on the metering device.
7. The ability for remote installation of meter or communication board firmware which may be required for upgradability.
8. Outage information and power status.
9. Time-of-Use (TOU) profiled energy usage data collection and access to any tariff that requires a device to collect TOU data.
10. Home Area Network (HAN) connectivity inside the home and access to any tariff or program that requires HAN in its application.

#### **4.1. Parties' Positions**

PG&E maintains that the radio off option is the most practical solution available because it optimizes the SmartMeters already deployed and additional SmartMeters already purchased for future deployment. It further states that the radio off option provides greater flexibility when customers choosing the opt-out option move or sell their homes. PG&E contends that the current options for offering a smart meter with wired communications are not technologically feasible as they are not available for gas meters and are limited to approximately 30,000 meters.<sup>10</sup> Additionally, PG&E argues that it makes no sense to offer a non-communicating SmartMeter (i.e., one with no radio unit installed), since that meter would serve the same function as a SmartMeter with the radio off. Finally, PG&E maintains that the analog meter opt-out option is not feasible, as these meters are no longer being manufactured. Moreover, PG&E states that offering an electric analog meter option is inconsistent with California's energy policy to implement mandatory TOU rates for residential customers, as analog meters cannot provide interval energy-consumption data.<sup>11</sup>

Many of the parties oppose PG&E's proposed option. Among other things, parties contend that the radio off option would not address the concerns raised by customers regarding the effect of RF emissions on health.<sup>12</sup> Network, EON and Fairfax all further assert that radio transmission is just a small part of the RF emissions from the SmartMeter. They maintain that even with the radio off, the SmartMeter still emits RF emissions. Consequently, they argue that an analog meter is the only feasible opt-out option.<sup>13</sup>

While DRA is generally supportive of PG&E's proposed opt-out option, it believes that the Commission should also consider whether the SmartMeters comply with the Federal Communication Commission's (FCC) guidelines.<sup>14</sup> It further notes that the Commission should consider the "functional requirements for alternative metering systems used by customers who opt out" in order to preserve the benefits of the SmartMeter system.<sup>15</sup>

Lake argues that widespread installation of SmartMeters could lead to violations of FCC compliance requirements.<sup>16</sup> It further alleges that the SmartMeters adversely affect the environment and overburden utility easements. Consequently, Lake asserts that installation of SmartMeters should be subject to review under the California Environmental Quality Act (CEQA)

(Public Resources Code §§ 21000 and 21001).<sup>17</sup>

TURN believes that while the radio off option may address the concerns expressed by customers regarding RF emissions and privacy, it would not resolve concerns over the accuracy of the meters.<sup>18</sup>

Network, EON and Fairfax further maintain that any opt-out option should also be made available to local governments (town and counties) that have enacted ordinances for community-wide opt-out.<sup>19</sup> Network also asserts that a radio off option is not acceptable because there is no assurance that the SmartMeter is actually turned off.<sup>20</sup>

## **4.2. Discussion**

PG&E's proposed radio off option is one of four possibilities that could be offered to residential customers who do not wish to have a wireless SmartMeter. While PG&E has argued that this option is the most feasible, we cannot ignore parties' comments questioning whether this option best addresses the concerns raised by customers. As evidenced by the numerous speakers at Commission meetings, letters to Commissioners and the ALJ, and comments made by parties and other individuals at the September 14 workshop, there is a great deal of concern that the radio off option would not reduce the level of RF emissions. In response to those concerns, the ALJ issued a ruling seeking information on the RF emissions under the various options.<sup>21</sup> Among other things, the ALJ's October 18<sup>th</sup> Ruling asked for both the average duration and duration of communications between the electric and gas SmartMeters with the utility and level of RF emissions at those times. The ALJ's Ruling also sought information comparing the level of RF emissions from a SmartMeter with the radio off, from a digital meter with no communications capability, and from an analog meter.

PG&E's responses to the questions in the ALJ's October 18<sup>th</sup> Ruling were filed on November 1, 2011. These responses directly address some of the more controversial questions that the Commission heard at the September 14<sup>th</sup> workshop, during the Public Comment period at Commission meetings, in letters to Commissioners, and/or calls to the ALJ and our Consumer Affairs Branch.

One of the more controversial disputes raised during the September 14<sup>th</sup> workshop was how many times in total (average and maximum) an electric SmartMeter transmits during a 24-hour period. At the workshop, PG&E stated that the cumulative transmission time was 45 seconds per day, while other parties maintained that the transmission was constant. PG&E's response reveals that the total average transmission duration is 45.3 seconds, while the maximum is about 15 minutes during a 24-hour time period.<sup>22</sup> PG&E's vendor, Silver Spring Network, reports that a typical electric SmartMeter will communicate for about 45 seconds per day not 15 minutes. However, in instances in which the network is not complete, then the meter may attempt to communicate with the network more often resulting in a maximum duty cycle of 15 minutes.<sup>23</sup>

PG&E also includes in its November 1<sup>st</sup> response the FCC's response to a request for the FCC to step in and ask for the removal of SmartMeters. The FCC said:

As general background information, the FCC's exposure limits are derived from recommendations from human exposure to RF fields by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) and the National Council on Radiation Protection and Measurements (NCRP), and by the U.S. Environmental Protection Agency (EPA), the Food and Drug Administration (FDA) and other federal health and safety agencies. These recommendations were developed by scientists and engineers with extensive experience and knowledge in the area of RF biological effects and related issues. The exposure limits were developed to ensure that FCC regulated transmitters do not expose the public or workers to levels of RF energy that are considered by expert organizations to be potentially harmful.

In the case of SmartMeters, the FCC has no data or report to suggest that exposure is occurring at levels of RF energy that exceed our RF exposure guidelines. In contrast, the California Council on Science and Technology recently released a report that found that "[s]cientific studies have not identified or confirmed negative health effects from potential non-thermal impacts of RF emissions such as those produced by existing common household electronic devices and smart meters." With no indication that the SmartMeters in question might not comply with FCC exposure limits we have no reason or authority to order them removed or their operation discontinued.

RF measurements reported by others indicate that Smart Meters produce exposure of no more than 65% of the FCC limit at the face of the meter when programmed to transmit continuously. The devices normally transmit for less than a one second a few times each day and consumers are normally tens of feet or more from the meter face, so the actual exposures are typically thousands of times less than this "worse case" measurement condition.<sup>24</sup>

Another issue that was the topic of intense discussion during the workshop was whether the SmartMeter was a 1-watt powered meter, as represented by PG&E, or actually two or more watts, as represented by EON. PG&E's response indicates that its electric SmartMeters are rated to transmit at one watt. However, PG&E also states the meter's instantaneous peak level in terms of "effective isotropic radiated power" (EIRP) is 2.5 watts based on the SmartMeters' 4.0 dB $\mu$  antenna gain.<sup>25</sup> This is similar to saying that a flashlight with a 1 watt bulb that focuses the light output in one direction appears as bright as a 2.5 watt bulb *without* the help of the flashlight's focusing capability. Therefore, while it is true that the EIRP from the SmartMeter is 2.5 watts, this level of emissions is below the FCC allowable RF emissions.<sup>26</sup>

The Commission has also received a number of questions regarding whether there is RF emission when the meter is not transmitting. PG&E states that "all digital circuitry - from that contained in clocks, in stereo equipment, or in answering machines - emits de minimus RF that is governed by FCC limits for unintentional RF emissions."<sup>27</sup> PG&E also includes a table in its response comparing the level of RF emissions under the radio-off and a radio out options. PG&E states that

these values were calculated as part of the SmartMeter's certification.<sup>28</sup> This table is reproduced in Table 1 below.

**Table 1**  
**RF Emissions by Meter Type**

| Meter Type    | RF Measured Value With Radio Out | RF Measured Value With Radio Off | FCC Allowable RF Emissions |
|---------------|----------------------------------|----------------------------------|----------------------------|
| Electric: GE  | 38.3 dBµV/m                      | 39.3 dBµV/m                      | 49.0 dBµV/m                |
| Electric: L+G | 31.3 dBµV/m                      | 24.7 dBµV/m                      | 49.0 dBµV/m                |
| Gas: Aclara   | No discernable emissions         | No discernable emissions         | 40.0 - 54.0 dBµV/m         |

PG&E acknowledges that the analog meters emit no RF.<sup>29</sup> However, this fact alone does not lead to the conclusion that the analog meter opt-out option should be selected. As noted in Table 1 above, the RF emissions for SmartMeters with the radio off and a digital meter with no radio installed are below the FCC allowable RF emissions.

In advocating for adoption of an analog meter opt-out option, various parties have asserted that this option is necessary due to the alleged effect of RF emissions on human health. However, the issue of whether RF emissions from SmartMeters have an effect on individuals is outside the scope of this proceeding. Further, we determined in Decision (D.) 10-12-001 that PG&E's SmartMeter technology complies with FCC requirements.

More importantly, the alleged effect of RF emissions on health is not material to the resolution of this application. Eligibility to opt out of receiving a wireless SmartMeter is not predicated on whether the meter has affected the customer's health. Rather, as has been stated by the ALJ, a customer shall be allowed to opt out of a wireless SmartMeter for any reason, or for no reason. Therefore, while some parties may argue that one opt-out option would address certain customer concerns better than another option, such an argument is not determinative of the option to be selected.

In determining the best opt-out option to be adopted, we must balance the concerns expressed by customers against California's overall energy policy. The Commission authorized the state's investor owned utilities to replace analog meters with smart meters in order to give consumers greater control over their energy use. Electric SmartMeters enable a utility to provide customers with detailed information about their electric energy usage at different times of the day, which in turn enables customers to manage their energy use more proactively.<sup>30</sup> In our decision authorizing smart meters for PG&E, we set the following minimum functionalities for these meters in order to proceed with California's goal to give customers information and choice about their energy consumption:<sup>31</sup>

- be capable of supporting a wide range of price responsive tariffs;
- collect data at a detail level that supports customer understanding of hourly usage patterns and their relation to energy costs;

- allow access to personal usage data such that customer access frequency does not result in additional AMI system hardware costs;
- be compatible with customer education, energy management, customized billing, and complaint resolution applications;
- be compatible with utility system applications that promote and enhance system operating efficiency and improve service reliability, such as remote meter reading, outage management, reduction of theft and diversion, improved forecasting, workforce management, etc.; and
- be capable of interfacing with load control communication technology.

Furthermore, in PG&E's most recent rate design decision we stated that "the Commission's dynamic pricing principles seek to increase customer involvement in (a) managing California's energy supply, (b) reducing greenhouse gas emissions, and (c) managing future power plant development costs, by providing real economic incentives to reduce electric demand during peak periods.<sup>32</sup> We remind parties that while we believe that residential customers should be offered an opportunity to opt-out of receiving a wireless SmartMeter, the selected option should not impede state energy objectives. As such, it is important that the selected opt-out option has the capability to allow customers to take advantage of smart grid benefits in the future.

PG&E states that although the SmartMeter with its radio turned off is not currently able to provide interval energy consumption data, there may be future technologies that allow for the manual retrieval of this data.<sup>33</sup> Since the ability to collect interval energy consumption data is a key component to attaining California's overall energy objectives, including matching customer demand with procurement of generation resources, we do not find it reasonable to adopt an electric SmartMeter opt-out option that would not be able to collect that information. As noted above the single most important reason to transition from analog meters has been the capability of supporting a wide range of price responsive tariffs that analog meters cannot do.

Although a wired smart meter would be capable of collecting and transmitting interval energy consumption data, we do not find it to be a reasonable opt-out option at this time. This option would likely require a significant investment in infrastructure and would not be available for use on a large scale within the near future. Additionally, this option is not available for gas SmartMeters.

The proposed decision also did not find the analog meter option reasonable, as this option is unable to track interval energy consumption data. However, TURN notes in its comments that "[a]ny future time variant pricing tariff must offer all residential customers an opportunity to 'opt-out' without penalty."<sup>34</sup> It therefore argues that any customer who opts out of wireless SmartMeter would also opt out of any time variant pricing. Other intervenors argue in their comments to the proposed decision that an analog meter opt-out option also be adopted. Finally, PG&E states in its reply comments that it supports approval of an analog meter opt-out option, in addition to the non-communicating option.<sup>35</sup>

The proposed decision recommended adoption of a non-communicating meter - that is, a SmartMeter with the radio-off or a digital meter with no communications capability. This option

was proposed to enable customers to take advantage of already deployed energy policies, such as net energy metering, demand response and energy efficiency measures. As stated above, California's energy policies encourage customers to become smart energy users by giving customers more information and better information about their usage in order for customers to make smart choices to reduce their consumption or shift their consumption to reduce the need for additional power plants and a better climate. For example, customers who install small solar, wind, biogas, and fuel cell generation facilities (1 MW or less) to serve all or a portion of onsite electricity needs are eligible for the state's net metering program. **Net Energy Metering (NEM) allows** a customer-generator to receive a financial credit for power generated by their onsite system and fed back to the utility. The credit is used to offset the customer's electricity bill. NEM is an important element in managing California's energy supply, reducing greenhouse gas emissions, and reducing the need to build future power plants.

Demand response is another program that requires interval energy consumption data. Demand response is a resource that allows end-use electric customers to reduce their electricity usage in a given time period, or shift that usage to another time period, in response to a price signal, a financial incentive, an environmental condition or a reliability signal. It also allows ratepayers to save money if they lower peak time energy usage, which are high-priced. This lowers the price of wholesale energy, and in turn, retail rates. Demand response may also prevent rolling blackouts by offsetting the need for more electricity generation and can mitigate generator market power. Demand response programs require a meter that is able to collect interval data.

In light of parties' comments on the proposed decision, however, we revise the proposed decision and now adopt an analog meter opt-out option. This determination, however, does not diminish our commitment and support to the development of California's energy policies. As such, further review of the feasibility of continuing to offer an analog meter opt-out option may be warranted in the future to ensure that this opt-out option does not impede the full implementation of net metering, demand response and smart grid. At a minimum, this opt-out option should be re-evaluated once default TOU pricing is employed for all residential customers.

Some parties have recommended in their comments that we adopt more than one opt-out option. However, we decline to do so at this time. From a customer standpoint, it would be less confusing if there is only a single opt-out option. Further, in its October 28, 2011 response to an ALJ Ruling requesting cost information, PG&E stated that it would incur additional costs if multiple opt-out options were offered.<sup>36</sup> As a result, we believe that further examination of the additional costs associated with offering multiple opt-out options is warranted before more than one opt-out option is offered.

Finally, we do not make any determination on whether to allow the opt-out option to be exercised by local entities and communities at this time. Parties advocating for a community opt-out option have not sufficiently addressed issues regarding implementation of such an option, including whether such an option is consistent with existing statutes and rules.<sup>37</sup> Further, as discussed below, we have determined that any residential customer electing the opt-out option will be assessed an initial fee and monthly charges. It is unknown at this time whether customers who are part of a community opt-out option should be assessed the same, or different, opt-out fees and charges. Consequently, we find that further consideration of whether to allow a community

opt-out option should be included in the second phase of this proceeding.

## 5. Cost of Opt-Out Plan

PG&E states that it had considered a radio-off, a wired smart meter and a legacy (analog) meter opt-out options. However, its application provided detailed cost information for only its proposed opt-out option, the radio-off option. PG&E states that its cost estimates represent the incremental costs related to turning off the radio, meter reading while the meters are in radio off mode, an expectation of requiring additional network equipment to compensate for the count of meters in radio off mode and turning the radio back on when the customer moves. This results in an estimated revenue requirement for 2012-2013 of \$113.4 million. This revenue requirement consists of the following:

### Incremental Expense Costs (thousand \$)

Field Deployment \$56,351

Information Technology 406

Customer Communications and

Operations Support 18,379

### **Total Incremental Expense Costs \$75,136**

### Incremental Capital Costs (thousand \$)

Field Deployment \$36,385

Information Technology 1,912

### **Total Incremental Capital Costs 38,297**

### **Total Incremental Costs \$113,433**

## 5.1. Parties' Comments

Various parties oppose PG&E's proposed revenue requirement. Aglet believes the costs are too high and that less expensive alternatives should be considered.<sup>38</sup> TURN echoes Aglet's comments and notes that some of the costs could possibly be reduced if customers were allowed to self-read the meters. It further urges further investigation of whether the radio transmission feature on the wireless SmartMeters could be turned off and on remotely.<sup>39</sup>

Fairfax also argues that PG&E's cost estimates are overstated since the costs are based on turning off already installed and functioning SmartMeters and do not consider those instances where an analog meter is installed, or where there is community wide opt-out. Fairfax further states that costs could be minimized if PG&E were ordered to retain a sufficient inventory of analog meters now. Similar to TURN, Fairfax also argues that costs could be lowered by allowing customers to read the meters and mail in a postcard.<sup>40</sup>

## 5.2. Discussion

Although only costs for the radio off option were provided, the Scoping Memo stated that other parties recommending other reasonable cost opt-out alternatives would provide the estimated costs of the recommended alternative(s).<sup>41</sup> Several parties proposed alternatives, but expressed difficulty in determining the costs for their recommended alternative. This difficulty was also noticed in a motion filed by DRA on July 22, 2011 and voiced at the September 14 workshop. Consequently,

an ALJ Ruling was issued on October 12, 2011 directing PG&E to provide cost information for the following opt-out options:

1. Replacement of wireless SmartMeter with an analog meter;
- 2 Replacement of wireless SmartMeter with a digital meter with no radio installed; and
3. Replacement of wireless SmartMeter with a wired smart meter (telephone or fiber-optic).

PG&E's response to the October 12 ALJ Ruling was filed and served on all parties on October 28, 2011. As presented in Table 1 below, PG&E's estimated costs would be the same for all non-communicating opt-out options, while certain costs for the wired option will be significantly higher.

**TABLE 2**  
**ESTIMATED COSTS FOR OPT-OUT OPTIONS**

|   | Analog Meter | Radio Out    | Wired         | Radio Off    |
|---|--------------|--------------|---------------|--------------|
| <u>Initial Costs</u>                        |              |              |               |              |
| Meter                                       | \$51.24      | \$29.28      | \$355.50      | N/A          |
| Labor (Site visit)                          | \$128.00     | \$128.00     | \$128.00*     | \$128.00     |
| <u>Monthly Charges</u>                      | \$10.69      | \$10.69      | \$10.42       | \$10.69      |
| <u>Other Costs</u>                          |              |              |               |              |
| Network Capital Costs                       | \$36,385,335 | \$36,385,335 | \$36,385,335  | \$36,385,335 |
| Information Technology Costs                | \$2,317,621  | \$2,317,621  | \$25,983,287  | \$2,317,621  |
| Call Center Operations Expenses             | \$3,007,620  | \$3,007,620  | \$3,007,620   | \$3,007,620  |
| Other Costs                                 | \$15,371,390 | \$15,371,390 | \$45,308,990  | \$15,371,390 |
| Revenue Requirement per Opt-Out Customer*** | \$57,081,966 | \$57,081,966 | \$115,766,712 | \$57,081,966 |
|   | \$416        | \$411        | \$613         | \$402        |

**NOTES:**

\* Excludes additional \$150.00 for wiring charge.

\*\* Costs to read gas meter

\*\*\* Assumes 145,800 Opt-Out Customers

As outlined in Table 2 above, PG&E estimates that the majority of the estimated costs for all of the opt-out alternatives are associated with developing and maintaining a separate back office system for the non-communicating meters. PG&E's cost estimates are based on offering a single opt-out option and, it contends that there would be increased costs if multiple opt-out options were offered.<sup>42</sup>



PG&E's application provided testimony to explain the costs associated with providing a radio-off opt-out option. However, since we have now decided that PG&E should provide an analog meter opt-out option, more detailed information concerning the costs associated with this option is needed. As such, a second phase is needed in this proceeding to consider the costs associated with offering an analog opt-out option. As discussed above, this phase may also consider whether opt-out costs will vary if community opt-out is permitted.

#### 6. Cost Recovery for the Opt-Out Plan and Rate Structure

PG&E proposes to recover the incremental costs to the SmartMeter Program to provide the opt-out option from customers exercising the option. Based on its estimated revenue requirement, PG&E proposes two fee schedules for customers electing to not have a wireless SmartMeter.<sup>43</sup> One schedule would have a lower initial opt-out fee, with higher monthly charges, while the other would have a higher initial opt-out fee, with lower monthly charges.<sup>44</sup> Under both schedules, there would be a 20 percent discount for customers enrolled in the California Alternate Rates for Energy (CARE) program. The proposed fees, assuming 148,500 customers decide to opt out, are:

Schedule A (lower initial fee and higher monthly charges)

Non-CARE \$135 upfront \$20 / month

CARE \$105 upfront \$16 / month

Schedule B (higher initial fee and lower monthly charges)

Non-CARE \$270 upfront \$14 / month

CARE \$215 upfront \$11 / month

In addition to the initial fee and monthly charges, customers would be charged a separate "exit" fee of \$135 (or \$105 for CARE customers) if the customer decides to have the radio communications turned on at a later date or terminates service at that location.<sup>45</sup> This fee is to cover costs associated with enabling the SmartMeter's radio communications.

In response to the ALJ's October 12, 2011 Ruling, PG&E also submitted proposed rates for each of the other opt-out options. These rates are as follows:<sup>46</sup>

**TABLE 3**  
**CUSTOMER CHARGES BY OPT-OUT OPTION**

|                | Analog | Radio Out | Wired Meter | Radio Off |
|----------------|--------|-----------|-------------|-----------|
| Initial Fee    | \$270  | \$270     | \$470       | \$270     |
| Monthly Charge | \$16   | \$15      | \$41        | \$14      |
| Exit Fee       | \$130  | \$130     | \$130       | \$130     |

#### 6.1. Parties' Comments

Most intervenors oppose imposing any fee on ratepayers for opting out. Both Lake and Mendocino maintain that PG&E should have already accounted for providing a radio off option, as it had been considered in Application (A.) 07-12-009. As such, they argue that PG&E should not now be imposing costs on customers to provide this option.<sup>47</sup> Network contends that customers have been harmed by the SmartMeters, and, thus, argues that it would be unfair to charge customers to opt-out.<sup>48</sup> EON further argues that ratepayers should not be required to pay for a solution that

does not solve the problems.<sup>49</sup> These parties generally maintain that costs for the opt-out option should be the responsibility of PG&E shareholders.

Aglet states that the majority of incremental costs for the opt-out option should be allocated to all customers. It contends that the need for an opt-out option is driven by the SmartMeter Program as a whole. Therefore, it believes that, just as the SmartMeter Program costs are allocated to all customers, so should the costs associated with the opt-out option.<sup>50</sup> DRA also states that the Commission should consider whether the program costs should be recovered from customers exercising the opt-out option, utility shareholders or all ratepayers.<sup>51</sup>

Alameda, Lake, and Mendocino also maintain that imposing opt-out fees on low-income customers is discriminatory. Lake argues that PG&E arbitrarily applies a 20 percent discount to customers enrolled in the CARE program but provides no discount for families enrolled in the Family Electric Rate Assistance (FERA) program. It further contends that imposing opt-out charges on low-income would be contrary to the objectives of these low income programs, "as these additional charges would place these low-income customers at the same rate as Non-CARE customers who do not opt to have the radios in their Smart Meters turned off."<sup>52</sup>

## 6.2. Discussion

We agree with PG&E that a customer selecting the opt-out option should be assessed an initial charge to install the non-communicating meter and a monthly charge. The Commission authorized the utilities to deploy SmartMeters throughout their territories and complete deployment by December 31, 2012. Consequently, the standard for metering has been transitioned from the older technology, analog meters, to today's technology, SmartMeters. In this decision we are not reversing that transition, however, we do approve an option for specific customers who, for whatever reason, would prefer a non-communicating meter. This option to move away from the standard will require PG&E to incur costs such as purchasing a new meter, going back to the customer location to install and service the meter, monthly cost of reading the meter, and labor involved in rendering the existing SmartMeter non-communicative.<sup>53</sup> These are some of the examples of the additional cost required to opt-out of the standard wireless SmartMeters.

The proposed decision had concluded that the costs for the opt-out option should not be solely the responsibility of those electing to opt-out, since some of the costs were related to the SmartMeter infrastructure as a whole. As a result, the proposed decision recommended that a portion of the opt-out costs be allocated to all residential ratepayers. In comments on the proposed decision, some parties have raised various legal and policy arguments on why some portion, or all, of these costs should be paid by all ratepayers or PG&E shareholders.<sup>54</sup> Based on these comments, we believe it is appropriate to consider allocation of costs as part of the second phase of this proceeding.

We agree with Lake that any discount provided to customers enrolled in the CARE program should also be provided to customers enrolled in the FERA programs. However, we do not agree with Lake's assertion that imposing opt-out charges on low-income would be contrary to the objectives of these low-income programs. Lake incorrectly compares the rates to be paid by CARE customers electing a non-communicating SmartMeter with Non-CARE customers who do not opt

out of wireless SmartMeters. These two groups of customers are not receiving the same type of service, since their meters will have different levels of functionality (wireless communications vs. no communications). Further, the wireless SmartMeter is the standard adopted for PG&E's Advanced Meter Infrastructure program. Therefore, any customer opting to have a non-communicating meter is electing to not have the standard. More importantly, the opt-out option is voluntary, as a customer may participate for any reason, or no reason at all. As such, the fact that a CARE customer's electric bill will increase because the customer has decided to participate in the opt-out option should not be considered "defeating" the purpose of the low-income programs.

The proposed decision had recommended the following fees and charges for customers electing a non-communicating digital meter opt-out option:

For Non-CARE and Non-FERA Customers:

Initial Fee \$90.00

Monthly Charge \$15.00/month

For CARE and FERA Customers:

Initial Fee \$0.

Monthly Charge \$5.00/month

We decline to adopt an exit fee at this time. PG&E's proposed exit fee would be the same regardless of which opt-out option is adopted, and the current record does not contain sufficient evidence to justify why such a fee is necessary. Therefore, we will consider the appropriateness of an exit fee in the second phase of this proceeding.

Parties' comments on this proposal have ranged from no additional fees for opting out<sup>55</sup> to setting a reasonable level of fees.<sup>56</sup> Additionally, DRA has recommended that there should be a different initial fee depending on whether the customer is selecting the opt-out option for one or two meters.<sup>57</sup> Based on these comments, and our determination to adopt an analog meter opt-out option, further consideration of the fees and charges to be assessed on customers electing the opt-out option should be included in the second phase of this proceeding.

We recognize that this second phase of the proceeding will take time to complete based on the number of issues identified in this decision. At the same time, we do not wish to delay the implementation of the opt-out option. Accordingly, we adopt interim fees and charges, subject to adjustment once a decision on costs and cost allocation for the opt-out option is issued, for customers electing the opt-out option. The interim fees and charges are as follows:

For Non-CARE and Non-FERA Customers:

Initial Fee \$75.00

Monthly Charge \$10.00/month

For CARE and FERA Customers:

Initial Fee \$10.00

Monthly Charge \$5.00/month

PG&E is authorized to establish new two-way electric and gas Modified SmartMeter Memorandum Accounts to track revenues and costs associated with providing the opt-out option. We allow PG&E to track these costs and revenues in a two-way memorandum account so that it will preserve the opportunity to seek recovery of these costs and revenues once a final decision on costs and cost allocation is issued.<sup>58</sup>

## 7. Next Steps

As noted above, it is our desire to have the opt-out option implemented without undue delay. Consequently, PG&E is directed to file a Tier 1 Advice Letter to implement the SmartMeter opt-out option and to establish a SmartMeter Opt-Out Tariff (SMOOT) within 15 days of the effective date of this decision. This Advice Letter filing shall:

1. Establish procedures for residential customers to select the opt-out option if they do not wish to have a wireless SmartMeter.
2. Establish procedures to inform customers that a SmartMeter opt-out option is available. A customer currently on the delay list shall be informed that the customer will be scheduled to receive a wireless SmartMeter unless the customer elects to exercise the opt-out option.
3. Adopt the following interim fees and charges for residential customers selecting the opt-out option:

For Non-CARE and Non-FERA Customers:

Initial Fee \$75.00

Monthly Charge \$10.00/month

For CARE and FERA Customers:

Initial Fee \$10.00

Monthly Charge \$5.00/month

4. Establish new two-way electric and gas Modified SmartMeter Memorandum Accounts to track revenues and costs associated with providing the SmartMeter opt-out option until a final decision on costs and cost allocation issues associated with providing an analog meter opt-out proposal is issued.

As part of implementing the opt-out option, PG&E shall comply with the following guidelines:

1. Residential customers may begin signing up to participate in the opt-out option 20 days after the effective date of this decision. PG&E shall have a dedicated phone number for customers to call and sign up for the opt-out option. This number shall be staffed by customer service representatives trained to explain the opt-out option and fees.
2. Since a residential customer may opt-out for any reason, or no reason, PG&E may not require a customer to explain or state why he or she wishes to participate in the opt-out option as a condition for signing up.<sup>59</sup>
3. A customer may only enroll in the opt-out program once per calendar year at the same residence.
4. Customers may pay the initial fee to participate in the opt-out option over a three month period. If the customer does not pay the fee within this period, the customer will be removed from participating in the opt-out option and returned to the wireless SmartMeter.
5. PG&E shall not charge customers the initial fee nor the monthly charges until the analog meter has been installed at the customer's residence.

6. Customers currently on the delay list shall be individually notified of the opt-out option by certified mail and shall have at least 30 days prior notice that their analog meter will be replaced with a wireless SmartMeter unless they contact PG&E to participate in the opt-out option.

The September 21, 2011 Assigned Commissioner's Ruling (ACR) directed the utilities to allow residential customers who had not yet received a wireless SmartMeter to retain their analog meter and be placed on a delay list while the Commission considered PG&E's opt-out proposal. Since we are now modifying the SmartMeter Program to include an opt-out option, the ACR is no longer in effect for PG&E.

This decision determines that a second phase in this proceeding is necessary to consider cost and cost allocation issues associated with providing the analog meter opt-out option, as well as issues associated with offering a community opt-out option. We anticipate that a prehearing conference to discuss the scope and schedule of this second phase will be scheduled within 45 days of the date this decision is issued. The assigned Commissioner will issue an amended scoping memo to reflect the new issues and schedule.

## **8. Comments on Proposed Decision**

The proposed decision of the assigned Commissioner in this matter was mailed to the parties in accordance with Section 311 of the Public Utilities Code and comments were allowed under Rule 14.3 of the Commission's Rules of Practice and Procedure. Comments were filed on December 12, 2011 by Aglet, SCE, Wilner, DRA, PG&E, TURN, Network, Fairfax, Alameda, EON, CCSF, and Lake. Reply comments were filed on December 19, 2011 by Wilner, SCE, Fairfax, Aglet, CARE, DRA, PG&E, and Network. Informal comments were also received from the public.

In response to comments, the proposed decision has been revised to adopt an analog opt-out option. The proposed decision has also been revised to include a second phase in this proceeding to consider costs and cost allocation issues associated with providing the analog meter opt-out option, as well as issues associated with offering a community opt-out option. Other revisions in response to comments have been made as appropriate.

## **Findings of Fact**

1. PG&E was directed by Commissioner Peevey to submit a proposal that would allow some form of opt-out for PG&E customers who did not wish to have a smart meter with RF transmission.
2. PG&E proposes that the SmartMeter Program be modified to provide residential customers the choice to disable (turn off) the radio inside their gas and/or electric meters.
3. The four possible alternatives for an opt-out option are: (1) SmartMeter with the radio transmission turned off; (2) digital meter with no radio installed; (3) analog meter; and (4) wired smart meter with wired transmission capability.
4. A non-communicating opt-out option would disable certain electric SmartMeter functions.
5. A wired smart meter option cannot currently be used on a large scale and are not available for gas smart meters.
6. Analog meters are unable to track interval energy consumption data.
7. Interval energy consumption data is a key component to attaining California's overall energy objectives.
8. Further review of the feasibility of continuing to offer an analog meter opt-out option may be warranted in the future to ensure that this opt-out option does not impede the full implementation of net metering, demand response and smart grid.
9. PG&E's application provided cost estimates for the radio-off option.
10. PG&E provided cost information for the radio out, analog meter and wired smart meter opt-out options in response to an ALJ Ruling.
11. PG&E's cost estimates assumed that a single opt-out option would be offered.
12. There is an insufficient record to determine whether to allow a community opt-out option.

## **Conclusions of Law**

1. A residential customer should be allowed to opt out of a wireless SmartMeter for any reason, or for no reason.
2. D.10-12-001 determined that PG&E's SmartMeter technology complies with FCC requirements.
3. The best opt-out option to be adopted must balance the concerns expressed by customers against California's overall energy policy.
4. Allowing residential customers an opportunity to opt out of receiving a wireless SmartMeter should not impede ongoing state energy objectives.
5. It is important that the selected opt-out option has the capability to allow customers to take advantage of smart grid benefits.
6. The wired smart meter opt-out option is not cost effective nor currently technologically feasible compared to the other options.
7. Although a non-communicating meter is the preferred opt-out option, it is appropriate to adopt an analog meter opt-out option at this time.
8. Until there is additional information on the costs to offer multiple opt-out options, only a single opt-out option should be offered.
9. There is insufficient evidence in the record to determine whether to allow the opt-out option to be exercised by local entities and communities.
10. **Since PG&E's implementation of the SmartMeter Program is consistent with the requirements of D.06-07-027, it should be allowed to recover the costs associated with the opt-out option to the extent those costs are found to be appropriate, reasonable and not already being recovered in rates.**
11. A residential customer selecting the opt-out option should be assessed an initial charge and a monthly charge.
12. A discount should be provided to customers enrolled in the CARE and FERA programs.
13. There should be a second phase in this proceeding to consider cost and cost allocation issues associated with offering the analog opt-out option.
14. The modifications to the SmartMeter Program should be implemented as quickly as possible.
15. An interim initial fee and monthly charge for customers electing the opt-out-option should be assessed until a final decision on cost and allocation issues is issued.
16. PG&E should be authorized to establish two-way electric and gas Modified SmartMeter Memorandum Accounts to track revenues and costs associated with providing the opt-out option until a final decision on cost and allocation issues is issued.
17. The September 21, 2011 Assigned Commissioner's Ruling directing the utilities to allow residential customers to be placed on a delay list should no longer be applicable for PG&E.

#### **ORDER**

##### **IT IS ORDERED that:**

1. Pacific Gas and Electric Company's (PG&E) SmartMeter Program is modified to include an option for residential customers who do not wish to have a wireless SmartMeter installed at their location to have an analog meter.
2. Within 15 days of the effective date of this order, Pacific Gas and Electric Company (PG&E) shall file a Tier 1 advice letter in compliance with General Order 96-B. The advice letter shall be served on the service list in Application 11-03-014.

The advice letter shall include tariff sheets to modify PG&E's SmartMeter Program to include an opt-out option for customers who do not wish to have a wireless SmartMeter installed at their location and to implement a SmartMeter Opt-Out Tariff (SMOOT). The Advice Letter filing shall:

- a. Establish procedures for residential customers to select the option to have an analog meter if they do not wish to have a wireless SmartMeter.
- b. Establish procedures to inform customers that a SmartMeter opt-out option is available. A customer currently on the delay list shall be informed that the customer will be scheduled to receive a wireless SmartMeter unless the customer elects to exercise the opt-out option.
- c. Adopt the following interim fees for residential customers selecting the opt-out option:

For Non-CARE and Non-FERA Customers:

Initial Fee \$75.00

Monthly Charge \$10.00/month

For CARE and FERA Customers:

Initial Fee \$10.00

Monthly Charge \$5.00/month

- d. Establish new two-way electric and gas Modified SmartMeter Memorandum Accounts to track revenues and costs associated with providing the SmartMeter opt-out option.

3. The September 21, 2011 Assigned Commissioner's Ruling directing the utilities to allow residential customers who had not yet received a wireless SmartMeter to retain their analog meter and to be placed on a delay list shall no longer be in effect for Pacific Gas and Electric Company.

4. Pacific Gas and Electric Company shall comply with the guidelines stated in Section 7 of this decision.

5. Application 11-03-014 remains open.

This order is effective today.

Dated , at San Francisco, California.

<sup>1</sup> *Assigned Commissioner Ruling and Scoping Memo*, issued May 25, 2011, at 3-4.

<sup>2</sup> See *Administrative Law Judge's Ruling Directing Pacific Gas and Electric Company to File Additional Cost Information*, issued October 12, 2011; *Administrative Law Judge's Ruling Seeking Clarification*, issued October 18, 2011. This second ruling also applied to SCE, SDG&E and SoCalGas.

<sup>3</sup> See *Assigned Commissioner's Ruling Concerning Customer Requests to Delay Installation of a Smart Meter*, issued September 21, 2011.

<sup>4</sup> PG&E Testimony at 1-5 - 1-6.

<sup>5</sup> The relocation option is an existing option and shall continue to be offered pursuant to Electric Rule 16. Under Rule 16, relocation costs could be between \$2,500 and \$11,000 depending on the specific characteristics of the relocation. Relocation costs would be paid by the customer requesting this option.

<sup>6</sup> PG&E Testimony at 3-2.

<sup>7</sup> Application at 5.

<sup>8</sup> In addition to A.11-03-014, the Commission is considering whether SDG&E and SCE should also be required to offer opt-out alternatives in A.11-03-015 and A.11-07-020, respectively.

<sup>9</sup> PG&E Testimony at 2A-4.

<sup>10</sup> The two wired communications possibilities it considered were power line carrier and traditional telephone line.

<sup>11</sup> PG&E Testimony at 1-6 - 1-8.

<sup>12</sup> See, Alameda Protest at 2; Lake Protest at 5-8; Mendocino Protest at 5-8; Network Protest at 4; EON Protest at 13-14; Wilner at 2.

<sup>13</sup> Network Protest at 4 & 6; EON Protest at 13-14; Fairfax Protest at 15.

<sup>14</sup> DRA Response at 7-8.

<sup>15</sup> DRA Response at 5.

<sup>16</sup> Lake Protest at 5.

<sup>17</sup> Lake Protest at 6 - 7.

<sup>18</sup> TURN Protest at 2.

<sup>19</sup> Network Protest at 5; EON Protest at 15; Fairfax Protest at 8-13.

<sup>20</sup> Network Protest at 6.

<sup>21</sup> See *Administrative Law Judge's Ruling Seeking Clarification*, issued October 18, 2011.

<sup>22</sup> PG&E's Response to ALJ's October 18 Ruling, filed November 1, 2011 at 5.

<sup>23</sup> PG&E's Response to ALJ's October 18 Ruling, filed November 1, 2011 at 5.

<sup>24</sup> PG&E's Response to ALJ's October 18 Ruling, filed November 1, 2011 (Attachment B).

<sup>25</sup> PG&E's Response to ALJ's October 18 Ruling, filed November 1, 2011 at 10 (Table 6-1).

<sup>26</sup> 47 C.F.R. § 15.247(c)(3) & (4).

<sup>27</sup> PG&E's Response to ALJ's October 18 Ruling, filed November 1, 2011 at 13 (citing to 47 C.F.R., Part 15, for a Class B digital device).

<sup>28</sup> PG&E's Response to ALJ's October 18 Ruling, filed November 1, 2011 at 14 (Table 10-1).

<sup>29</sup> PG&E's Response to ALJ's October 18 Ruling, filed November 1, 2011 at 15.

<sup>30</sup> D.08-09-039, at 2.

<sup>31</sup> D.05-09-044, at 3 and 4.

<sup>32</sup> D.10-02-032, at 4.

<sup>33</sup> PG&E Testimony at 1-6.

<sup>34</sup> TURN Comments, filed December 12, 2011, at 4. See also, Aglet Comments, filed December 12, 2011, at 4.

<sup>35</sup> PG&E Reply Comments, filed December 19, 2011, at 1-2.

<sup>36</sup> PG&E's Response to Administrative Law Judge's October 12, 2011 Ruling, filed October 28, 2011, at 2.

<sup>37</sup> For example, both PG&E's gas and electric rules define a "customer" as the person "in whose name service is rendered" and whose signature is on the application, contract or agreement for service. (See PG&E Electric Rule 1; PG&E Gas Rule



1.) The rules further state that a customer may seek relief from the Commission if it is "dissatisfied with [PG&E's] determination regarding level, charge or type of service, or refusal to provide service as requested." (See PG&E Electric Rule 4; PG&E Gas Rule 4.) Further development of the record is needed so that we may address whether and how a local entity or community can lawfully impact a customer's utility bill.

<sup>38</sup> Aglet Protest at 3.

<sup>39</sup> TURN Protest at 3-4.

<sup>40</sup> Fairfax Protest at 15-17.

<sup>41</sup> *Assigned Commissioner Ruling and Scoping Ruling, May 25, 2011*, at 3.

<sup>42</sup> PG&E Response of ALJ October 12, 2011 Ruling, filed October 28, 2011 at 2.

<sup>43</sup> PG&E Testimony at 1-2 - 1-3.

<sup>44</sup> Customer could pay for monthly charges on either a flat-fee basis or based on their energy consumption.

<sup>45</sup> PG&E Testimony at 2A-5.

<sup>46</sup> PG&E Response to ALJ October 12, 2011 Ruling, filed October 28, 2011, Attachment A, Summary. On November 9, 2011, PG&E filed a revised version of Attachment A to correct some calculation errors. The charges in Table 3 include the corrections contained in the November 9 filing.

<sup>47</sup> Lake Protest at 4; Mendocino Protest at 3-4.

<sup>48</sup> Network Protest at 5.

<sup>49</sup> EON Protest at 14.

<sup>50</sup> Aglet Protest at 3.

<sup>51</sup> DRA Response at 6.

<sup>52</sup> Lake Protest at 4.

<sup>53</sup> PG&E's Response to the October 12, 2011 ALJ Ruling.

<sup>54</sup> See, e.g., Lake Comments, filed December 12, 2011, at 8 (allocation of costs to all ratepayers is inconsistent with § 728, as non opt-out customers would pay for a benefit received only by opt-out customers); TURN Comments, filed December 12, 2011, at 14-15 (costs associated with offering an opt-out option are a reasonable risk of the AMI program and should be borne by PG&E shareholders).

<sup>55</sup> See, e.g., CCSF Comments, filed December 12, 2011, at 4-5; Network Comments, filed December 12, 2011, at 4.

<sup>56</sup> See, e.g., Aglet Comments, filed December 12, 2011, at 4 (opt-out charges be set at a level that would discourage "frivolous opting out."); TURN Comments, filed December 12, 2011, at 8-10 (need to consider affordability and equity when setting fees).

<sup>57</sup> DRA Comments, filed December 12, 2011, at 6-9.

<sup>58</sup> Authorization of a memorandum account does not necessarily mean that the Commission has decided that the types of costs to be recorded in the account should be recoverable in addition to rates that have been otherwise authorized, e.g., in a general rate case. Instead, the utility shall bear the burden when it requests recovery of the recorded costs, to show that separate recovery of the types of costs recorded in the account is appropriate, that the utility acted prudently when it incurred these costs and that the level of costs is reasonable. Thus, PG&E is reminded that just because the Commission has authorized these memorandum accounts does not mean that recovery of costs in the memorandum accounts from ratepayers is appropriate.

<sup>59</sup> However, PG&E may ask this question if a response is optional.

Top of Page

# EXHIBIT 4



# 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](http://www.crs.gov)

R42338

---

**CRS Report for Congress**  
*Prepared for Members and Committees of Congress*

## Summary

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

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

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

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

## Contents

|  |    |
|--|----|
| Overview.....  | 1  |
| Smart Meter Data: Privacy and Security Concerns .....        | 3  |
| Detailed Information on Household Activities .....           | 3  |
| Increased Potential for Theft or Breach of Data.....         | 6  |
| Smart Meters and the Fourth Amendment .....                  | 7  |
| State Action: Privately Versus Publicly Owned Utilities..... | 8  |
| Privately Owned and Operated Utilities.....                  | 8  |
| Publicly Owned and Operated Utilities.....                   | 10 |
| Reasonable Expectation of Privacy in Smart Meter Data .....  | 13 |
| Third-Party Doctrine .....                                   | 14 |
| Privacy in the Home.....                                     | 16 |
| Mosaic and Dragnet Theories.....                             | 19 |
| Assumption of the Risk—Consent.....                          | 21 |
| Statutory Protection of Smart Meter Data .....               | 22 |
| The Electronic Communications Privacy Act (ECPA).....        | 23 |
| The Stored Communications Act (SCA) .....                    | 24 |
| Electronic Communication Services .....                      | 25 |
| Remote Computing Services.....                               | 27 |
| The Computer Fraud and Abuse Act (CFAA) .....                | 28 |
| The Federal Trade Commission Act (FTC Act).....              | 29 |
| Covered Electric Utilities .....                             | 29 |
| Investor-Owned Utilities .....                               | 30 |
| Publicly Owned Utilities .....                               | 30 |
| Federally Owned Utilities .....                              | 34 |
| Cooperatively Owned Utilities.....                           | 35 |
| Enforcement of Data Privacy and Security .....               | 40 |
| “Deceptive” Privacy Statements .....                         | 40 |
| “Unfair” Failure to Secure Consumer Data.....                | 41 |
| Penalties .....  | 42 |
| The Federal Privacy Act of 1974 (FPA).....                   | 43 |
| Federally Owned Utilities as “Agencies” .....                | 43 |
| Smart Meter Data as a Protected “Record” .....               | 44 |
| Requirements.....  | 44 |

## Figures

|   |   |
|---|---|
| Figure 1. Identification of Household Activities from Electricity Usage Data..... | 5 |
|---|---|

## Contacts

|                                 |    |
|---------------------------------|----|
| Author Contact Information..... | 45 |
|---------------------------------|----|

## Overview

Smart meter technology is a key component of the Advanced Metering Infrastructure (AMI)<sup>1</sup> that will help the smart grid<sup>2</sup> link the “two-way flow of electricity with the two-way flow of information.”<sup>3</sup> Privacy and security concerns surrounding smart meter technology arise from the meters’ essential functions, which include (1) recording near-real time data on consumer electricity usage; (2) transmitting this data to the smart grid using a variety of communications technologies;<sup>4</sup> and (3) receiving communications from the smart grid, such as real-time energy prices or remote commands that can alter a consumer’s electricity usage to facilitate demand response.<sup>5</sup>

Beneficial uses of AMI are developing rapidly, and like the early Internet, many applications remain unforeseen.<sup>6</sup> At a basic level, smart meters will permit utilities to “collect, measure, and analyze energy consumption data for grid management, outage notification, and billing purposes.”<sup>7</sup> The meters may increase energy efficiency by giving consumers greater control over their use of electricity,<sup>8</sup> as well as permitting better integration of plug-in electric vehicles and renewable energy sources.<sup>9</sup> They may also aid in the development of a more reliable electricity grid that is better equipped to withstand cyber attacks and natural disasters, and help to decrease peak demand for electricity.<sup>10</sup> To be useful for these purposes, and many others, data recorded by

---

<sup>1</sup> AMI includes the meters at the consumer’s residence or business, the communications networks that send data between the consumer and utility, and the data management systems that store and process data for the utility. ELECTRIC POWER RESEARCH INST., ADVANCED METERING INFRASTRUCTURE (AMI) (2007), *available at* <http://www.ferc.gov/eventcalendar/Files/20070423091846-EPR1%20-%20Advanced%20Metering.pdf>. The primary function of AMI is to “combine interval data measurement with continuously available remote communications” to increase energy efficiency and grid reliability, and decrease expenses borne by the utility and consumer. *Id.*

<sup>2</sup> The Energy Independence and Security Act of 2007 (EISA) lists ten characteristics of a smart grid. These include “[i]ncreased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid”; “[d]evelopment and incorporation of demand response, demand-side resources, and energy-efficiency resources”; and “[d]eployment 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.” EISA, P.L. 110-140, §1301, 121 Stat. 1492, 1783-84 (2007) (to be codified at 42 U.S.C. §17381).

<sup>3</sup> DEP’T OF ENERGY, COMMUNICATIONS REQUIREMENTS OF SMART GRID TECHNOLOGIES 1 (2010) [hereinafter DEP’T OF ENERGY COMMUNICATIONS REPORT], *available at* [http://energy.gov/sites/prod/files/gcprod/documents/Smart\\_Grid\\_Communications\\_Requirements\\_Report\\_10-05-2010.pdf](http://energy.gov/sites/prod/files/gcprod/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf).

<sup>4</sup> *Id.* at 3, 5. These technologies include fiber optics, wireless networks, satellite, and broadband over power line. *Id.*

<sup>5</sup> *Id.* at 20. “Demand response is the reduction of the consumption of electric energy by customers in response to an increase in the price of electricity or heavy burdens on the system.” *Id.*

<sup>6</sup> DEP’T OF ENERGY, DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES 5, 9 (2010) [hereinafter DEP’T OF ENERGY PRIVACY REPORT], *available at* [http://energy.gov/sites/prod/files/gcprod/documents/Broadband\\_Report\\_Data\\_Privacy\\_10\\_5.pdf](http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf); *see also* ELIAS LEAKE QUINN, SMART METERING & PRIVACY: EXISTING LAW AND COMPETING POLICIES: A REPORT FOR THE COLORADO PUBLIC UTILITIES COMMISSION 1, 12 (2009) [hereinafter COLORADO PRIVACY REPORT], *available at* [http://www.dora.state.co.us/puc/docketsdecisions/DocketFilings/09I-593EG/09I-593EG\\_Spring2009Report-SmartGridPrivacy.pdf](http://www.dora.state.co.us/puc/docketsdecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-SmartGridPrivacy.pdf).

<sup>7</sup> DEP’T OF ENERGY COMMUNICATIONS REPORT, *supra* note 3, at 12.

<sup>8</sup> Companies are developing several new applications that use smart meter data to offer consumers and utilities better control over energy usage, for example by determining the energy efficiency of specific appliances within the household. DEP’T OF ENERGY PRIVACY REPORT, *supra* note 6, at 5, 9; *see also* COLORADO PRIVACY REPORT, *supra* note 6, at 1, 12.

<sup>9</sup> DEP’T OF ENERGY COMMUNICATIONS REPORT, *supra* note 3, at 1.

<sup>10</sup> *Id.* at 3.

smart meters must be highly detailed, and, consequently, it may show what individual appliances a consumer is using.<sup>11</sup> The data must also be transmitted to electric utilities—and possibly to third parties outside of the smart grid—subjecting it to potential interception or theft as it travels over communications networks and is stored in a variety of physical locations.<sup>12</sup>

These characteristics of smart meter data present privacy and security concerns that are likely to become more prevalent as government-backed initiatives expand deployment of the meters to millions of homes across the country. In the American Recovery and Reinvestment Act of 2009 (ARRA), Congress appropriated funds for the implementation of the Smart Grid Investment Grant (SGIG) program administered by the Department of Energy.<sup>13</sup> This program now permits the federal government to reimburse up to 50% of eligible smart grid investments, which include the cost to electric utilities of buying and installing smart meters.<sup>14</sup> In its annual report on smart meter deployment, the Federal Energy Regulatory Commission cited statistics showing that the SGIG program has helped fund the deployment of about 7.2 million meters as of September 2011.<sup>15</sup> At completion, the program will have partially funded the installation of 15.5 million meters.<sup>16</sup> By 2015, the Institute for Electric Efficiency expects that a total of 65 million smart meters will be in operation throughout the United States.<sup>17</sup>

Installation of smart meters and the communications technologies that accompany them may have unforeseen legal consequences for those who generate, seek, or use the data recorded by the meters. These consequences may arise under existing federal laws or constitutional provisions governing the privacy of electronic communications, data retention, computer misuse, foreign surveillance, and consumer protection. This report examines federal privacy and cybersecurity laws that may apply to consumer data collected by residential smart meters. It examines the legal implications of smart meter technology for consumers who generate the data, law enforcement officers who seek smart meter data from utilities, utilities that store the data, and hackers who access smart grid technology to steal consumer data or interfere with it. This report looks at federal laws that may pertain to the data when it is (1) stored in a utility-owned smart meter at a consumer's residence; (2) in transit between the meter and the smart grid by way of various communications technologies; and (3) stored on computers in the grid. This report does not address state or local laws, such as regulations by state Public Utilities Commissions, that may establish additional responsibilities for some electric utilities with regard to smart meter data. It also does not discuss the mandatory cybersecurity and reliability standards enforced by the North

---

<sup>11</sup> See NAT'L INST. OF STANDARDS AND TECH., GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 14 (2010) [hereinafter NIST PRIVACY REPORT], available at [http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628\\_vol2.pdf](http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf).

<sup>12</sup> *Id.* at 3-4, 23-24, 29.

<sup>13</sup> The act provides \$4.5 billion for “electricity delivery and energy reliability,” which includes “activities to modernize the electric grid, to include demand responsive equipment,” as well as “programs authorized under title XIII of the Energy Independence and Security Act of 2007.” ARRA, P.L. 111-5, 123 Stat. 115, 138-39.

<sup>14</sup> ARRA §405(5), (8), 123 Stat. 115, 143-44 (amendment to be codified at 42 U.S.C. §17386) (amending the Energy Independence and Security Act of 2007 (EISA) to allow for the reimbursement of up to 50% of qualifying smart grid investments instead of only 20%); see also EISA, P.L. 110-140, §1306, 121 Stat. 1492, 1789-91 (to be codified as amended at 42 U.S.C. §17386) (initially establishing the SGIG program).

<sup>15</sup> FED. ENERGY REGULATORY COMM'N, ASSESSMENT OF DEMAND RESPONSE & ADVANCED METERING 3 (2011), available at <http://www.ferc.gov/legal/staff-reports/11-07-11-demand-response.pdf>.

<sup>16</sup> *Id.*

<sup>17</sup> INST. FOR ELECTRIC EFFICIENCY, UTILITY-SCALE SMART METER DEPLOYMENTS, PLANS & PROPOSALS 1 (2011), available at [http://www.edisonfoundation.net/iee/issuebriefs/SmartMeter\\_Rollouts\\_0911.pdf](http://www.edisonfoundation.net/iee/issuebriefs/SmartMeter_Rollouts_0911.pdf).



American Electric Reliability Corporation, which impose obligations on utilities that participate in the generation or transmission of electricity.<sup>18</sup>

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<sup>19</sup> that are likely to evolve with the technology.<sup>20</sup> 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;<sup>21</sup> 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.<sup>22</sup>

### 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.<sup>23</sup> 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

---

<sup>18</sup> 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.

<sup>19</sup> 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.

<sup>20</sup> See NIST PRIVACY REPORT, *supra* note 11, at 1.

<sup>21</sup> *Id.* at 4, 11. Data that offers a high degree of detail is said to be “granular.” *Id.*

<sup>22</sup> See *id.* at 4, 23-24, 29.

<sup>23</sup> *Id.* at 2, 9.

minutes.<sup>24</sup> Current smart meter technology allows utilities to measure usage as frequently as once every minute.<sup>25</sup> 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.”<sup>26</sup> 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.”<sup>27</sup> 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.<sup>28</sup> 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.<sup>29</sup>

By combining appliance usage patterns, an observer could discern the behavior of occupants in a home over a period of time.<sup>30</sup> 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.”<sup>31</sup> 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.”<sup>32</sup> **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.

---

<sup>24</sup> *Id.* at 13.

<sup>25</sup> 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.

<sup>26</sup> NIST PRIVACY REPORT, *supra* note 11, at 2, 14.

<sup>27</sup> *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”).

<sup>28</sup> COLORADO PRIVACY REPORT, *supra* note 6, at 3 n.7, A-8.

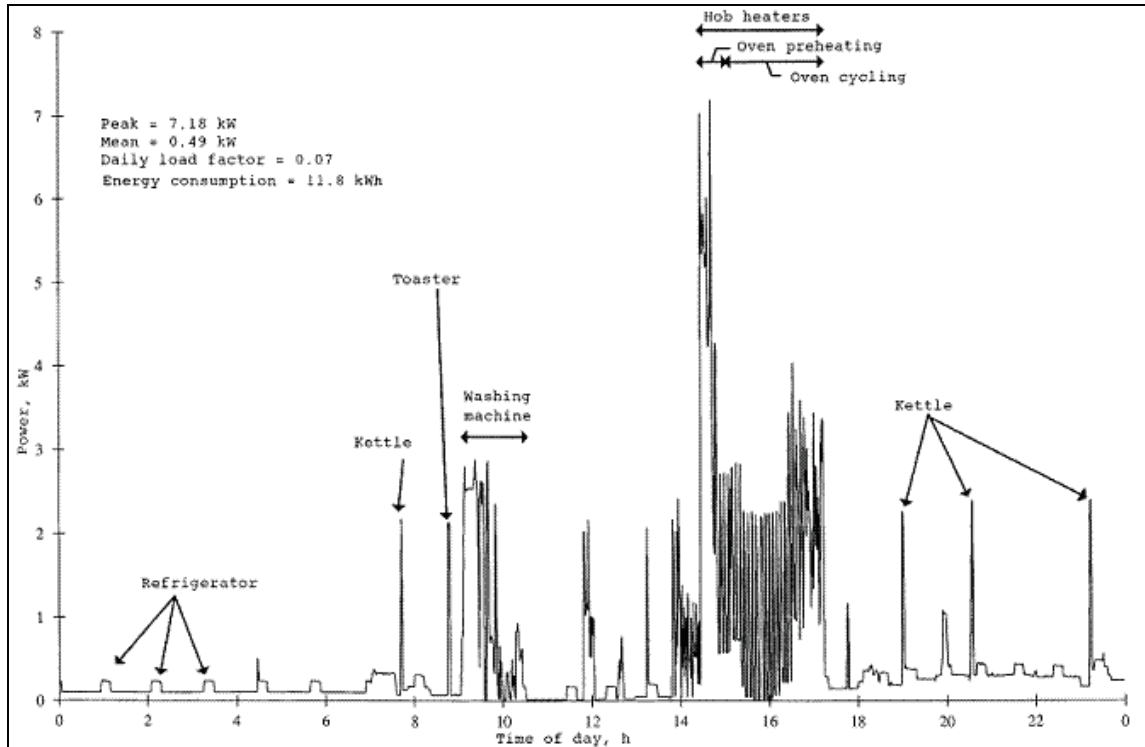
<sup>29</sup> *Id.* at A-9.

<sup>30</sup> NIST PRIVACY REPORT, *supra* note 11, at 6 & n.9.

<sup>31</sup> *Id.* at 11.

<sup>32</sup> 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](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.<sup>33</sup> 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."<sup>34</sup> 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.<sup>35</sup> For example, by observing when occupants use the most electricity, it may be possible to discern their daily schedules.<sup>36</sup>

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

<sup>34</sup> *Kyllo*, 190 F.3d at 1043.

<sup>35</sup> See *supra* notes 26-32 and accompanying text.

<sup>36</sup> See *supra* note 32 and accompanying text.

As smart meter technology develops and usage data grows more detailed, it could also become more valuable to private third parties outside of the grid.<sup>37</sup> Data that reveals which appliances a person is using could permit health insurance companies to determine whether a household uses certain medical devices, and appliance manufacturers to establish whether a warranty has been violated.<sup>38</sup> Marketers could use it to make targeted advertisements.<sup>39</sup> Criminals could use it to time a burglary and figure out which appliances they would like to steal.<sup>40</sup> If a consumer owned a plug-in electric vehicle, data about where the vehicle has been charged could permit someone to identify a person's location and travel history.<sup>41</sup>

Even privacy safeguards, such as “anonymizing” data so that it does not reflect identity, are not foolproof.<sup>42</sup> By comparing anonymous data with information available in the public domain, it is sometimes possible to identify an individual—or, in the context of smart meter data, a particular household.<sup>43</sup> Moreover, a smart grid will collect more than just electricity usage data. It will also store data on the account holder's name, service address, billing information, networked appliances in the home, and meter IP address, among other information.<sup>44</sup> Many smart meters will also provide transactional records as they send data to the grid, which would show the time that the meter transmitted the data and the location or identity of the transmitter.<sup>45</sup>

## Increased Potential for Theft or Breach of Data

Smart grid technology relies heavily on two-way communication to increase energy efficiency and reliability, including communication between smart meters and the utility (or other entity) that stores data for the grid.<sup>46</sup> Many different technologies will transmit data to the grid, including “traditional twisted-copper phone lines, cable lines, fiber optic cable, cellular, satellite, microwave, WiMAX, power line carrier, and broadband over power line.”<sup>47</sup> Of these communications platforms, wireless technologies are likely to play a “prominent role” because they present fewer safety concerns and cost less to implement than wireline technologies.<sup>48</sup> According to the Department of Energy, a typical utility network has four “tiers” that collect and transmit data from the consumer to the utility.<sup>49</sup> These include “(1) the core backbone—the primary path to the utility data center; (2) backhaul distribution—the aggregation point for

---

<sup>37</sup> NIST PRIVACY REPORT, *supra* note 11, at 14, 35-36.

<sup>38</sup> *Id.* at 27-28.

<sup>39</sup> *Id.* at 28.

<sup>40</sup> *Id.* at 31.

<sup>41</sup> *Id.*

<sup>42</sup> *Id.* at 13.

<sup>43</sup> *See id.* at 13, 25.

<sup>44</sup> *Id.* at 26-27.

<sup>45</sup> *Id.* at 12 (drawing a comparison to telecommunications providers' “call detail records”).

<sup>46</sup> *Id.* at 3; DEP'T OF ENERGY COMMUNICATIONS REPORT, *supra* note 3, at 3 (stating that “integrated two-way communications ... allows for dynamic monitoring of electricity use as well as the potential for automated electricity use scheduling.”). As more consumers become generators of electricity through the use of “fuel cells, wind turbines, solar roofs, and the like,” the importance of two-way communication will increase. MIT GRID STUDY, *supra* note 18, at 201.

<sup>47</sup> DEP'T OF ENERGY COMMUNICATIONS REPORT, *supra* note 3, at 3.

<sup>48</sup> *Id.* at 5, 51 n.215.

<sup>49</sup> *Id.* at 16.

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

As NIST explains, consumer data moving through a smart grid becomes stored in many locations both within the grid and within the physical world.<sup>55</sup> Thus, because it is widely dispersed, it becomes more vulnerable to interception by unauthorized parties<sup>56</sup> and to accidental breach.<sup>57</sup> The movement of data also increases the potential for it to be stolen by unauthorized third parties while it is in transit, particularly when it travels over a wireless network<sup>58</sup>—or through communications components that may be incompatible with one another or possess outdated security protections.<sup>59</sup>

## Smart Meters and the Fourth Amendment

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

---

<sup>50</sup> *Id.*

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

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

<sup>53</sup> *Id.* at 16, 19.

<sup>54</sup> *Id.* at 4, 19, 44.

<sup>55</sup> NIST PRIVACY REPORT, *supra* note 11, at 23.

<sup>56</sup> *Id.* at 23-24.

<sup>57</sup> *Id.* at 29.

<sup>58</sup> *See id.* at 9, 12, 33, and 36.

<sup>59</sup> MIT GRID STUDY, *supra* note 18, at 209, 213-16.

<sup>60</sup> Jack I. Lerner & Deirdre K. Mulligan, *Taking the “Long View” on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, ¶ 3 (2008).

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

<sup>62</sup> U.S. CONST. amend IV.

contravene this protection. Although there is no Fourth Amendment case on point, analogous cases may provide guidance.<sup>63</sup>

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.<sup>64</sup> 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.<sup>65</sup> 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.<sup>66</sup> 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.<sup>67</sup> 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.<sup>68</sup> 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.<sup>69</sup>

---

<sup>63</sup> For additional analyses of smart meters under the Fourth Amendment, see Cheryl Dancy 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.”).

<sup>64</sup> *California v. Ciraolo*, 476 U.S. 207, 211 (1986) (citing *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

<sup>65</sup> *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) (8<sup>th</sup> ed. 2010).

<sup>66</sup> NOWAK & ROTUNDA, *supra* note 65.

<sup>67</sup> 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).

<sup>68</sup> *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921).

<sup>69</sup> 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.<sup>70</sup> Determining when this exception applies has not proved easy,<sup>71</sup> 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.<sup>72</sup> 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.<sup>73</sup> Although the utility was heavily regulated by the state, it was held not to be a state actor.<sup>74</sup> The Court reasoned that the provision of utility service is not generally an “exclusive prerogative of the State.”<sup>75</sup> Also absent was the symbiotic relationship between the utility and the state found in previous cases.<sup>76</sup> 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.<sup>77</sup> 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.<sup>78</sup> 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.<sup>79</sup> 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.<sup>80</sup> For example, the Fourth Amendment does not apply when a telephone company installs a pen register on its own initiative.<sup>81</sup> The same action constitutes a search, however, if requested by the government.<sup>82</sup>

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.<sup>83</sup> In *United States v. Davis*, the airline

---

<sup>70</sup> *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).

<sup>71</sup> See NOWAK & ROTUNDA, *supra* note 65, §12.2.

<sup>72</sup> *Jackson*, 419 U.S. at 347; see also *Mays v. Buckeye Rural Elec. Coop., Inc.*, 277 F.3d 873, 880-81 (6<sup>th</sup> 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 (1<sup>st</sup> Cir. March 31, 2003) (holding that private electric utility company was not a state actor).

<sup>73</sup> *Jackson*, 419 U.S. at 351.

<sup>74</sup> *Id.* at 358-59.

<sup>75</sup> *Id.* at 353.

<sup>76</sup> *Id.* at 357.

<sup>77</sup> *Id.* at 351.

<sup>78</sup> 1 WAYNE R. LAFAYE, SEARCH AND SEIZURE §1.8, at 255 (4<sup>th</sup> ed. 2004).

<sup>79</sup> *United States v. Howard*, 752 F.2d 220, 227-28 (6<sup>th</sup> Cir. 1985).

<sup>80</sup> *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971) (internal quotation marks omitted); see LAFAYE, *supra* note 78, §1.8(b).

<sup>81</sup> *United States v. Manning*, 542 F.2d 685, 686 (6<sup>th</sup> Cir. 1976).

<sup>82</sup> *People of Dearborn Heights v. Hayes*, 82 Mich. App. 253, 258 (1978).

<sup>83</sup> *United States v. Davis*, 482 F.2d 893, 897-903 (9<sup>th</sup> Cir. 1973).

searched a passenger based on these requirements and found a loaded gun.<sup>84</sup> 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.”<sup>85</sup> 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,”<sup>86</sup> 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,”<sup>87</sup> and even less frequently as to “noncriminal *noninvestigatory* governmental conduct.”<sup>88</sup> 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.<sup>89</sup> It is premised on the notion that “‘special needs,’ beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.”<sup>90</sup> If, on the one hand, the objective of the search is not for law

---

<sup>84</sup> *Id.* at 895.

<sup>85</sup> *Id.* at 904.

<sup>86</sup> *United States v. Howard*, 752 F.2d 220, 228 (6<sup>th</sup> Cir. 1985).

<sup>87</sup> *The Supreme Court, 1986-Term—Leading Cases*, 101 HARV. L. REV. 119, 230 (1987).

<sup>88</sup> *United States v. Attson*, 900 F.2d 1427, 1430 (9<sup>th</sup> Cir. 1990) (emphasis in original).

<sup>89</sup> *Ferguson v. City of Charleston*, 532 U.S. 67, 77-78 (2001).

<sup>90</sup> *Skinner v. Ry. Labor Executives’ Ass’n*, 489 U.S. 602, 620 (1989) (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987)).



enforcement purposes but for other reasons such as public safety<sup>91</sup> or ensuring the integrity of sensitive government positions,<sup>92</sup> then the doctrine will apply. If, however, the “primary purpose” or “immediate objective” was “to generate evidence for law enforcement purposes,” then application of the special needs doctrine is not appropriate, and the government must adhere to general Fourth Amendment principles.<sup>93</sup> Again, the primary inquiry is the purpose of the search.

Some circuit courts of appeal have extended the special needs theory, holding that the Fourth Amendment does not apply (in contrast to a reduced standard of suspicion as with the special needs cases) unless the “conduct has as its purpose the intention to elicit a benefit for the government in either its investigative or administrative capacities.”<sup>94</sup> In *United States v. Attson*, the Ninth Circuit held that the collection of blood by a government-employed physician, which was subsequently used by the police in a drunk driving prosecution, was not within the scope of Fourth Amendment protection.<sup>95</sup> The panel reasoned that the doctor drew the blood for medical purposes, not to further a governmental purpose in obtaining evidence against the defendant in its criminal investigation, so the Fourth Amendment did not apply.<sup>96</sup>

Applying these two theories to smart meters, a court would focus on the publicly owned utility’s purpose in collecting the data. If it were for ordinary business purposes such as billing, informing the customer of its usage patterns, or aiding the utility in making the grid more energy-efficient, then it would not violate the Fourth Amendment. If, however, the public utility began aggregating data at the request of a law enforcement agency, with the purpose of aiding a criminal investigation or other administrative purpose, the Fourth Amendment would seemingly apply. As with private utilities, if the government requested that the public utility report any suspicious electricity usage, or created a program where certain data was regularly transmitted to the police, this might become investigatory and warrant Fourth Amendment protections. It appears law enforcement cannot evade Fourth Amendment restrictions by requesting a publicly owned utility to collect data for it.

Law enforcement might also request smart meter data under a public records theory. It is generally accepted that public records are not accorded Fourth Amendment protection.<sup>97</sup> Unless there is a state or federal statute prohibiting disclosure, “law enforcement access to state public records is unrestricted.”<sup>98</sup> Thus the inquiry hinges on whether a document is a public record.

---

<sup>91</sup> *Id.*

<sup>92</sup> *Nat’l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 670 (1989).

<sup>93</sup> *Ferguson*, 532 U.S. at 83 (emphasis in original).

<sup>94</sup> *See United States v. Attson*, 900 F.2d 1427, 1431 (9<sup>th</sup> Cir. 1990); *Poe v. Leonard*, 282 F.3d 123, 137 (2d Cir. 2002); *United States v. Elliot*, 676 F. Supp. 2d 431, 435-36 (D. Md. 2009).

<sup>95</sup> *Attson*, 900 F.2d at 1433.

<sup>96</sup> *Id.*

<sup>97</sup> *See Nilson v. Layton City*, 45 F.3d 369, 372 (10<sup>th</sup> Cir. 1995) (“Information readily available to the public is not protected by the constitutional right to privacy.”); *Doe v. City of New York*, 15 F.3d 264, 268 (2d Cir. 1994) (“Certainly, there is no question that an individual cannot expect to have a constitutionally protected privacy interest in matters of public record.”); *United States v. Ellison*, 462 F.3d 557, 562 (6<sup>th</sup> Cir. 2006) (accessing license plate number from computer database held not an intrusion of a constitutionally protected area, thus not a Fourth Amendment “search”); *United States v. Baxter*, 492 F.2d 150, 167 (9<sup>th</sup> Cir. 1973) (holding that Fourth Amendment protections do not extend to telephone company toll and billing records); *see also* Christopher Slobogin, *The Search and Seizure of Computers and Electronic Evidence: Transaction Surveillance by the Government*, 75 *Miss. L. J.* 139, 156 (2005).

<sup>98</sup> Slobogin, *supra* note 97.

Whether a person's utility records are public records differs from state to state.<sup>99</sup> Some states deem records of a municipally owned and operated electric utility as public records open for public inspection, while others have accorded these records statutory and constitutional protections.

In Florida, for example, records kept in connection with the operation of a city-operated utility are considered public records.<sup>100</sup> A similar policy applies in Georgia, where all records of a government agency, including utility records, must be open for inspection.<sup>101</sup> South Carolina, too, takes a similar approach.<sup>102</sup> It is not clear, however, from the reported cases whether these statutes permit access to personally identifiable information or simply operating records of the utility. Oklahoma is more explicit, permitting access to "records of the address, rate paid for services, charges, consumption rates, adjustments to the bill, reasons for adjustment, the name of the person that authorized the adjustment, and payment for each customer."<sup>103</sup> Oklahoma does protect some confidentiality, including "credit information, credit card numbers, telephone numbers, social security numbers, [and] bank account information for individual customers."<sup>104</sup> Other states, like Washington, specifically protect personally identifiable utility records. Washington does not require a showing of probable cause, but instead "a reasonable belief" that the record will help establish the customer committed a crime.<sup>105</sup> North Carolina likewise states that any "[b]illing information compiled and maintained by a city or county or other public entity providing utility services in connection with the ownership or operation of a public enterprise" is not a public record.<sup>106</sup>

---

<sup>99</sup> Because the focus of this report is federal law and the Fourth Amendment, a full treatment of state privacy law is beyond its scope.

<sup>100</sup> *In re Public Records—Records of Municipally Operated Utility*, Op. Att'y Gen. Fla. 74-35 (1974), available at <http://www.myfloridalegal.com/ago.nsf/Opinions/B4AED736C2272860852566B30067371A>; see FLA. STAT. §119.01(1) (2008) ("It is the policy of this state that all state, county, and municipal records are open for personal inspection by any person.").

<sup>101</sup> See GA. CODE ANN. §50-18-70(b) (2011); Op. Att'y Gen. Ga. 2000-4 (2000) (requiring personal utility records of certain public employees to be disclosed under public records law). Georgia defines a "public record" as "all documents, papers, letters, maps, books, tapes, photographs, computer based or generated information, or similar material prepared and maintained or received in the course of the operation of a public office or agency." GA. CODE ANN. §50-18-70(a).

<sup>102</sup> In South Carolina, public records include "information in or taken from any account, voucher, or contract dealing with the receipt or expenditure of public or other funds by public bodies." S.C. CODE ANN. §30-4-50 (2011). See Kelsey M. Swanson, *The Right to Know: An Approach to Gun Licenses and Public Access to Government Records*, 56 UCLA L. REV. 1579, 1601 (2009).

<sup>103</sup> OKLA. STAT. tit. 51, §24A.10 (2011).

<sup>104</sup> *Id.*

<sup>105</sup> WASH. REV. CODE §42.56.335 (2011). In Washington, the following rule applies to public utility districts and municipally owned electrical utilities:

A law enforcement authority may not request inspection or copying of records of any person who belongs to a public utility district or a municipally owned electrical utility unless the authority provides the public utility district or municipally owned electrical utility with a written statement in which the authority states that it suspects that the particular person to whom the records pertain has committed a crime and the authority has a reasonable belief that the records could determine or help determine whether the suspicion might be true. Information obtained in violation of this section is inadmissible in any criminal proceeding.

WASH. REV. CODE §42.56.335. The Washington Supreme Court has raised this protection to state constitutional status in *In re Personal Restraint of Maxfield*, 133 Wash. 2d 332, 344 (1997).

<sup>106</sup> However, the North Carolina public records law declares that "[n]othing contained herein is intended to limit public disclosure by a city or county of bill information: ... that is necessary to assist law enforcement, public safety, fire (continued...)

Determining whether a utility is a state actor or whether smart meter data is a public record are merely threshold matters. A finding that an entity is a state actor or data is public does not foreclose law enforcement's ability to retrieve customer smart meter data, but instead activates the next step of Fourth Amendment analysis: whether the government invaded a reasonable expectation of privacy.

## Reasonable Expectation of Privacy in Smart Meter Data

Under the modern conception of the Fourth Amendment, the government may not intrude into an area in which a person has an actual expectation of privacy that society would consider reasonable.<sup>107</sup> In the case of smart meter data, the government presumably seeks records in the custody of third-party utilities on the energy use at a specific home. However, a significant body of cases has refused to recognize constitutionally protected privacy interests in information provided by customers to businesses as part of their commercial relationships.<sup>108</sup> This theory, the third-party doctrine, permits police access to the telephone numbers a person dials<sup>109</sup> and to a person's bank documents,<sup>110</sup> free from Fourth Amendment constraints.

There are two relevant differences, however, between smart meters and the traditional third-party cases that may warrant a shift in approach. First is the possible judicial unease with the notion that advancement of technology threatens to erode further the constitutional protection of privacy.<sup>111</sup> From that perspective, as technology progresses, society faces an ever-increasing risk that an individual's activities will be monitored by the government. This is coupled with the concern that the breadth and granularity of personal information that new technology affords provide a far more intimate picture of an individual than the more limited snapshots available through prior technologies. Do the richness and scope of new information technologies warrant increased constitutional scrutiny?

Second, smart meters can convey information about the activities that occur inside the home, an area singled out for specific textual protection in the Fourth Amendment and one deeply ingrained in Anglo-Saxon law.<sup>112</sup> Even when the Court declared that "the Fourth Amendment protects people, not places,"<sup>113</sup> ostensibly shifting away from a property-based conception of the Fourth Amendment, it has still carved out special protections for the home.<sup>114</sup> However, concomitant with the increased use of technology in our private lives is increased exposure of our private activities, including those conducted in the home. Commonly, we share more personal

---

(...continued)

protection, rescue, emergency management, or judicial officers in the performance of their duties." N.C. GEN. STAT. §132-1.1(c)(3).

<sup>107</sup> *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

<sup>108</sup> *See Smith v. Maryland*, 442 U.S. 735 (1979).

<sup>109</sup> *Id.*

<sup>110</sup> *United States v. Miller*, 425 U.S. 435 (1976).

<sup>111</sup> *Kyllo v. United States*, 533 U.S. 27, 33-4 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

<sup>112</sup> *See Entick v. Carrington*, 19 How. St. Tr. 1029 (C.P. 1765).

<sup>113</sup> *Katz v. United States*, 389 U.S. 347, 351 (1967).

<sup>114</sup> *See Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809-10 (2004) [hereinafter Kerr, *Fourth Amendment and New Technologies*].

information, even as our concerns grow that more individuals, businesses, and others can glean more information about our personal lives as a matter of course. As with technology generally, does the fact that more of our lives are becoming “public” call for lesser or greater constitutional protection, and how does a “reasonable expectation”-based model continue to apply in a technologically intensive society?

This subpart will first look at the third-party doctrine as it is commonly conceived by the courts. Then it will discuss whether there are sufficient differences between the use of smart meters and traditional third-party cases to counsel against its application.

### Third-Party Doctrine

Traditionally, there has been no Fourth Amendment protection for information a consumer gives to business as part of their business dealings.<sup>115</sup> This doctrine dates back to the secret agent cases, in which any words uttered to another person, including a government agent or informant, were not covered by the Fourth Amendment.<sup>116</sup> It was later extended to business records, giving police access to documents such as telephone records,<sup>117</sup> bank records,<sup>118</sup> motel registration records,<sup>119</sup> and cell phone records.<sup>120</sup> The Supreme Court has reasoned that the customers assume the risk that the information could be handed over to government authorities,<sup>121</sup> and also that they consent to such access.<sup>122</sup> Some lower courts have applied this theory to traditional analog utility meters.<sup>123</sup> This section discusses the possible application of the third-party doctrine to smart meters.

In *Miller v. United States*, agents of the Bureau of Alcohol, Tobacco, and Firearms (ATF) subpoenaed several banks for records pertaining to the defendant, including copies of the defendant’s checks, deposit slips, and financial statements.<sup>124</sup> The defendant moved to suppress the records at trial, arguing that a warrantless retrieval of the bank records (his “private papers”)<sup>125</sup> was an intrusion into an area protected by the Fourth Amendment. The Court

---

<sup>115</sup> Orin S. Kerr, *The Case for a Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) [hereinafter Kerr, *Third-Party Doctrine*]. While the third-party doctrine has supporters like Professor Kerr, this group is overshadowed by its vocal detractors. Professor LaFave described its underpinnings as “dead wrong” and that the “Court’s woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection which the Court developed in *Katz*.” LAFAVE, *supra* note 78, §2.7(c). Justice Sotomayor lent credence to this sentiment in *United States v. Jones*, where she posited that it “may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” *United States v. Jones*, 565 U.S. \_\_\_, 5 (Sotomayor, J., concurring in the judgment and the opinion).

<sup>116</sup> *United States v. White*, 401 U.S. 745, 750 (1971) (holding that the Fourth Amendment “affords no protection to a wrongdoer’s misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.”) (internal quotation marks omitted).

<sup>117</sup> *Smith v. Maryland*, 442 U.S. 735 (1979).

<sup>118</sup> *United States v. Miller*, 425 U.S. 435 (1976).

<sup>119</sup> *United States v. Willis*, 759 F.2d 1486, 1498 (11<sup>th</sup> Cir. 1985).

<sup>120</sup> *United States v. Hynson*, No. 05-576, 2007 WL 2692327, at \*6 (E.D. Pa. Sept. 11, 2007).

<sup>121</sup> *Smith*, 442 U.S. at 744.

<sup>122</sup> Kerr, *Third-Party Doctrine*, *supra* note 115.

<sup>123</sup> *United States v. McIntyre*, 646 F.3d 1107 (8<sup>th</sup> Cir. 2011).

<sup>124</sup> *Miller*, 425 U.S. at 437-438.

<sup>125</sup> Brief for Respondent at 4, *Miller*, 425 U.S. 435 (No. 74-1179), 1975 WL 173642, at \*4 (“The Fourth Amendment is historically rooted in a concern for control over personal and private information in the face of governmental demands (continued...)”).

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

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

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

---

(...continued)

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

<sup>126</sup> *Miller*, 425 U.S. at 443.

<sup>127</sup> *Id.*

<sup>128</sup> *Smith v. Maryland*, 442 U.S. 735 (1979).

<sup>129</sup> *Id.* at 737.

<sup>130</sup> *Id.*

<sup>131</sup> *Id.*

<sup>132</sup> *Id.* at 743-44.

<sup>133</sup> *Id.* at 744.

<sup>134</sup> *United States v. Starkweather*, No. 91-30354, 1992 WL 204005, at \*2 (9<sup>th</sup> Cir. Aug. 24, 1992).

<sup>135</sup> *Id.*

<sup>136</sup> *United States v. McIntyre*, 646 F.3d 1107 (8<sup>th</sup> Cir. 2011).

<sup>137</sup> *Id.* at 1111.

<sup>138</sup> *Id.*

*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.<sup>139</sup>

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.<sup>140</sup> 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.”<sup>141</sup> 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.<sup>142</sup> 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.<sup>143</sup> 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.”<sup>144</sup> 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

---

<sup>139</sup> *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).

<sup>140</sup> *See Duncan Kennedy, Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1687, 1710 (1976).

<sup>141</sup> Kerr, *Third-Party Doctrine*, *supra* note 115, at 564.

<sup>142</sup> 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.

<sup>143</sup> *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.”).

<sup>144</sup> *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.<sup>145</sup>

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.<sup>146</sup> 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.<sup>147</sup> The agent used a thermal imager to scan the outside of Kyllo's apartment to determine if he was using these "grow" lamps.<sup>148</sup> Thermal imagers can detect energy emitting from the outside surface of an object.<sup>149</sup> 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.<sup>150</sup> From the passenger seat of his car, the agent scanned Kyllo's home for several minutes.<sup>151</sup> From his scan, he determined that the area over the garage and one side of his home were relatively hot compared to neighboring homes.<sup>152</sup> Based on utility bills, informant tips, and the results of thermal imaging, the agents obtained a warrant to search Kyllo's home.<sup>153</sup> As suspected, inside the home the agents found a marijuana growing operation, including over 100 plants.<sup>154</sup>

Justice Scalia first posited that "with very few exceptions, the question whether a warrantless search of the home is reasonable must be answered no."<sup>155</sup> Searches of the home were historically analyzed under the common law doctrine of trespass,<sup>156</sup> but during the mid-20<sup>th</sup> century the Court instead anchored the Fourth Amendment to a conception of privacy.<sup>157</sup> 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

---

<sup>145</sup> 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.

<sup>146</sup> *Kyllo v. United States*, 533 U.S. 27, 29 (2001).

<sup>147</sup> *Id.*

<sup>148</sup> *Id.*

<sup>149</sup> *Id.*

<sup>150</sup> *Id.* at 29-30.

<sup>151</sup> *Id.* at 30.

<sup>152</sup> *Id.*

<sup>153</sup> *Id.*

<sup>154</sup> *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 (9<sup>th</sup> 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.

<sup>155</sup> *Kyllo*, 533 U.S. at 31.

<sup>156</sup> See *Olmstead v. United States*, 277 U.S. 438 (1928).

<sup>157</sup> *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.

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.<sup>158</sup>

The Court ultimately held that “obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search—at least where (as here) the technology in question is not in general public use.”<sup>159</sup> *Kyllo* affirmed the notion that “an expectation of privacy in activities taking place inside the home is presumptively reasonable.”<sup>160</sup>

The Court also protected home privacy by prohibiting the monitoring of the location of a beeper while inside a residence.<sup>161</sup> In *United States v. Karo*, with the consent of a government informant the police attached a beeper to the false bottom of a can of ether, which was sold to Karo.<sup>162</sup> The can of ether was transported between several residences and storage facilities.<sup>163</sup> The police used the beeper to monitor the location of the can several times while it was located inside of the residences.<sup>164</sup> The Court was asked to determine “whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.”<sup>165</sup> The Court answered in the affirmative.

The Court reiterated the long-standing notion that “private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.”<sup>166</sup> Unless there are exigent circumstances, “searches and seizures inside a home without a warrant are presumptively unreasonable....”<sup>167</sup> The Court ultimately held that the warrantless monitoring of the beeper in the home was a Fourth Amendment violation.<sup>168</sup>

*Kyllo* and *Karo* demonstrate that the Supreme Court “has defended the home as a sacred site at the ‘core of the Fourth Amendment.’”<sup>169</sup> Although neither the Supreme Court nor any lower federal court has ruled on the use of smart meters, a few propositions can be deduced from *Kyllo* and *Karo* bearing on this question.

Because smart meters allow law enforcement to access information regarding intimate details occurring inside the home, a highly invasive investigation that could not otherwise be performed without intrusion into the home, a court may require a warrant to access this data. In *Kyllo*, the

---

<sup>158</sup> *Kyllo*, 533 U.S. at 34.

<sup>159</sup> *Id.* (internal quotation marks omitted).

<sup>160</sup> Lerner & Mulligan, *supra* note 60, ¶ 18.

<sup>161</sup> *United States v. Karo*, 468 U.S. 705 (1984).

<sup>162</sup> *Id.* at 708.

<sup>163</sup> *Id.*

<sup>164</sup> *Id.* at 709-10.

<sup>165</sup> *Id.*

<sup>166</sup> *Id.* at 714.

<sup>167</sup> *Id.* at 714-15.

<sup>168</sup> *Id.* at 718.

<sup>169</sup> Stephanie M. Stern, *The Inviolable Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 913 (2010) (citing *Wilson v. Layne*, 526 U.S. 603, 612 (1999)).



police merely obtained the relative temperatures of a house,<sup>170</sup> and in *Karo* the police only generally located the beeper in the house.<sup>171</sup> 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.<sup>172</sup> 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.)<sup>173</sup> Unfortunately, the Court provided no criterion for making this determination.<sup>174</sup> Several courts applying this test have held that night vision goggles were in general public use.<sup>175</sup> 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.<sup>176</sup> In 2009, the Department of Energy estimated that 4.75% of all electric meters were smart meters.<sup>177</sup> The department projects that by 2012 approximately 52 million more meters will be installed.<sup>178</sup> 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.<sup>179</sup> 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.<sup>180</sup> 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

---

<sup>170</sup> *United States v. Kyllo*, 533 U.S. 27, 30 (2001).

<sup>171</sup> *Karo*, 468 U.S. at 705, 709-10.

<sup>172</sup> 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.

<sup>173</sup> *Kyllo*, 533 U.S. at 34.

<sup>174</sup> 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).

<sup>175</sup> See *United States v. Dellas*, 355 F. Supp. 2d 1095, 1107 (N.D. Cal. 2005).

<sup>176</sup> *United States v. Vela*, 486 F. Supp. 2d 587, 590 (W.D. Tex. 2005).

<sup>177</sup> DEP’T OF ENERGY, SMART GRID SYSTEM REPORT vi (2009), available at [http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SGSRMain\\_090707\\_lowres.pdf](http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SGSRMain_090707_lowres.pdf).

<sup>178</sup> *Id.*

<sup>179</sup> *United States v. Kyllo*, 533 U.S. 27, 29 (2001).

<sup>180</sup> *United States v. McIntyre*, 646 F.3d 1107, 1111-12 (8<sup>th</sup> Cir. 2011).

more invasive than a look at each item in isolation.<sup>181</sup> 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.<sup>182</sup> In *United States v. Jones*, the police used a GPS tracking device to track Jones’s movements for almost a month.<sup>183</sup> 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.<sup>184</sup> The physical intrusion, rather than a *Katz*-type invasion of privacy, was the lynchpin of the decision.<sup>185</sup> 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.”<sup>186</sup> 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.”<sup>187</sup> 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.”<sup>188</sup>

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

<sup>181</sup> See *Cent. Intelligence Agency v. Sims*, 471 U.S. 159, 178 (1985).

<sup>182</sup> 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/>.

<sup>183</sup> *United States v. Jones*, 565 U.S. \_\_\_, 2 (2012).

<sup>184</sup> *Id.* at 3.

<sup>185</sup> *Id.* at 4.

<sup>186</sup> *Id.* at 13 (Alito, J., concurring in the judgment).

<sup>187</sup> *Id.* at 3 (Sotomayor, J., concurring in the judgment and the opinion).

<sup>188</sup> *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010).

conducted on a prolonged, 24-hour basis.<sup>189</sup> “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.”<sup>190</sup> 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.<sup>191</sup> In comparison, in *Katz* the police listened to the contents of *Katz*’s phone call—the actual words spoken.<sup>192</sup> 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.<sup>193</sup> 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.”<sup>194</sup>

With banking or telephone services, a customer has the option of transferring his business to another bank or another telephone carrier.<sup>195</sup> 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,

---

<sup>189</sup> *Id.* at 558.

<sup>190</sup> *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.

<sup>191</sup> *Smith*, 442 U.S. at 741 (citing *Katz v. United States*, 389 U.S. 347 (1967)).

<sup>192</sup> *Katz*, 389 U.S. at 348.

<sup>193</sup> *Smith*, 442 U.S. at 744 (citing *United States v. Miller*, 425 U.S. 435 (1976)).

<sup>194</sup> Kerr, *Third-Party Doctrine*, *supra* note 115, at 588.

<sup>195</sup> *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.<sup>196</sup>

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.<sup>197</sup>

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."<sup>198</sup>

## 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),<sup>199</sup> the Stored Communications Act (SCA),<sup>200</sup> and the Computer Fraud and Abuse Act (CFAA)<sup>201</sup> may be applicable to these situations and are discussed in more detail below.

---

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

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

<sup>198</sup> Kerr, *Fourth Amendment and New Technologies*, *supra* note 114, at 806.

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

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

<sup>201</sup> 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.”<sup>202</sup> 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....”<sup>203</sup> Based on the description of the smart meter network provided above,<sup>204</sup> 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.<sup>205</sup> 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.<sup>206</sup> 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.<sup>207</sup>

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.<sup>208</sup> 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<sup>209</sup> 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

---

<sup>202</sup> S.Rept. 99-541 at 3.

<sup>203</sup> 18 U.S.C. §2510(12).

<sup>204</sup> 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).

<sup>205</sup> 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.

<sup>206</sup> 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.

<sup>207</sup> “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).

<sup>208</sup> 18 U.S.C. §2511(2)(c).

<sup>209</sup> 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.<sup>210</sup> It also limits the use and dissemination of information intercepted.<sup>211</sup> In addition, when an interception order expires, authorities must notify those whose communications have been intercepted.<sup>212</sup> Law enforcement may also conduct electronic surveillance when acting in an emergency situation pending issuance of a court order.<sup>213</sup>

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.<sup>214</sup> Although it is often discussed in relation to the prevention of terrorism, it applies to the gathering of foreign intelligence information for other purposes.<sup>215</sup> Although some exceptions apply, such as for emergency situations,<sup>216</sup> 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.<sup>217</sup>

## The Stored Communications Act (SCA)

The SCA was enacted in 1986 as Title II of the Electronic Communications Privacy Act (ECPA),<sup>218</sup> to “address[] access to stored wire and electronic communications and transactional records.”<sup>219</sup> 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.<sup>220</sup> 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.<sup>221</sup> The SCA also provides a mechanism by which law enforcement may compel the disclosure of stored communications.<sup>222</sup>

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

---

<sup>210</sup> 18 U.S.C. §§2516, 2518(3).

<sup>211</sup> 18 U.S.C. §2517.

<sup>212</sup> 18 U.S.C. §2518(8).

<sup>213</sup> 18 U.S.C. §2518(7).

<sup>214</sup> See 50 U.S.C. §1801(a) (definition of “foreign power”).

<sup>215</sup> 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”).

<sup>216</sup> 50 U.S.C. §1805(e).

<sup>217</sup> 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.

<sup>218</sup> P.L. 99-508.

<sup>219</sup> S.Rept. 99-541 at 3.

<sup>220</sup> 18 U.S.C. §2701(a). Unauthorized access includes exceeding an authorization to use the facility. *Id.*

<sup>221</sup> 18 U.S.C. §2702.

<sup>222</sup> 18 U.S.C. §2703.

discuss the protections and disclosure restrictions that might apply to any smart meter network that qualifies as an ECS or RCS.

## Electronic Communication Services

An ECS is defined by the SCA as any service which provides users “the ability to send or receive wire or electronic communications.”<sup>223</sup> The statute also defines an “electronic communication” 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.”<sup>224</sup> As described above, one of the essential functions of a smart meter would appear to be the capability to transmit consumer electricity usage data to the smart grid using a variety of communications technologies.<sup>225</sup> These transmissions would seem to fall neatly within the SCA’s definition of an electronic communication. Therefore, whether a smart meter network would qualify as an ECS would likely depend on whether the deployed smart meters could be said to be providing this ability to users.

It is not clear whether it would be accurate to categorically describe smart meters as providing customers with “the ability to send or receive” communications. It could be argued that a utility customer would use the smart meter to transmit usage information to the utility, in the same way that the same customer uses a traditional meter to record household electricity usage over a billing period. However, the Ninth Circuit has suggested that an ECS should not include situations in which electronic communications are used only “as an incident to providing some other service, as is the case with a street-front shop that requires potential customers to speak into an intercom device before permitting entry, or a ‘drive-thru’ restaurant that allows customers to place orders via a two-way intercom located beside the drive-up lane.”<sup>226</sup> On one hand, it may not be accurate to describe utility customers as users of smart meters at all, particularly if the deployment of such smart meters is intended principally for the benefit of the utility and does not change the experience of utility customers. On the other hand, some of the proposed uses of deployed smart meters may include using collected data for the benefit of the customers, for example by determining the energy efficiency of specific household appliances.<sup>227</sup> As a result, the ultimate classification of a particular smart meter network as an ECS may depend largely on the specific facts present, such as the manner in which it is marketed, or the ostensible purposes for which the transmissions are intended to be used.

If a smart meter network qualifies as an ECS, then transmissions containing smart meter data would be protected under the SCA only while such transmissions are in electronic storage, as that term is defined by the statute.<sup>228</sup> Therefore, one must first determine whether, and under what circumstances, the data collected by a smart meter network is in electronic storage in order to determine what protections apply.

---

<sup>223</sup> 18 U.S.C. §2510(15).

<sup>224</sup> 18 U.S.C. §2510(12). Wire communications are defined as communications containing the human voice and are not implicated here. 18 U.S.C. §2510(1).

<sup>225</sup> See *supra* note 47 and accompanying text.

<sup>226</sup> *Company v. United States (In re United States)*, 349 F.3d 1132, 1141 (9<sup>th</sup> Cir. 2003) (holding that definition of ECS includes service that provides drivers with the ability to make phone calls from their car for directory assistance, driving directions, or roadside assistance because those activities are intrinsically communicative).

<sup>227</sup> See *supra* note 8.

<sup>228</sup> 18 U.S.C. §2701.

For purposes of the SCA, a communication is in electronic storage at an ECS if it is in temporary, intermediate storage incidental to electronic transmission or in storage for backup protection.<sup>229</sup> As applied to the smart meter network, data residing on the smart meter itself prior to being sent to the utility would appear to be in electronic storage, as such storage is likely temporary and undertaken solely in anticipation of some eventual transmission to the utility. In contrast, once the data has arrived at the utility and resides on its servers, it may no longer be in temporary or intermediate storage. However, some form of the communications may still be being held for backup purposes, and in such a case might be considered in electronic storage under the statute. To the extent that the data would be considered in electronic storage, either while on the meter or on the utility's computers, the data would appear to be subject to the SCA's provisions applicable to providers of ECS.

The SCA prohibits intentionally accessing without authorization, a facility through which an ECS is provided and obtaining, altering, or preventing access to an electronic communication while it is in electronic storage.<sup>230</sup> Criminal penalties for violating the SCA's prohibitions on unauthorized access start at imprisonment for not more than one year (not more than five years for a subsequent conviction) and/or a fine of not more than \$100,000.<sup>231</sup> However, violations committed for malicious, mercenary, tortious or criminal purposes are subject to higher penalties and may be punished by imprisonment for not more than five years (not more than 10 years for a subsequent conviction) and/or a fine of not more than \$250,000 (not more than \$500,000 for organizations).<sup>232</sup> Victims of a violation of the SCA also have a civil cause of action for equitable relief, reasonable attorneys' fees and costs, and damages equal to the loss and gain associated with the offense but not less than \$1,000.<sup>233</sup>

The SCA generally restricts the ability of providers of ECS to disclose the contents of communications in electronic storage, if the ECS is offering those services to the public.<sup>234</sup> However, the statute also permits certain disclosures to law enforcement. Such permitted disclosures by a provider of electronic communication services to law enforcement can be either voluntary or compelled. Normally, voluntary disclosure to law enforcement is authorized only if the contents of the communication were inadvertently obtained by the service provider and appear to pertain to the commission of a crime.<sup>235</sup> However, it should be noted that the utility in this case appears to be the intended recipient of all communications sent over the smart meter network, and the SCA's restrictions on disclosures of electronically stored information held by ECS or RCS providers may generally be overcome if an intended recipient of the communication consents to the disclosure.<sup>236</sup> Consequently, the utility may have more latitude to share communications in electronic storage with law enforcement than a traditional provider of ECS, such as a telephone company, would have.

---

<sup>229</sup> 18 U.S.C. §2510(17).

<sup>230</sup> 18 U.S.C. §2701(a). Unauthorized access includes exceeding an authorization to use the facility. *Id.*

<sup>231</sup> 18 U.S.C. §2701(b)(2).

<sup>232</sup> 18 U.S.C. §2701(b)(1).

<sup>233</sup> 18 U.S.C. §2707.

<sup>234</sup> 18 U.S.C. §2702(a)(1) ("a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service").

<sup>235</sup> 18 U.S.C. §2702(b)(7).

<sup>236</sup> *See* 18 U.S.C. §2702(b)(3).



For purposes of compelled disclosures to law enforcement, the SCA distinguishes between recent communications and those that have been in electronic storage for more than 180 days. A search warrant is required to compel providers to disclose communications held in electronic storage for 180 days or less.<sup>237</sup> However, communications held for more than 180 days may be obtained by law enforcement through a warrant, subpoena, or a court order supported by specific and articulable facts sufficient to establish reasonable grounds to believe that the contents are relevant and material to an ongoing criminal investigation.<sup>238</sup> Customers whose communications have been disclosed are generally required to be given notice of such disclosure, but such disclosure may be delayed if notification might result in endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial.<sup>239</sup>

## Remote Computing Services

It is likely that the classification of a smart meter network as an RCS would similarly be fact-dependent. The SCA defines an RCS as a service in which computer storage or processing services by means of an ECS are provided to the public.<sup>240</sup> It is conceivable that the data collected by smart meters may in fact be stored or processed by the utility, but there is no indication that such storage or processing would be categorically provided as a service to the public, rather than solely for the utility's internal benefit.<sup>241</sup> If such service is not provided to the public, then it would likely be inaccurate to classify the smart meter network as an RCS. However, if one of the features of a particular smart meter deployment is to give customers the ability to store or process their usage data, then it would appear to qualify as an RCS.

For those smart meter networks which qualify as an RCS, the SCA generally protects the contents of electronically transmitted communications "carried or maintained on that service" for customers of the service. Disclosures of such information are generally prohibited,<sup>242</sup> but the SCA also provides a means for law enforcement to obtain access to the contents of such communications. The government may obtain a warrant supported by probable cause, or use a subpoena or a court order supported by specific and articulable facts sufficient to establish reasonable grounds to believe that the contents are relevant and material to an ongoing criminal investigation.<sup>243</sup> However, use of a subpoena or court order supported by specific and articulable facts also requires the government to give prior notice to the customer whose information is sought, unless particular circumstances warrant delayed notice.<sup>244</sup> RCS customers whose

---

<sup>237</sup> 18 U.S.C. §2703(a).

<sup>238</sup> 18 U.S.C. §2703(d). Some courts have held that this "reasonable grounds" standard is a less demanding standard than "probable cause." See *In re Application of the United States*, 620 F.3d 304, 313 (3d Cir. 2010) ("We also conclude that this [§2703(d)] standard is a lesser one than probable cause.").

<sup>239</sup> 18 U.S.C. §2705(a).

<sup>240</sup> 18 U.S.C. §2711(2).

<sup>241</sup> However, if some other service provided by the utility allows the data collected by a smart meter to be stored or manipulated for the benefit of the utility's customers, it is possible that this system would fall within the definition of an RCS.

<sup>242</sup> The SCA allows providers of an RCS to disclose stored communications with the consent of the subscriber of an RCS. 18 U.S.C. §2702(b)(3).

<sup>243</sup> 18 U.S.C. §2703(b)(1).

<sup>244</sup> 18 U.S.C. §2703(b)(1)(B).

communications have been disclosed in violation of the SCA may pursue a civil cause of action for equitable relief, reasonable attorneys' fees and costs, and damages equal to the loss and gain associated with the offense but not less than \$1,000.<sup>245</sup>

## The Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) prohibits intentionally accessing and obtaining information from a computer used in or affecting interstate commerce, without authorization or in excess of a granted authorization.<sup>246</sup> The definition of a computer for purposes of the CFAA is “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” excluding “an automated typewriter or typesetter, a portable hand held calculator, or other similar device....”<sup>247</sup>

The servers on a utility's network would likely fall squarely within the definition of a computer under the CFAA. Similarly, smart meters themselves also appear to meet the definition of a computer, insofar as they store customers' energy usage data and also perform logical operations by routing transmissions across the utility's network. Additionally, in light of the significant role that energy utilities play in the modern economy, the smart meter network would also likely be considered to have an effect on interstate commerce, even if they operate entirely within one state. Therefore, intentionally gaining access to the utility's servers or smart meters to obtain customer data would likely constitute a violation of the CFAA if done without the utility's authorization or in excess of an authorization granted by the utility.

The criminal penalties for violating the unauthorized access provisions of the CFAA have a three tier sentencing structure. Simple violations are punished as misdemeanors, imprisonment for not more than one year and/or a fine of not more than \$100,000 (\$200,000 for organizations).<sup>248</sup> At the next level, cases in which: “(i) the offense was committed for purposes of commercial advantage or private financial gain; (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or (iii) the value of the information obtained exceeds \$5,000” may be punished by imprisonment for not more than five years and/or a fine of not more \$250,000 (\$500,000 for organizations).<sup>249</sup> The third tier is for repeat offenders whose punishment is increased to imprisonment of not more than 10 years and/or a fine of not more than \$250,000 (\$500,000 for organizations) for a second or subsequent conviction.<sup>250</sup>

---

<sup>245</sup> 18 U.S.C. §2707.

<sup>246</sup> 18 U.S.C. §1030(a)(2). 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.

<sup>247</sup> 18 U.S.C. §1030(e)(1).

<sup>248</sup> 18 U.S.C. §1030(c)(2)(A).

<sup>249</sup> 18 U.S.C. §1030(c)(2)(B).

<sup>250</sup> 18 U.S.C. §§1030(c), 3571.

## The Federal Trade Commission Act (FTC Act)

Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce”<sup>251</sup> and gives the Federal Trade Commission (FTC) jurisdiction to bring enforcement actions against “persons, partnerships, or corporations” that engage in these practices.<sup>252</sup> In the past, the FTC has used its authority under Section 5 to take action against businesses that violate their own privacy policies or that fail to adequately safeguard a consumer’s personal information.<sup>253</sup> Although there do not appear to be any cases in which the FTC has taken action against an electric utility for failing to protect consumer smart meter data, the Commission would have authority to enforce Section 5 against a utility that fell within its statutory jurisdiction.

### Covered Electric Utilities

This section considers whether the FTC would have Section 5 jurisdiction over each of the four types of electric utilities identified by the Energy Information Administration (EIA): investor-owned, publicly owned, federally owned, and cooperative.<sup>254</sup> It finds that the FTC clearly has jurisdiction over investor-owned utilities. It is unclear whether the Commission has jurisdiction over publicly owned utilities or federally owned utilities. The FTC could enforce Section 5 against for-profit electric cooperatives, and case law suggests that nonprofit electric cooperatives may also be subject to the act’s requirements.

The FTC has jurisdiction to enforce Section 5 against “persons, partnerships, or corporations,” with exceptions not applicable here.<sup>255</sup> Utilities that are “persons” or “partnerships” would be subject to the FTC’s enforcement powers automatically,<sup>256</sup> as the statute does not provide any additional jurisdictional requirements for these entities. Most electric utilities, however, are organized as legal entities that would potentially fit within the definition of “corporation.” The FTC Act states that, for the purposes of Section 5, the term “corporation”:

shall be deemed to include any company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, which is organized to carry on business for its own profit or that of its members, and has shares of capital or capital stock or certificates of interest, and any company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, without shares of capital or capital stock or certificates of interest, except partnerships, which is organized to carry on business for its own profit or that of its members.<sup>257</sup>

---

<sup>251</sup> 15 U.S.C. §45(a)(1).

<sup>252</sup> 15 U.S.C. §45(a)(2).

<sup>253</sup> See “Enforcement of Data Privacy and Security,” *infra* p. 41; see also NIST PRIVACY REPORT, *supra* note 11, at 23 n.48.

<sup>254</sup> ENERGY INFO. ADMIN., ELECTRIC POWER INDUSTRY OVERVIEW (2007) [hereinafter EIA ELECTRIC POWER OVERVIEW], available at <http://www.eia.gov/cneaf/electricity/page/prim2/toc2.html>.

<sup>255</sup> 15 U.S.C. §45(a)(2).

<sup>256</sup> The FTC Act does not further define “persons” or “partnerships” or impose any additional jurisdictional requirements on these entities in the way that it does for “corporations.” See 15 U.S.C. §44.

<sup>257</sup> 15 U.S.C. §44.

This definition, particularly in its use of the words “shall be deemed to include,” suggests that a wide variety of legal entities could potentially constitute “corporations.” Moreover, in *California Dental Ass’n v. FTC*, the Supreme Court remarked that the “FTC Act directs the Commission to prevent the *broad set of entities* under its jurisdiction” from violating Section 5.<sup>258</sup> In that case, the Court found that the term “corporation” also included *nonprofit* entities, so long as they imparted significant economic benefit to their members.<sup>259</sup> Thus, as the Court’s opinion demonstrates, the key question when determining whether an entity is a “corporation” for the purposes of Section 5 jurisdiction is not what legal form the entity takes, but rather whether the entity is “organized to carry on business for its own profit or that of its members.”

### Investor-Owned Utilities

Investor-owned utilities are clearly subject to the FTC’s Section 5 jurisdiction as “corporations.” The EIA defines investor-owned electric utilities as those that “have the fundamental objective of producing a profit for their investors” and distributing these profits as dividends or reinvesting them in the business.<sup>260</sup> These utilities satisfy the definition of “corporation” under the statute because they are companies organized to carry on business for the profit of their investors.<sup>261</sup>

### Publicly Owned Utilities

It is unclear whether the FTC has Section 5 jurisdiction over publicly owned utilities. The agency probably lacks jurisdiction over these utilities if it characterizes them as “corporations,” but it is possible that it may have jurisdiction over them if it characterizes them as “persons.” Publicly owned utilities include “municipals, public utility districts and public power districts, State authorities, irrigation districts, and joint municipal action agencies.”<sup>262</sup> The EIA describes these as “nonprofit government entities that are organized at either the local or State level,” are exempt from state and federal income taxes, and “provide service to their communities and nearby consumers at cost.”<sup>263</sup> In contrast to investor-owned utilities or cooperatively owned utilities, publicly owned utilities obtain capital by issuing debt rather than selling an ownership interest in the utility to investors or members.<sup>264</sup>

### As “Corporations”

Publicly owned utilities probably do not fall within the FTC’s Section 5 jurisdiction over “corporations” because they are not organized to carry on business for profit. Rather, governments form these utilities for the sole purpose of distributing electricity to consumers at

---

<sup>258</sup> Cal. Dental Ass’n v. FTC, 526 U.S. 756, 768 (1999) (emphasis added) (internal quotation marks omitted).

<sup>259</sup> *Id.* at 766-69.

<sup>260</sup> EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

<sup>261</sup> Indeed, the FTC has asserted Section 5 jurisdiction over holding companies with investor-owned electric utility subsidiaries in the past. *See, e.g., DTE Energy Co.*, 131 F.T.C. 962 (May 15, 2001) (complaint); *CMS Energy Corp.*, 127 F.T.C. 827 (June 2, 1999) (complaint). *See also In re DTE Energy Co.*, FTC File No. 001 0067 (May 15, 2001) (consent order); *In re CMS Energy Corp.*, FTC File No. 991 0046 (June 2, 1999) (consent order).

<sup>262</sup> EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

<sup>263</sup> *Id.*

<sup>264</sup> DAVID E. McNABB, PUBLIC UTILITIES: MANAGEMENT CHALLENGES FOR THE 21<sup>ST</sup> CENTURY 165 (2005).

cost.<sup>265</sup> Significantly, when publicly owned utilities realize net income—that is, revenues they earn in excess of their expenses—they either (1) use it to finance their operations in lieu of issuing more debt,<sup>266</sup> or (2) transfer it to the general fund of the political subdivision that they serve.<sup>267</sup> These utilities typically lack investors or members to which they could distribute net income as dividends.<sup>268</sup> Thus, publicly owned utilities are probably not “organized to carry on business” for profit and are probably exempt from the FTC’s Section 5 jurisdiction if characterized as “corporations.”

### As “Persons”

It is unclear whether a court would find that the FTC has Section 5 jurisdiction over publicly owned utilities as “persons,” as a court could employ several different canons of statutory interpretation when deciding whether “persons” includes state or local government entities.<sup>269</sup> In the 1980s, the FTC attempted to assert Section 5 jurisdiction over two state-chartered municipal corporations—the cities of New Orleans and Minneapolis—as “persons,” alleging that the cities engaged in unfair methods of competition by assisting taxicab companies in maintaining high prices and stifling competition.<sup>270</sup> The Commission later withdrew both complaints, and thus no court considered whether jurisdiction was proper. More recently, the Commission has asserted jurisdiction over state government agencies that regulate certain professions such as dentistry,<sup>271</sup> optometry,<sup>272</sup> and funeral services.<sup>273</sup>

There appears to be only one court case that engages in a full discussion and interpretation of the meaning of “persons” under Section 5. In *California State Board of Optometry v. FTC*, the D.C. Circuit Court of Appeals considered “whether a State acting in its sovereign capacity is a ‘person’ within the FTC’s enforcement jurisdiction.”<sup>274</sup> The FTC had issued a rule declaring “certain state laws restricting the practice of optometry to be unfair acts or practices.”<sup>275</sup> Petitioners, which were state boards of optometry and professional associations, argued that the court should strike down the rule because it went beyond the FTC’s statutory authority.<sup>276</sup> In vacating the rule, the court found nothing in the relevant provisions of the FTC Act “to indicate that Congress intended to authorize the FTC to reach the ‘acts or practices’ of States acting in their sovereign capacities.”<sup>277</sup>

<sup>265</sup> EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

<sup>266</sup> MCNABB, *supra* note 264, at 165.

<sup>267</sup> EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

<sup>268</sup> MCNABB, *supra* note 264, at 165.

<sup>269</sup> In contrast to entities that are “corporations,” the FTC does not have to show that entities qualifying as “persons” are organized for profit. See 15 U.S.C. §44.

<sup>270</sup> *In re City of Minneapolis*, 105 F.T.C. 304 (May 7, 1985) (order withdrawing complaint); *In re City of New Orleans*, 105 F.T.C. 1 (Jan. 3, 1985) (order withdrawing complaint).

<sup>271</sup> *In re N.C. State Bd. of Dental Exam’rs*, 151 F.T.C. 607 (Feb. 3, 2011) (state action opinion); *In re South Carolina State Bd. of Dentistry*, 138 F.T.C. 229 (Sept. 12, 2003) (complaint).

<sup>272</sup> *In re Mass. Board of Registration in Optometry*, 110 F.T.C. 549 (June 13, 1988) (decision).

<sup>273</sup> *In re Va. Bd. of Funeral Dirs. & Embalmers*, 138 F.T.C. 645 (Oct. 1, 2004) (complaint).

<sup>274</sup> 910 F.2d 976, 979 (D.C. Cir. 1990).

<sup>275</sup> *Id.* at 978.

<sup>276</sup> *Id.* at 978-79.

<sup>277</sup> *Id.* at 980, 982.

A court approaching the question of whether “persons” includes publicly owned utilities would start with the language of the statute. Courts traditionally give broad deference to an agency when the agency interprets the extent of its own jurisdiction unless the reach of its jurisdiction is clear from reading the statute “under ordinary principles of construction.”<sup>278</sup> Attempting to discern the Commission’s jurisdiction under Section 5 of the FTC Act is difficult, as the statute does not define the term “persons” for the purposes of that provision. Title 1, Section 1 of the United States Code (the Dictionary Act) provides: “In determining the meaning of any Act of Congress, *unless the context indicates otherwise* ... the words ‘person’ and ‘whoever’ include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals.”<sup>279</sup>

However, the context in which “persons” appears in Section 5 probably forecloses the use of the default definition of “person” in the Dictionary Act. In Section 5, Congress listed the terms “persons,” “partnerships,” and “corporations” separately, which indicates that it intended to give each term independent significance. The terms “corporations” and “partnerships” would not have independent meaning in Section 5 if the term “persons” in Section 5 included the entities listed in the Dictionary Act. Furthermore, the FTC Act requires that “corporations” be organized for their own profit or the profit of their members in order for the FTC to exercise jurisdiction over them—a requirement it does not impose on the other entities.<sup>280</sup> By reading the term “persons” to include the entities listed in the Dictionary Act, the FTC could evade this additional requirement simply by bringing its complaint against an entity as a “person” rather than a “corporation”—a result that Congress probably did not intend. Thus, a court that ended its analysis here could find that the meaning of “persons” remains ambiguous. The court could then choose to defer to the FTC’s broad interpretation of its own jurisdiction under the Supreme Court’s decision in *Chevron U.S.A., Inc. v. NRDC, Inc.*<sup>281</sup>

The *California Optometry* court, however, declined to defer to the FTC’s interpretation of its own jurisdiction because it found that principles of federalism outweighed *Chevron* deference.<sup>282</sup> Quoting the Supreme Court’s decision in *Will v. Michigan Department of State Police*,<sup>283</sup> the

<sup>278</sup> See *Cal. Dental Ass’n v. FTC*, 526 U.S. 756, 765-66 (1999) (“Respondent urges deference to this interpretation of the Commission’s jurisdiction as reasonable. But we have no occasion to review the call for deference here, the interpretation urged in respondent’s brief being clearly the better reading of the statute under ordinary principles of construction.”) (internal citations omitted); see also *Chevron U.S.A., Inc. v. NRDC, Inc.*, 467 U.S. 837, 842-43 (1984).

<sup>279</sup> 1 U.S.C. §1 (emphasis added).

<sup>280</sup> See 15 U.S.C. §44.

<sup>281</sup> *Chevron*, 467 U.S. at 842-43. In that case, the Court held that

When a court reviews an agency’s construction of the statute which it administers, it is confronted with two questions. First, always, is the question whether Congress has directly spoken to the precise question at issue. If the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress. If, however, the court determines Congress has not directly addressed the precise question at issue, the court does not simply impose its own construction on the statute, as would be necessary in the absence of an administrative interpretation. Rather, if the statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency’s answer is based on a permissible construction of the statute. *Id.*

<sup>282</sup> Todd H. Cohen, *Double Vision: The FTC, State Regulation, and Deciding What’s Best for Consumers*, 59 GEO. WASH. L. REV. 1249, 1267 (1991) (“In sum, the *California State Board of Optometry* court relied on federalism principles to justify protecting state interests. The court extended the judicially-created *Parker* state action doctrine to cover FTC trade regulation rules and applied the clear statement doctrine to prevent the FTC from invalidating a state law as unfair without additional congressional action.”).

<sup>283</sup> 491 U.S. 58 (1989).

*California Optometry* court stated that “in common usage, the term person does not include the sovereign, and statutes employing the word are ordinarily construed to exclude it.”<sup>284</sup> In the *Will* case, the Court considered whether the term “person” as it appeared in 42 U.S.C. §1983 included a state.<sup>285</sup> The Court held that it did not, invoking the principles of federalism when it wrote that “[t]his approach is particularly applicable where it is claimed that Congress has subjected the States to liability to which they had not been subject before.”<sup>286</sup> The Court found that the statute’s language fell “far short of satisfying the ordinary rule of statutory construction that if Congress intends to alter the ‘usual constitutional balance between the States and Federal Government,’ it must make its intention to do so ‘unmistakably clear in the language of the statute.’”<sup>287</sup>

The Court’s decision in *Will*, as interpreted by the D.C. Circuit in *California Optometry*, suggests that Congress must clearly indicate in a particular statute when it wishes to subject states to a new form of liability, particularly when this would change the balance between state and federal authority by intruding on the actions a state takes in its sovereign capacity. There does not appear to be a clear indication that Congress intended the word “persons” in the FTC Act to subject publicly owned utilities to FTC enforcement actions.<sup>288</sup> Thus, if the FTC’s enforcement of Section 5 against a publicly owned utility would alter the balance between the state and federal governments, a court might read “persons” to exclude these utilities. As the *California Optometry* court indicated, whether the balance is altered may depend on whether the operation of the utility amounts to the state acting in its sovereign capacity (balance altered) or merely engaging in a proprietary function (balance not altered).<sup>289</sup> The *California Optometry* court suggested that whether a state is acting in its sovereign capacity or engaging in a proprietary function may vary according to the antitrust laws’ state action doctrine, a multi-pronged analysis that is beyond the scope of this report.<sup>290</sup> If a court found that the state was acting in its sovereign capacity when the state (or one of its subdivisions) operated an electric utility, the court could hold that the FTC does not have Section 5 jurisdiction because of the federalism principles and clear statement rule that guided the interpretation of the statute in *Will* and were adopted by the court in *California Optometry*.<sup>291</sup>

A third possible choice for a court would be to adopt the reasoning of the FTC and find that Congress clearly intended “persons” to include government entities, because under the other antitrust laws, the term “persons” includes state and local government entities, and the antitrust

<sup>284</sup> *California Optometry*, 910 F.2d 976, 980 (D.C. Cir. 1990) (internal quotation marks omitted).

<sup>285</sup> *Will*, 491 U.S. at 60.

<sup>286</sup> *Id.* at 64.

<sup>287</sup> *Id.* at 65 (citations omitted).

<sup>288</sup> Representative Covington, the sponsor of the act, explained during floor debate on the measure that Section 5 “embraces within the scope of that section every kind of person, natural or artificial, who may be engaged in interstate commerce.” 51 CONG. REC. 14,928 (1914). Despite this remark, courts have not taken such a broad view of the FTC’s jurisdiction under the act. Even the Supreme Court has held that there are some limits on the entities covered by Section 5. See *Cal. Dental Ass’n v. FTC*, 526 U.S. 756, 766-67 (1999) (requiring, for jurisdiction, that a “proximate relation” must exist between the activities of a nonprofit and the benefit it provides to its members, and implying that the activities must confer “more than *de minimis* or merely presumed economic benefits” on the members).

<sup>289</sup> See *California Optometry*, 910 F.2d at 980-81 (“This rule of statutory construction serves to ensure that the States’ sovereignty interests are adequately protected by the political process.”).

<sup>290</sup> *Id.* at 980. For more information on the factors that courts consider when making this determination, see FED. TRADE COMM’N, REPORT OF THE STATE ACTION TASK FORCE (2003), available at <http://www.ftc.gov/os/2003/09/stateactionreport.pdf>.

<sup>291</sup> See Cohen, *supra* note 282, at 1267.

laws, including the FTC Act,<sup>292</sup> should be read together.<sup>293</sup> The *California Optometry* court acknowledged this argument, writing that “several Supreme Court decisions hold that a State *is* a person for purposes of the antitrust laws.”<sup>294</sup> The court ultimately rejected the argument, however, because it found that “when a State acts in a sovereign rather than a proprietary capacity, it is exempt from the antitrust laws even though those actions may restrain trade,” and that this state action doctrine may “limit the reach of the FTC’s enforcement jurisdiction.”<sup>295</sup> Thus, if a court found that a state acted in its *proprietary* capacity when the state (or one of its subdivisions) operated a public utility, then the state action doctrine would not apply, and it would be possible for a court to find jurisdiction even under the *California Optometry* case. The FTC has advanced this reasoning, arguing that the state boards over which it asserts jurisdiction do not amount to the states acting in their sovereign capacities.<sup>296</sup> Whether the operation of a particular publicly owned utility consists of the state acting in its sovereign capacity or engaging in a proprietary function may vary according to the antitrust laws’ state action doctrine, a multi-pronged analysis that is beyond the scope of this report.<sup>297</sup>

Thus, whether a court would find that the word “persons” in Section 5 includes certain government entities such as publicly owned utilities is unclear because it may depend on which, if any, of several principles of statutory construction the court adopts. A court could, among other options: (1) find that the meaning of “persons” in Section 5 is ambiguous, and thus defer to the FTC’s broad interpretation of its own jurisdiction because of the *Chevron* doctrine; (2) find that the statute is ambiguous, but that principles of federalism outweigh the court’s usual *Chevron* deference to the Commission’s interpretation of its own jurisdiction—a determination that may require a court to find that the state is acting in its sovereign capacity when the state (or one of its subdivisions) operates an electric utility; or (3) find that Congress clearly intended “persons” to include government entities because Section 5 should be read together with the other antitrust laws, under which the term “person” includes state and local government entities—a determination that may require a court to find that the state is performing a proprietary function when the state (or one of its subdivisions) operates a utility.

## Federally Owned Utilities

It is unclear whether the FTC could enforce Section 5 against a federally owned utility. Indeed, there does not appear to be any case in which the FTC has sought to enforce Section 5 against a federal agency.<sup>298</sup> The FTC probably lacks Section 5 jurisdiction over the nine federally owned

<sup>292</sup> Although this report focuses on the FTC’s consumer law cases under Section 5 (“unfair or deceptive acts or practices”), and not its antitrust cases (“unfair methods of competition”), both types of prohibited activities share the same phrase for the purposes of determining the agency’s jurisdiction: “persons, partnerships, or corporations.” See 15 U.S.C. §45(a)(2).

<sup>293</sup> See *In re Mass. Board of Registration in Optometry*, 110 F.T.C. 549 (June 13, 1988) (decision) (citations omitted).

<sup>294</sup> *California Optometry*, 910 F.2d at 980 (citations omitted).

<sup>295</sup> *Id.* at 980 (citation omitted).

<sup>296</sup> See, e.g., *In re N.C. State Bd. of Dental Exam’rs*, 151 F.T.C. 607 (Feb. 3, 2011) (state action opinion); *In re Mass. Board of Registration in Optometry*, 110 F.T.C. 549 (June 13, 1988) (decision).

<sup>297</sup> For more information on the factors that courts consider when making this determination, see FED. TRADE COMM’N, REPORT OF THE STATE ACTION TASK FORCE (2003), available at <http://www.ftc.gov/os/2003/09/stateactionreport.pdf>.

<sup>298</sup> This report does not consider whether any constitutional implications would result if the FTC, an independent executive branch agency, brought an enforcement proceeding against another executive branch agency. See generally Michael Eric Herz, *When Can the Federal Government Sue Itself?*, 32 WM. & MARY L. REV. 893 (1991).



utilities operating in the United States<sup>299</sup> if it characterizes them as “corporations.” Like publicly owned utilities, federally owned utilities are not organized for profit. As the EIA notes, “federal power is not sold for profit, but to recover the costs of operations and repay the Treasury for funds borrowed to construct generation and transmission facilities.”<sup>300</sup> If the Commission characterizes these utilities as “persons,” it is unclear whether a court would find that this term includes government entities.<sup>301</sup>

As a practical matter, FTC enforcement of Section 5 against federally owned utilities is probably unnecessary in the context of smart meter data because of other federal laws, such as the Privacy Act,<sup>302</sup> that would likely protect this data when it is stored in records systems maintained by federal agencies, including federally owned utilities.<sup>303</sup>

### Cooperatively Owned Utilities

For-profit electric cooperatives would clearly fall within the Commission’s Section 5 jurisdiction over “corporations” operated for their own profit or that of their members.<sup>304</sup> Indeed, the FTC has maintained jurisdiction over for-profit cooperatives as “corporations” in the past, including a rural healthcare cooperative<sup>305</sup> and a wine maker.<sup>306</sup> However, it appears that most electric cooperatives—and particularly the cooperatives that will receive funds under the Department of Energy’s Smart Grid Investment Grant program—are nonprofits.<sup>307</sup>

It is possible that the FTC would have Section 5 jurisdiction over these nonprofit electric cooperatives as “corporations” organized for profit. These distribution utilities are owned by the “consumers they serve,” and those that are tax-exempt must “provide electric service to their members at cost, as that term is defined by the Internal Revenue Service.”<sup>308</sup> However, when the activities of a cooperative result in revenues that exceed the cooperative’s costs, these “net margins ... are considered a contribution of equity by the members that are required to be returned to the members consistent with the organization’s bylaws and lender limitations imposed as a condition of loans.”<sup>309</sup> Thus, in contrast to publicly owned utilities, which typically transfer any net income to the general fund of the government that they serve, electric cooperatives return net margins to their members as equity, and when that equity is retired by the board of directors, members receive cash payments.<sup>310</sup> Although it does not appear that a court has considered

<sup>299</sup> EIA ELECTRIC POWER OVERVIEW, *supra* note 254. Among these utilities are the Tennessee Valley Authority, the four power marketing administrations in the Department of Energy, and the Army Corps of Engineers. *Id.*

<sup>300</sup> *Id.*

<sup>301</sup> See *supra* notes 269-97 and accompanying text.

<sup>302</sup> 5 U.S.C. §552a.

<sup>303</sup> See “The Federal Privacy Act of 1974,” *infra* p. 45.

<sup>304</sup> 15 U.S.C. §44.

<sup>305</sup> *In re* Minn. Rural Health Coop., FTC File No. 051 0199 (Dec. 28, 2010) (decision and order).

<sup>306</sup> *In re* Heublein, Inc., 96 F.T.C. 385 (Oct. 7, 1980) (final order).

<sup>307</sup> See DEP’T OF ENERGY, CASE STUDY – NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION SMART GRID INVESTMENT GRANT 1, available at [http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NRECA\\_case\\_study.pdf](http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NRECA_case_study.pdf).

<sup>308</sup> EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

<sup>309</sup> *Id.* “Net margins” is the term given to “revenues in excess of the cost of providing service.” *Id.*

<sup>310</sup> See, e.g., Cent. Rural Electric Coop., Patronage Capital, <http://www.crec.coop/CRECAvantage/PatronageCapital/tabid/711/Default.aspx> (“Allocated patronage capital appears as an entry on the permanent financial records of the (continued...)”).

whether the FTC has Section 5 jurisdiction over a nonprofit electric cooperative that returns its net margins to its consumer-members in addition to providing them with electricity service, the Supreme Court, as well as lower federal courts, have issued guidance on factors that a court may consider in answering this question.

### *Applicable Law*

Under Section 5, the FTC Act requires that a “corporation” be “organized to carry on business for its own profit or that of its members.”<sup>311</sup> In *California Dental Ass’n v. FTC*, the Court considered whether the FTC could enforce Section 5 against a “voluntary nonprofit association of local dental societies” that was exempt from paying federal income tax and furnished its members with “advantageous insurance and preferential financing arrangements” in addition to lobbying, litigating, and advertising on their behalf.<sup>312</sup> The Court found that the FTC had jurisdiction over the California Dental Association as a “corporation,” stating that

the FTC Act is at pains to include not only an entity “organized to carry on business for its own profit,” but also one that carries on business for the profit “of its members.” While such a supportive organization may be devoted to helping its members in ways beyond immediate enhancement of profit, no one here has claimed that such an entity must devote itself single-mindedly to the profit of others. It could, indeed, hardly be supposed that Congress intended such a restricted notion of covered supporting organizations, with the opportunity this would bring with it for avoiding jurisdiction where the purposes of the FTC Act would obviously call for asserting it.<sup>313</sup>

The Court declined to specify the percentage of a nonprofit entity’s activities that must be “aimed at its members’ pecuniary benefit” to subject it to FTC jurisdiction.<sup>314</sup> However, the Court wrote that a “proximate relation” must exist between the activities of the entity and the profits of its members, and implied that the activities must confer “more than *de minimis* or merely presumed economic benefits” on the members.<sup>315</sup> The Court’s justification for this result was that “nonprofit entities organized on behalf of for-profit members have the same capacity and derivatively, at

---

(...continued)

cooperative and reflect [sic] your equity or ownership in CREC. When patronage capital is retired, a check or bill credit is issued to you and your equity in the cooperative is reduced. ... When considering a retirement, the board analyzes the financial health of the cooperative and will not authorize a retirement that will adversely affect the financial integrity of the cooperative.”); Fall River Rural Electric Coop., Patronage Capital, <http://www.frrec.com/myAccount/patronageCapital.aspx> (“The Cooperative’s Board of Directors retires patronage capital when finances allow, often on an annual basis. The oldest patronage capital is retired first. Fall River currently retires patronage capital on a rotation of approximately 20 years.”); Kauai Island Util. Coop., Member Patronage Capital Information, [http://www.kiuc.coop/member\\_patcap-qa.htm](http://www.kiuc.coop/member_patcap-qa.htm) (“A portion of Patronage Capital may be periodically paid to the members upon approval of the Board of Directors and our lenders.”); Sulphur Springs Valley Electric Coop., Inc., Patronage Capital Credits, [http://www.ssvvec.org/?page\\_id=583](http://www.ssvvec.org/?page_id=583) (“Capital credits represent your share of the Cooperative’s margins – margins are the operating revenue remaining after operating expenses. The amount assigned in your name depends on your energy purchases. To calculate this, we divide your annual energy purchase by the Cooperative’s operating income for the year. The more electricity you buy, the more capital credits you earn.”).

<sup>311</sup> 15 U.S.C. §44 (emphasis added).

<sup>312</sup> 526 U.S. 756, 759-60, 767 (1999).

<sup>313</sup> *Id.* at 766 (internal citations omitted).

<sup>314</sup> *Id.*

<sup>315</sup> *Id.* at 766-67.

least, the same incentives as for-profit organizations to engage in unfair methods of competition or unfair and deceptive acts.”<sup>316</sup>

It is clear that the FTC may still have Section 5 jurisdiction even when the benefits that a nonprofit provides to its members are secondary to its charitable functions. In *American Medical Ass’n v. FTC*, the Second Circuit considered whether the FTC could enforce Section 5 against three medical professional associations, including the American Medical Association (AMA), a nonprofit corporation composed of “physicians, osteopaths, and medical students.”<sup>317</sup> The court, acknowledging that the associations served “both the business and non-business interests of their member physicians,” found jurisdiction because the “business aspects” of their activities, including lobbying for members and offering business advice to them, subjected them to the FTC’s jurisdiction despite the fact that the business aspects “were considered secondary to the charitable and social aspects of their work.”<sup>318</sup>

When determining whether jurisdiction exists, a court may consider other factors in addition to the benefits that the nonprofit provides to its members. In *Community Blood Bank v. FTC*, the Eighth Circuit considered whether a “corporation” included all nonprofit corporations.<sup>319</sup> The appeals court held that the FTC lacked Section 5 jurisdiction over nonprofit blood banks because the banks’ activities did not result in “profit” in the sense of “gain from business or investment over and above expenditures.”<sup>320</sup> The blood banks, the court observed, lacked shares of capital, capital stock, or certificates, and were “organized for and actually engaged in business for only charitable purposes.”<sup>321</sup> One bank’s articles of incorporation touted the entity’s charitable purposes, and all of the banks were exempt from paying federal income taxes.<sup>322</sup> Upon dissolution, the corporations would transfer their assets to other charitable or nonprofit organizations.<sup>323</sup> In addition, none of the funds collected by the blood banks had “ever been distributed or inured to the benefit of any of their members, directors or officers.”<sup>324</sup> The court found that these factors made the blood banks “charitable organizations” both “in law and in fact,” exempting them from the FTC’s Section 5 jurisdiction.<sup>325</sup>

## Analysis

The case law suggests several factors that a court may weigh when determining whether a private, nonprofit entity composed of members, such as an electric cooperative, is subject to the FTC’s Section 5 jurisdiction as a “corporation.”<sup>326</sup> The most significant factor is whether the nonprofit

---

<sup>316</sup> *Id.* at 768.

<sup>317</sup> 638 F.2d 443, 446 (1980).

<sup>318</sup> *Id.* at 448. The court noted in passing that the AMA’s articles of incorporation stated that one purpose of the organization was to “safeguard the material interests of the medical profession.” *Id.*

<sup>319</sup> 405 F.2d 1011, 1015 (8<sup>th</sup> Cir. 1969).

<sup>320</sup> *See id.* at 1017. The court also remarked that at least one case had established that “even though a corporation’s income exceeds its disbursements its nonprofit character is not necessarily destroyed.” *Id.*

<sup>321</sup> *Id.* at 1020, 1022.

<sup>322</sup> *Id.* at 1020.

<sup>323</sup> *Id.*

<sup>324</sup> *Id.*

<sup>325</sup> *Id.* at 1019.

<sup>326</sup> This analysis assumes that a court would extend the holdings of the applicable case law, which covered entities organized as nonprofit corporations and professional associations, to include entities organized as nonprofit electric (continued...)

provides an economic benefit to its members that is more than *de minimis* and that is proximately related to the nonprofit's activities. This benefit need not be the sole—or even primary—function of the nonprofit. Additional factors that the case law suggests weigh in favor of a finding of jurisdiction include that the nonprofit: (1) has gain from its business or investments that exceeds its expenditures; (2) has shares of capital or capital stock or certificates; (3) is not organized solely for charitable purposes or does not engage only in charitable work; (4) has articles of incorporation that list profit-seeking objectives; (5) is subject to federal income tax liability; (6) would distribute its assets to profit-seeking entities upon dissolution; and (7) distributes any of the funds it collects to its members, directors, or officers.

It is possible that the FTC has Section 5 jurisdiction over nonprofit electric cooperatives, although the outcome in any particular case may depend on the characteristics of the individual utility. A court could find that the typical nonprofit electric cooperative provides “economic benefit” to its members in at least two ways: (a) by providing electricity service to members,<sup>327</sup> and (b) by returning net margins to members in the form of patronage capital, which is an ownership interest in the cooperative that is later converted to cash payments to members when that capital is retired.<sup>328</sup> With regard to (a), it is likely that a court would find that electricity service is an “economic benefit” as defined in the case law. In *California Dental Ass’n*, the nonprofit professional association provided “advantageous insurance and preferential financing arrangements,” as well as lobbying, litigation, and advertising services to its members.<sup>329</sup> In *American Medical Ass’n*, the nonprofit lobbied on behalf of its members and offered business advice to members.<sup>330</sup> These benefits, it is assumed, enabled the members to more easily conduct business profitably. Electricity service allows people to conduct activities at all times of the day, and thus provides a similar and clearly significant economic benefit to those who use it, whether for business or recreational purposes. As the primary objective of an electric cooperative is to provide electricity service to members, the necessary proximate relation between the activities of the nonprofit and the benefit to its members clearly exists.

Despite its pecuniary nature, there are a few problems with considering benefit (b), patronage capital, to be an “economic benefit” as defined by the Court. First, it is not clear that patronage capital actually is a benefit. A court could view patronage capital as a no-interest *loan* from the consumer-member to the utility,<sup>331</sup> or, because it is typically allocated to member accounts in a manner proportional to members’ spending on electricity, simply a *refund* of money collected from the members that reflects the actual cost of providing service in a particular year.<sup>332</sup> If

---

(...continued)

cooperatives.

<sup>327</sup> Many cooperatives provide other services to their communities that could constitute “economic benefits.” The National Rural Electric Cooperative Association notes that, “In addition to electric service, many electric co-ops are involved in community development and revitalization projects” that include “small business development and jobs creation, improvement of water and sewer systems, and assistance in delivery of health care and educational services.” Nat’l Rural Electric Coop. Ass’n, Member Directory, <http://www.nreca.coop/members/MemberDirectory/Pages/default.aspx>.

<sup>328</sup> See sources cited *supra* note 310.

<sup>329</sup> Cal. Dental Ass’n v. FTC, 526 U.S. 756, 759-60, 767 (1999).

<sup>330</sup> Am. Med. Ass’n v. FTC, 638 F.2d 443, 448 (1980).

<sup>331</sup> See, e.g., Cent. Rural Electric Coop., Patronage Capital, <http://www.crec.coop/CRECAvantage/PatronageCapital/tabid/711/Default.aspx> (“These margins represent an interest-free loan of operating capital by the membership to the cooperative.”).

<sup>332</sup> See, e.g., Kauai Island Util. Coop., Member Patronage Capital Information, [http://www.kiuc.coop/member\\_patcap-\(continued...\)](http://www.kiuc.coop/member_patcap-(continued...))

adopted by a court, neither of these characterizations would appear to be consistent with the “profit” that the statute describes<sup>333</sup> or the “economic benefit” that the Supreme Court requires for a nonprofit to be a “corporation.”

Second, even if a court found patronage capital to be an economic benefit, it is not clear that it is more than *de minimis*. Patronage capital must be “retired” before members receive cash payments for it.<sup>334</sup> Retirements are made at the discretion of the cooperative’s board of directors because the capital is needed to finance the cooperative’s ongoing expenses, and thus retirement of a class of capital typically occurs after a long rotation period, such as 20 years.<sup>335</sup> Although the Supreme Court did not hold that an “economic benefit” must produce *immediate* advantage to the members of a nonprofit, a court could potentially view the decades-long delay in cash payments as significantly decreasing the degree of economic benefit that the capital provides. In addition, patronage capital would probably be considered *de minimis* if the cooperative’s net margins were small, as this would mean that little capital would be issued to members. It is thus difficult to discern whether a court would find that an economic benefit accrues to members as a result of their receipt of patronage capital, which nevertheless probably bears the requisite “proximate relation” to the activities of the cooperative that produce any net margins distributed as capital.

With regard to the additional factors, those favoring jurisdiction include (2) cooperatives typically have shares of capital stock, including patronage capital,<sup>336</sup> (3) cooperatives do not operate solely for the benefit of the people outside of the organization like the nonprofits in *Community Blood Bank* did because cooperatives provide electricity service and patronage capital to their members,<sup>337</sup> and (7) an electric cooperative typically returns any net margins to members in the form of patronage capital, an ownership interest refunded to consumer-members as cash when the capital is retired.<sup>338</sup> Factors that cannot be evaluated because they are specific to each individual cooperative include (1) whether the revenues of the cooperative exceed its expenditures; (4) the particular objectives listed in a cooperative’s articles of incorporation or other foundational document; (5) whether a nonprofit electric cooperative is exempt from federal income tax liability, which depends on whether it meets the requirements under Section 501(c)(12) of the Internal Revenue Code;<sup>339</sup> and (6) whether a cooperative would distribute its assets to profit-seeking entities upon dissolution—a factor that also may depend on state laws.<sup>340</sup>

It is likely that a court would find that nonprofit electric cooperatives impart economic benefits to their members by distributing electricity to them or, possibly, by issuing patronage capital to them. However, because many of the other factors that courts consider may differ for each

---

(...continued)

qa.htm (characterizing the retirement of patronage capital as a “refund”).

<sup>333</sup> 15 U.S.C. §44.

<sup>334</sup> See sources cited *supra* note 310.

<sup>335</sup> See *id.*

<sup>336</sup> See Nat’l Rural Electric Coop. Ass’n, Seven Cooperative Principles, <http://www.nreca.coop/members/SevenCoopPrinciples/Pages/default.aspx> (describing “Members’ Economic Participation”).

<sup>337</sup> Whether electricity service and patronage capital, which are clearly benefits, constitute “economic benefits” within the meaning of the Supreme Court’s holding in *California Dental Ass’n* is a separate question.

<sup>338</sup> See sources cited *supra* note 310.

<sup>339</sup> I.R.C. §501(c)(12).

<sup>340</sup> See *Cnty. Blood Bank v. FTC*, 405 F.2d 1011, 1020 (8<sup>th</sup> Cir. 1969).

particular cooperative, it is not possible to draw any general conclusions about whether the FTC would have Section 5 jurisdiction over these entities as “corporations.”

## Enforcement of Data Privacy and Security

If the FTC has Section 5 jurisdiction over a particular electric utility, it may bring an enforcement action against the utility if its privacy or security practices with regard to consumer smart meter data constitute “unfair or deceptive acts or practices in or affecting commerce.”<sup>341</sup> The FTC Act defines an “unfair” act or practice as one that “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”<sup>342</sup> According to the FTC, an act or practice is “deceptive” if it is a material “representation, omission or practice” that is likely to mislead a consumer acting reasonably in the circumstances.<sup>343</sup> The history of the Commission’s enforcement of consumer data privacy and security practices shows that the agency has brought complaints against entities that (1) engage in “deceptive” acts or practices by failing to comply with their stated privacy policies; or (2) employ “unfair” practices by failing to adequately secure consumer data from unauthorized parties.<sup>344</sup> Often, conduct constituting a violation could fall under either category, as a failure to protect consumer data may be an unfair practice because of the unavoidable injury it causes, as well as a deceptive practice because it renders an entity’s privacy policy materially misleading.

### “Deceptive” Privacy Statements

A utility that fails to comply with its own privacy policy may engage in a “deceptive” act or practice under Section 5 of the FTC Act. In *Facebook, Inc.*, the FTC alleged, among other things, that the social networking site violated promises contained in its privacy policy when it made users’ personal information accessible to third parties without users’ consent.<sup>345</sup> Facebook had claimed that users could limit third-party access to their personal information on the site. Despite this promise, applications run by users’ Facebook friends were able to access the users’ personal information. The Commission also charged that Facebook altered its privacy practices without users’ consent, causing personal information that had been restricted by users to be available to third parties. This change, which allegedly “caused harm to users, including, but not limited to, threats to their health and safety, and unauthorized revelation of their affiliations” constituted both a “deceptive” and an “unfair” practice in the view of the Commission.<sup>346</sup> Finally, the Commission alleged that Facebook had represented to users that it would not share their personal information with advertisers but had done so anyway.

---

<sup>341</sup> 15 U.S.C. §45(a)(1). For more details on FTC enforcement of consumer data privacy and security under Section 5, see CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens.

<sup>342</sup> 15 U.S.C. §45(n).

<sup>343</sup> *In re Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984) (policy statement at end of opinion).

<sup>344</sup> See *Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 11<sup>th</sup> Cong. (2010) (statement of Jon D. Leibowitz, Chairman, Fed. Trade Comm’n) (describing the FTC’s enforcement activity in the areas of consumer data privacy and security), available at <http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf>. The FTC recently released a preliminary report on the consumer privacy implications of new technologies. FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (2010), available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

<sup>345</sup> FTC File No. 092 3184 (Nov. 29, 2011) (complaint).

<sup>346</sup> *Id.*

In *Twitter, Inc.*, the FTC alleged that the social networking site engaged in “deceptive” acts when it violated claims made in its privacy policy about the security of consumer data by failing to “use reasonable and appropriate security measures to prevent unauthorized access to nonpublic user information.”<sup>347</sup> The Commission found that Twitter had permitted its administrators to access the site with easy-to-guess passwords and failed to limit the extent of administrators’ access according to the requirements of their jobs. In a consent order, the company agreed not to misrepresent its privacy controls and to implement a comprehensive information security program that would be assessed by an independent third party.<sup>348</sup>

As smart meter data becomes valuable to third parties,<sup>349</sup> utilities may be tempted to sell or share this information with others to increase revenues and provide new services to their customers. If prohibited by the terms of the utility’s privacy policy, it may be a “deceptive” act or practice for the utility to share a consumer’s personal information with third parties without a consumer’s consent.<sup>350</sup> The FTC could also find deception when a utility represents that its privacy controls are capable of protecting smart meter data when, in fact, they are not.

## “Unfair” Failure to Secure Consumer Data

### *Failure to Protect Against Common Technology Threats or Unauthorized Access*

The FTC may consider it an “unfair” practice when an electric utility fails to safeguard smart meter data from well-known technology threats as the data travels across the utility’s communications networks. For example, in *DSW Inc.*, the FTC brought enforcement proceedings against the respondent, the owner of several shoe stores.<sup>351</sup> The agency alleged that the respondent failed to protect customers’ credit card and check information as it was transmitted to the issuing bank for authorization. The information collected at the register traveled wirelessly to the store’s computer network, and from there to the bank or check processor, which communicated its response back to the store through the same channels. The agency charged that

[a]mong other things, respondent (1) created unnecessary risks to the information by storing it in multiple files when it no longer had a business need to keep the information; (2) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks; (3) stored the information in unencrypted files that could be accessed easily by using a commonly known user ID and password; (4) did not limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and (5) failed to employ sufficient measures to detect unauthorized access. As a result, a hacker could use the wireless access points on one in-store computer network to connect to, and access personal information, on the other in-store and corporate networks.<sup>352</sup>

<sup>347</sup> FTC File No. 092 3093 (Mar. 2, 2011) (complaint).

<sup>348</sup> FTC File No. 092 3093 (Mar. 2, 2011) (decision and order).

<sup>349</sup> NIST PRIVACY REPORT, *supra* note 11, at 14, 35-36.

<sup>350</sup> As suggested below, it may also be an “unfair” practice, regardless of whether the utility has a privacy policy.

<sup>351</sup> FTC File No. 052 3096 (Mar. 7, 2006) (complaint).

<sup>352</sup> *Id.*

Similarly, in *Cardsystems Solutions, Inc.*, the Commission brought a complaint against a credit and debit card authorization processor.<sup>353</sup> The FTC alleged that the respondent failed to protect its systems by neglecting to guard its network against “commonly known or reasonably foreseeable attacks” that could be avoided using low-cost methods.<sup>354</sup> As part of settlement agreements in *DSW* and *Cardsystems*, the respondents had to create “a comprehensive information security program” to protect consumer information that would be assessed periodically by an independent third party.<sup>355</sup>

Smart meters also transmit personal consumer information, often wirelessly, across several different communications networks located in various physical places.<sup>356</sup> Thus, it is possible that the FTC would view a utility’s failure to protect smart meter data against common technology threats as an “unfair” practice if the utility could have avoided the threats by using low-cost methods such as encrypting the data; storing it in fewer places and for no longer than needed; implementing basic wireless network security; and taking other reasonable measures suggested by the agency in *DSW Inc.*

### *Failure to Dispose of Data Safely*

A utility’s failure to dispose of smart meter data safely may also constitute an “unfair” practice under Section 5. For example, in *Rite Aid Corp.*, the respondent, the owner of retail pharmacy stores, purportedly failed to safely dispose of personal information in its possession when it neglected to: “(1) implement policies and procedures to dispose securely of such information,” including rendering “the information unreadable in the course of disposal; (2) adequately train employees to dispose securely of such information; (3) use reasonable measures to assess compliance with its established policies and procedures for the disposal of such information; and (4) employ a reasonable process for discovering and remedying risks to such information.”<sup>357</sup> The information was later found in various publicly accessible garbage dumpsters in readable form. This suggests that utilities holding smart meter data and other personal information, whether on electronic or physical media, must ensure that the methods used to destroy this data render it unreadable to third parties.

### **Penalties**

There is no private right of action in the FTC Act. If the Commission has “reason to believe” that a violation has occurred, it may, after notice to the respondent and an opportunity for a hearing, issue an order directing the respondent to cease and desist from acts or practices that the agency finds violate the act.<sup>358</sup> If the respondent disobeys an order that has become final, the U.S. Attorney General may bring an action in district court seeking the imposition of civil monetary

---

<sup>353</sup> FTC File No. 052 3148 (Sept. 5, 2006) (complaint).

<sup>354</sup> *Id.*

<sup>355</sup> *See, e.g., In re Cardsystems Solutions, Inc.*, FTC File No. 052 3148 (Sept. 5, 2006) (decision and order).

<sup>356</sup> NIST PRIVACY REPORT, *supra* note 11, at 23.

<sup>357</sup> FTC File No. 072 3121 (Nov. 12, 2010) (complaint).

<sup>358</sup> 15 U.S.C. §45(b). The Commission may seek a preliminary injunction in district court if it “has reason to believe” that an entity subject to the Commission’s jurisdiction “is violating, or is about to violate, any provision of law enforced” by the FTC, and such an injunction would be in the public interest. 15 U.S.C. §53(b). In “proper cases the Commission may seek, and after proper proof, the court may issue, a permanent injunction.” *Id.*



penalties of up to \$16,000 per violation (\$16,000 per day for continuing violations), as well as further injunctive and equitable relief that the court deems appropriate.<sup>359</sup>

After a party becomes subject to a final cease and desist order under the act, the Commission may seek redress for consumers by bringing suit in state or federal court against the party if the Commission “satisfies the court that the act or practice to which the cease and desist order relates is one which a reasonable man would have known under the circumstances was dishonest or fraudulent.”<sup>360</sup> “Such relief may include, but shall not be limited to, rescission or reformation of contracts, the refund of money or return of property, the payment of damages,” and public notification of the violation, “except nothing in [15 U.S.C. §57b(b)] is intended to authorize the imposition of any exemplary or punitive damages.”<sup>361</sup> Once the Commission has issued a final cease and desist order (not a consent order) finding an act or practice to be deceptive, then it may bring suit in district court to obtain a civil penalty against an entity that engages in that act or practice: (1) after the order became final (“whether or not such person, partnership, or corporation was subject to such cease and desist order”); and (2) “with actual knowledge that such act or practice is unfair or deceptive and is unlawful” under Section 5 of the FTC Act.<sup>362</sup>

## The Federal Privacy Act of 1974 (FPA)

Smart meter electricity usage data pertaining to U.S. citizens or permanent residents that is retrievable by personal identifier from a system of records maintained by any federal “agency,” including federally owned utilities, is subject to the protections contained in the Privacy Act<sup>363</sup> when it is maintained, collected, used, or disseminated by the agency.

### Federally Owned Utilities as “Agencies”

All nine of the federally owned utilities are federal agencies covered by the Privacy Act. For the purposes of the act, the term “agency” includes, but is not limited to, “any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.”<sup>364</sup> According to EIA, utilities that are part of an executive department include the four power marketing administrations in the Department of Energy (Bonneville, Southeastern, Southwestern, and Western), the International Boundary and Water Commission in the Department of State, and the Bureau of Indian Affairs and the Bureau

<sup>359</sup> 15 U.S.C. §45(l). The size of the civil monetary penalty was last adjusted for inflation in 2009. 16 C.F.R. §1.98.

<sup>360</sup> 15 U.S.C. §57b(a)(2).

<sup>361</sup> 15 U.S.C. §57b(b).

<sup>362</sup> 15 U.S.C. §45(m)(1)(B).

<sup>363</sup> 5 U.S.C. §552a. The federally owned utilities primarily sell electricity to nonprofit electric utilities on the wholesale markets rather than distribute electricity directly to consumers. EIA ELECTRIC POWER OVERVIEW, *supra* note 254. As these utilities provide only about 1% of total sales of electricity to end user consumers, *id.*, they may be unlikely to acquire consumer smart meter data, which is typically transmitted to distribution utilities. However, as the smart grid becomes more interconnected, more utilities at different points in the smart grid may come into possession of this data. NIST PRIVACY REPORT, *supra* note 11, at 23.

<sup>364</sup> See 5 U.S.C. §552(f)(1). The act also covers data in a “system of records” operated by a government contractor on behalf of a federal agency. See 5 U.S.C. §552a(m).

of Reclamation in the Department of the Interior.<sup>365</sup> The U.S. Army Corps of Engineers resides in the Department of Defense, which is an executive department.<sup>366</sup> The Tennessee Valley Authority is a government-owned corporation.<sup>367</sup>

## Smart Meter Data as a Protected “Record”

The Privacy Act protects the type of electricity usage data gathered by smart meters, provided that the data pertains to U.S. citizens or permanent residents, is personally identifiable, and is retrievable by the individual’s name or another personal identifier. The Privacy Act “governs the collection, use, and dissemination of a ‘record’ about an ‘individual’ maintained by federal agencies in a ‘system of records.’”<sup>368</sup> Under the statute, a “record” is “any item, collection, or grouping of information about an individual that is maintained by an agency ... that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.”<sup>369</sup>

An “individual” is defined as “a citizen of the United States or an alien lawfully admitted for permanent residence.”<sup>370</sup> A “system of records” is “a group of any records under the control of any agency from which information is retrieved by the name of the individual” or other personal identifier “assigned to the individual.”<sup>371</sup>

Smart meter data held by an agency certainly fits within the broad definition of a “record” because it is a grouping of information about an individual, namely, data on that individual’s electricity usage. The data is typically stored along with a consumer’s account information, which usually includes a consumer’s name, social security number, or other “identifying particular.”<sup>372</sup> Thus, smart meter data would constitute a protected “record” under the Privacy Act, assuming that it pertains to a citizen of the United States or lawful permanent resident and is retrievable by a personal identifier such as a consumer’s name or account number.

## Requirements

For information on the general safeguards that the Privacy Act provides for data that is maintained by a federal agency and meets the other requirements for a covered record under the act, see CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens.

---

<sup>365</sup> EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

<sup>366</sup> DEP’T OF THE ARMY CORPS OF ENG’RS, CIVIL WORKS STRATEGIC PLAN 1 (2004), *available at* [http://www.corpsresults.us/pdfs/cw\\_strat.pdf](http://www.corpsresults.us/pdfs/cw_strat.pdf). It is also a “Major Command within the Army.” *Id.*

<sup>367</sup> Tenn. Valley Auth., About TVA, <http://www.tva.com/abouttva/index.htm>.

<sup>368</sup> See CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens (citations omitted).

<sup>369</sup> 5 U.S.C. §552(a)(4).

<sup>370</sup> 5 U.S.C. §552a(a)(2).

<sup>371</sup> 5 U.S.C. §552a(a)(5).

<sup>372</sup> NIST PRIVACY REPORT, *supra* note 11, at 26-27.

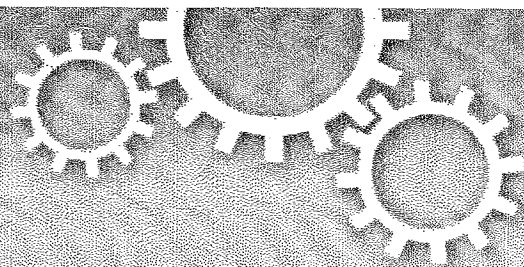
## **Author Contact Information**

Brandon J. Murrill  
Legislative Attorney  
bmurrill@crs.loc.gov, 7-8440

Edward C. Liu  
Legislative Attorney  
eliu@crs.loc.gov, 7-9166

Richard M. Thompson II  
Legislative Attorney  
rthompson@crs.loc.gov, 7-8449

# EXHIBIT 5



SUBJECT AREAS:  
DEVELOPMENT  
PATTERN FORMATION  
BIOPHYSICS  
ANIMAL BEHAVIOUR

Received  
13 July 2011

Accepted  
17 February 2012

Published  
15 March 2012

Correspondence and  
requests for materials  
should be addressed to  
H.S.T. (hugh.taylor@  
yale.edu)

# Fetal Radiofrequency Radiation Exposure From 800-1900 Mhz-Rated Cellular Telephones Affects Neurodevelopment and Behavior in Mice

Tamir S. Aldad<sup>1,2</sup>, Geliang Gan<sup>2</sup>, Xiao-Bing Gao<sup>2,3</sup> & Hugh S. Taylor<sup>1,2,4</sup>

<sup>1</sup>Department of Molecular, Cellular, and Developmental Biology, Yale University, New Haven, CT 06520, <sup>2</sup>Department of Obstetrics, Gynecology, and Reproductive Sciences, Yale University School of Medicine, New Haven, CT 06520, <sup>3</sup>Section of Comparative Medicine, Yale University School of Medicine, New Haven, CT 06520, <sup>4</sup>Environment and Human Health, New Haven, CT.

**Neurobehavioral disorders are increasingly prevalent in children, however their etiology is not well understood. An association between prenatal cellular telephone use and hyperactivity in children has been postulated, yet the direct effects of radiofrequency radiation exposure on neurodevelopment remain unknown. Here we used a mouse model to demonstrate that in-utero radiofrequency exposure from cellular telephones does affect adult behavior. Mice exposed in-utero were hyperactive and had impaired memory as determined using the object recognition, light/dark box and step-down assays. Whole cell patch clamp recordings of miniature excitatory postsynaptic currents (mEPSCs) revealed that these behavioral changes were due to altered neuronal developmental programming. Exposed mice had dose-responsive impaired glutamatergic synaptic transmission onto layer V pyramidal neurons of the prefrontal cortex. We present the first experimental evidence of neuropathology due to in-utero cellular telephone radiation. Further experiments are needed in humans or non-human primates to determine the risk of exposure during pregnancy.**

To date, 3–7% of school-aged children suffer from attention deficit hyperactivity disorder (ADHD)<sup>1</sup>. Children diagnosed with ADHD are at greater risk for low academic achievement, poor school performance, and delinquent behavior inconsistent with their developmental level<sup>2,3</sup>. The diagnosis of ADHD has increased at an average rate of 3% per year since 1997, making the condition a growing public health concern<sup>1</sup>. The behavioral problems in ADHD have been associated with neuropathology localized primarily to the prefrontal cortex. Children with ADHD have a reduction in prefrontal cortex volume, a reduction in gray and white matter, and asymmetry<sup>4,5</sup>. These children also have a deficit in working memory associated with inattention and controlled by activity of neurons in the prefrontal cortex<sup>6</sup>. A recent study showed that poor attention and low working memory capacity may be due to the inability to override the involuntary capture of attention by irrelevant information<sup>7</sup>. This too is controlled by the prefrontal cortex, as the shifting of one's attention voluntarily is driven by "top-down" signals in the prefrontal cortex while the involuntary capture of attention depends on "bottom-up" signals from both subcortical structures and the visual cortex<sup>7</sup>.

The etiology of ADHD remains unknown and growing evidence suggests that it is not solely due to genetic factors<sup>8</sup>. Risk factors include family psychiatric history, socioeconomic status, gender, and smoking during pregnancy<sup>9,10</sup>. A recent epidemiologic study found an association between prenatal cellular telephone exposure and subsequent behavioral problems in the exposed offspring<sup>11</sup>. This association is important given the increasing number of cellular phone users worldwide, reaching approximately four billion as of December 2008<sup>12</sup>. However, evidence of direct causation is lacking.

The specific absorption rate (SAR) is a measure of tissue radiation exposure. The European Union has set a SAR limit of 2.0 W/kg and in the United States this limit is set at 1.6 W/kg<sup>13</sup>. The *in-utero* effects of radiation exposure



within this SAR limit on neurodevelopment remain unknown. To determine if prenatal exposure to radiofrequency radiation leads to impaired memory or behavior after birth, we performed behavioral and electrophysiological studies in mice exposed *in-utero* to 800–1900 Mhz radiofrequency radiation from cellular telephones.

## Results

In order to determine if *in-utero* cell phone radiation exposure affects behavior we chose to conduct a battery of tests that identify impairments in memory, hyperactivity, anxiety, and fear, which are often associated with ADHD. Thirty-three female mice were exposed throughout gestation (days 1–17) to radiation from muted and silenced 800–1900 Mhz cellular phones with a SAR of 1.6 W/kg. The phones were positioned above each cage over the feeding bottle area at a distance of 4.5–22.3 cm from each mouse, depending on the location of the animal within the cage, and placed on an uninterrupted active call for the duration of the trial. A control group of forty-two female mice was kept concurrently under the same conditions, however using a deactivated phone. Parturition was not different between groups and occurred at 19 days  $\pm$  1 day. In order to evaluate memory in the exposed and unexposed mice, 161 progeny were given a standard object recognition memory test in three different cohorts at 8, 12, and 16 weeks of age (82 experimental and 79 control mice). The mice were allowed to explore two identical objects for 15 minutes per day for two days and on the third day one object was replaced with a novel object. On day 3 the mice were filmed for 5 minutes exploring the novel and familiar objects. Three observers, blinded to the treatment, viewed the footage and recorded the exploration time for the novel and familiar objects. The preference index was defined as the time spent exploring the new object divided by the time spent exploring both the new and old object, multiplied by one hundred. A decrease in preference index indicates diminished memory. The preference index of the experimental group at 8, 12, and 16 weeks was less than the control and the results were significant at each time point [Figure 1]. The mean preference index in the exposed group was 56.8, 69.4 and 63.5 compared to 66.5, 71.7, and 71.2 in the control group at 8, 12 and 16 weeks, respectively. The experimental group had a cumulative mean preference index of 63.0% and the control group 69.9% ( $p = 0.003$ ,  $n = 161$ ,  $t$  test). Compared to the control group, the exposed mice had a significantly lower mean preference index suggesting impairment in memory [Figure 1]. In order to ensure that our findings are in fact due to memory deficits and not distractibility or hyperactivity we calculated the percent time spent idle - not exploring either of the objects. The mean idle time in the exposed group was 90.06, 90.53, and 96.48 compared to 92.12, 91.89, and 97.07 in the control group at 8, 12 and 16 weeks, respectively. The control group had a cumulative mean idle time of 90.8% while the experimental group had a cumulative mean idle time of 90.4% and the difference between the two groups was not statistically significant ( $p = .58$ ).

To explore fearful behavior we performed the light/dark box test measuring hyperactivity/anxiety and the step down assay assessing fear of exploring the environment. The light/dark box test measures anxiety using a rodent's natural aversion to bright light<sup>14</sup>. The box contained two compartments: one white compartment that was illuminated and one black compartment that remained dark. The number of transitions between the two compartments was used to determine locomotion and in turn hyperactivity<sup>15</sup>. Anxious behavior is measured by recording the time spent in each compartment<sup>15</sup>. A total of 141 progeny were given the light/dark box test in three different cohorts at 12, 15, and 18 weeks of age (71 experimental and 70 control mice). Each mouse was placed in the light/dark box for 5 minutes and filmed. Three observers, blinded to the treatment regimen, viewed the footage and recorded the time spent in the dark compartment along with the number of transitions between each compartment. The

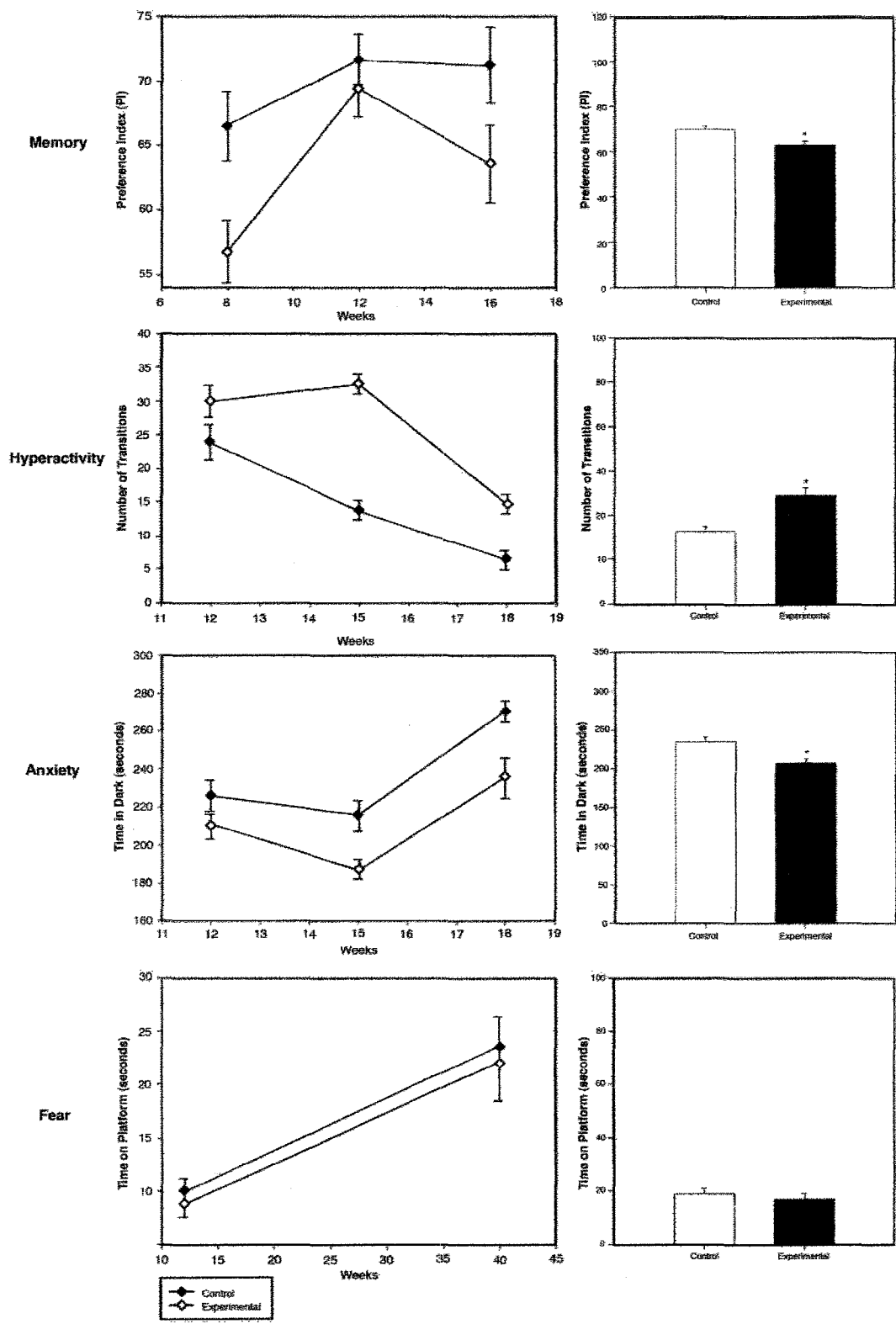
average number of transitions in the experimental group at 12, 15, and 18 weeks was fewer than in respective controls and the results were significant at each time point [Figure 1]. The average number of transitions in exposed mice was 29.9, 32.5 and 14.8 compared to 23.9, 13.8, and 6.5 in the control group at 12, 15 and 18 weeks, respectively. The experimental group showed a cumulative mean of 24.4 transitions and the control group showed a mean of 16.4 transitions ( $p < 0.001$ ). Compared to the control group, the greater number of transitions between the two compartments in the experimental group suggested hyperactive behavior [Figure 1].

To identify whether anxiety might be a factor contributing to the behavioral phenotype reported in the light/dark box experiment, we first compared the duration of time in the dark versus the time spent in the light. An increased time in the dark indicates anxious behavior<sup>15</sup>. At 12, 15, and 18 weeks the experimental group spent less time in the dark and the results were significant at each time point [Figure 1]. The duration of time in darkness of the exposed group was 210.8, 187.0 and 235.8 seconds compared to 225.6, 215.5 and 270.6 seconds in the control group at 12, 15 and 18 weeks, respectively. The mice exposed *in utero* spent a cumulative average of 207 seconds in the dark while the control mice spent an average of 234 seconds in the dark indicating decreased anxiety in the cellular phone exposed mice ( $p < 0.001$ ) [Figure 1].

The Step Down Assay was performed on 98 mice at 12 weeks and in adulthood to determine fear of exploring the environment (51 control and 47 experimental mice). The test is performed by recording the time spent on a standard platform. A greater period of time on the platform indicates increased fearfulness. Exposed mice showed no significant difference in time spent on the platform when compared to the controls [Figure 1]. The control mice spent an average of 18.5 seconds while the experimental group spent an average of 16.7 seconds ( $p = 0.59$ ) [Figure 1].

Overall, the mice exposed *in-utero* to radiation were hyperactive, had decreased memory, and decreased anxiety.

To understand the mechanisms underlying the changes in the memory and hyperactivity in animals exposed to radiation *in-utero*, we examined whether changes in the neuronal circuitry occurred in brain areas responsible for these compromised behaviors. Specifically, we asked whether changes in the synaptic transmission in CNS neurons are responsible for impaired memory and hyperactivity in radiation-exposed animals. The prefrontal cortex (PFC) is responsible for executive functions by screening distractions and maintaining attention in goal-oriented behaviors. Impairment of the PFC leads to dysregulated behavior/emotion such as ADHD<sup>16</sup>. The pyramidal neurons, the primary cell type in this structure, regulate attention and behavior through a complex and interconnected network. Whole cell patch clamp recordings of miniature excitatory postsynaptic currents (mEPSCs) were performed in pyramidal neurons of the PFC in control and cell phone-exposed mice. mEPSCs were generated by random vesicle release of glutamate from presynaptic neurons in the absence of stimulation. The measurement of mEPSCs is used to analyze the efficacy of synaptic transmission. Changes in mEPSC frequency are thought to result from modification of the presynaptic component of synaptic transmission, while amplitude changes indicate alterations in the postsynaptic component<sup>17,18</sup>. Coronal prefrontal cortex slices (300  $\mu$ m) were prepared from 3–4 week old mice. mEPSCs were recorded in layer V pyramidal neurons in the prefrontal cortex in mice exposed to *in-utero* radiation for 9, 15 and 24 hours/day throughout gestation; the detection and analysis of mEPSC frequency and amplitude were performed as we described previously<sup>18</sup>. In animals exposed to *in-utero* radiation for 24 hours/day, a decrease in the frequency of mEPSCs was seen (control:  $1.00 \pm 0.12$  Hz,  $n = 40$ ; 24 hours/day:  $0.72 \pm 0.06$  Hz,  $n = 43$ ,  $p < 0.05$ ,  $t$  test, Figure 2A and B). The cumulative probability curves for the amplitude of mEPSC events recorded from the *in utero* cell phone-exposed mice (24 hours/day) shifted

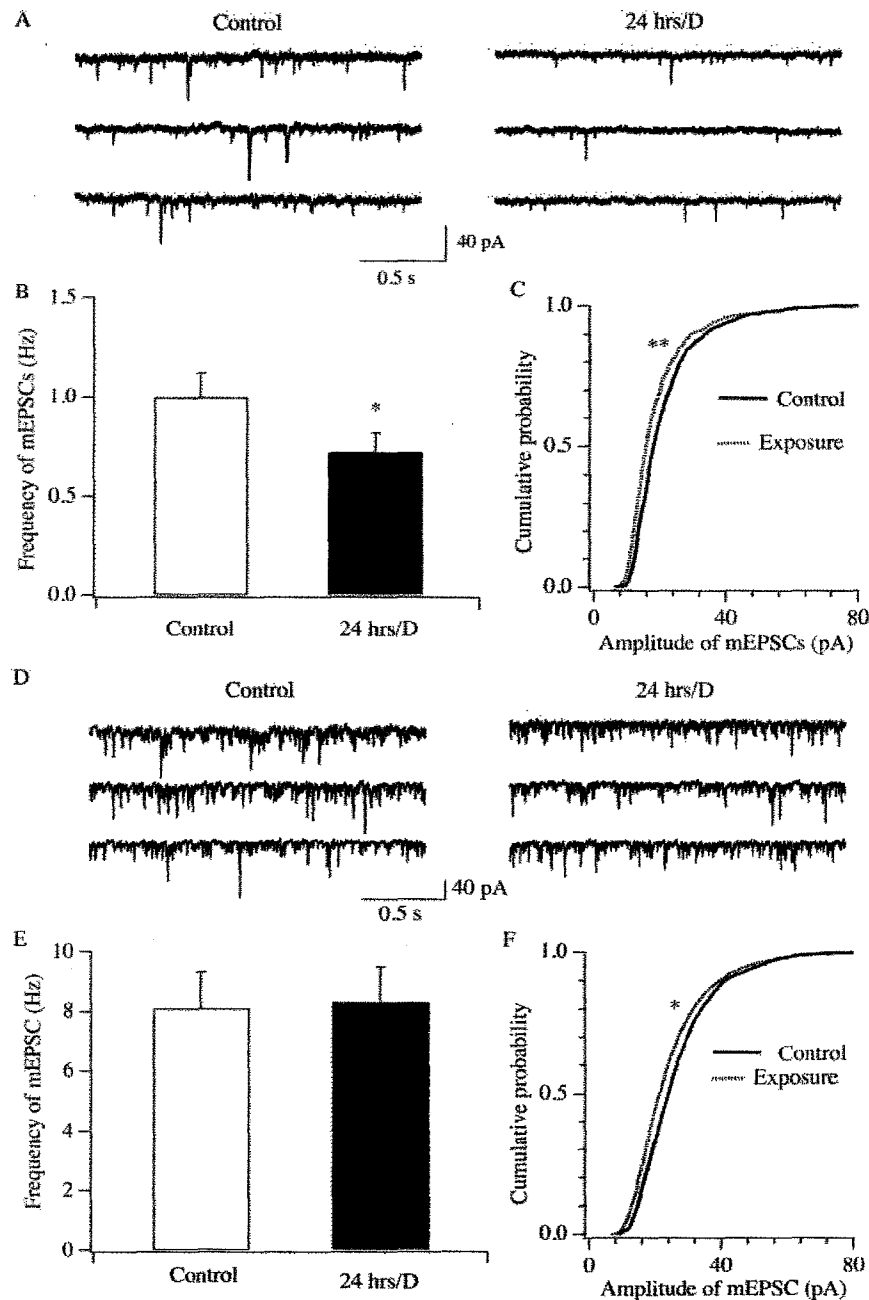


**Figure 1 | Behavioral testing in exposed and control mice.** The left column displays the data determined in mice at several ages after exposure. The right column demonstrates the cumulative average. To test memory the Standard object recognition memory test was used and a Preference Index (percent of total exploration time spent exploring the new object) shown at 8, 12, and 16 weeks of age. The cumulative mean preference index of the experimental group was 63.0% and the control group 69.9% (\* $p = 0.003$ ,  $n = 161$ ). To test hyperactivity we used the Light/Dark box test and display transitions at 12, 15, and 18 weeks of age. The cumulative mean number of transitions in the experimental group was 24.4 and the control group 16.4 (\* $p < 0.001$ ,  $n = 141$ ). To test anxiety we measured time spent in the dark at 12, 15, and 18 weeks of age. The cumulative average time spent in the dark in the experimental group was 207 seconds and in the control was 234 seconds (\* $p < 0.001$ ,  $n = 141$ ). To measure fear we used the Step down assay and display the time spent on the platform at 12 weeks and adulthood. The cumulative mean time spent on the platform in the experimental group was 16.7 seconds and in the control was 18.5 seconds ( $p = 0.59$ ,  $n = 98$ ).

significantly to the left relative to those recorded from the controls ( $P < 0.01$ , Kolmogorov-Smirnov test; control: 2765 events, cell phone exposure: 2224 events), indicating that the amplitude of mEPSCs was decreased [Figure 2C]. In a subset of experiments, we examined whether the reduction of mEPSC frequency depended on dosages of exposure in mice prenatally exposed 0, 9, 15 and 24 hours per day [Figure 3]. The trend of the dose-dependent decrease in the frequency of mEPSCs (0 hour/day:  $1.37 \pm 0.41$ ,  $n = 9$ ; 9 hours/day:  $1.27 \pm 0.21$  Hz,  $n = 9$ ; 15 hours/day:  $1.04 \pm 0.20$  Hz,  $n = 10$ ; 24 hours/day:  $0.72 \pm 0.13$ ,  $n = 11$ ) was statistically significant (linear correlation: Correlation Coef =  $-0.97$ , Unadjusted  $r^2 = 0.94$ ,  $P < 0.05$ ).

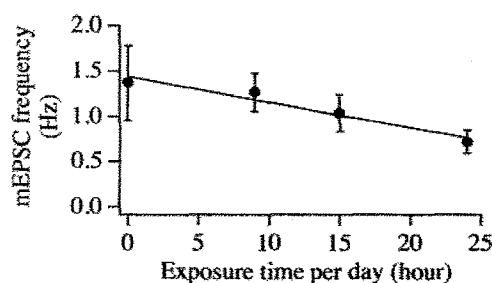
Altogether, these results indicate that synaptic efficacy of glutamatergic transmission decreases at both pre- and postsynaptic sites in layer V pyramidal neurons. Thus, we demonstrate impairment in glutamatergic transmission (release from nerve terminals and glutamate receptor response) onto pyramidal neurons in the PFC after *in-utero* exposure to radiation from cellular telephones.

In a parallel experiment we examined whether *in-utero* radiation exposure led to changes in synaptic transmission in another brain area. mEPSCs were recorded in neurons in the ventral medial hypothalamus (VMH), a brain area implicated in the regulation of energy homeostasis<sup>19,20</sup>. Our results indicated that in mice exposed to radiation for 24 hours/day, the frequency of mEPSCs (control:



**Figure 2 | Synaptic efficacy of glutamatergic synapses is decreased in brain neurons of mice after prenatal exposure to cell phone radiation.** A–C, mEPSCs were recorded in layer V pyramidal neurons of the prefrontal cortex. Representative traces of mEPSCs from control and cell phone exposure groups are shown in A. mEPSC frequency and cumulative probability of mEPSC amplitude from both groups are shown in B (\*,  $P < 0.05$ , t test) and C (\*\*,  $P < 0.01$ , Kolmogorov-Smirnov test; controls, 2225 events; Exposed, 2766 events). D–F, representative traces, frequency and amplitude of mEPSCs recorded in neurons in the VMH are shown. \*,  $P < 0.05$ , Kolmogorov-Smirnov test; Control: 2161 events, Cell phone group: 2261 events.





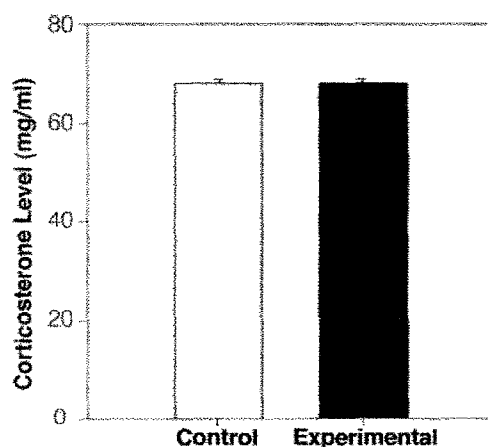
**Figure 3** | A dose-dependent attenuation in the frequency of mEPSCs in layer V pyramidal neurons in mice. The frequency of mEPSCs recorded in mice prenatally exposed to cell phone radiation at of dose of 0, 9, 15 and 24 hrs per day are shown. Error bars are SEM. The dose responsive relationship is determined using regression analysis (Correlation coefficient,  $-0.97$ ;  $r^2$ ,  $0.94$ ;  $P < 0.05$ ).

$8.13 \pm 1.20$  Hz,  $n = 14$ ; cell phone radiation:  $8.32 \pm 1.17$  Hz,  $n = 14$ ) was not significantly different from that in control mice ( $P > 0.05$ ,  $t$  test, Figure 2D and E). However, the cumulative probability of mEPSC amplitude recorded in radiation-exposed mice significantly shifted to the left ( $P < 0.05$ , Kolmogorov-Smirnov test; control: 2161 events, cell phone group: 2261 events; Figure 2F), suggesting that the amplitude of mEPSCs is smaller in the cell-phone exposed group than in controls. This result implies that an impairment of glutamatergic transmission occurs at the postsynaptic site. In summary, our results suggest that the effects of prenatal exposure to the cell phone radiation were not limited to the cortex.

Maternal stress can alter fetal development by increasing offspring exposure to corticosterone, causing cognitive deficits, hyperactivity, and alterations of the hypothalamo-pituitary-adrenal axis<sup>21</sup>. In order to exclude the possibility that impaired memory and behavior in exposed mice was caused by stress resulting from experimental manipulation, we measured serum corticosterone levels on day twelve of gestation using an ELISA assay. The mean corticosterone level in the exposed female mice ( $69.91$  ng/ml,  $n = 6$ ) was not significantly different from that in the control females ( $69.94$  ng/ml,  $n = 6$ ) [Figure 4], eliminating stress as a source of the observed behavioral and electrophysiological differences.

## Discussion

Here we demonstrate that fetal exposure to 800–1900 Mhz-rated radiofrequency radiation from cellular telephones leads to behavioral and neurophysiological alterations that persist into adulthood. Mice



**Figure 4** | Corticosterone levels during pregnancy were unaltered by exposure. The mean corticosterone level in the pregnant control females was  $69.94$  ng/ml and in the exposed female mice was  $69.91$  ng/ml.

exposed during pregnancy had impaired memory, were hyperactive, and had decreased anxiety, indicating that *in-utero* exposure to radiofrequency is a potential cause of neurobehavioral disorders. We further demonstrated impairment of glutamatergic synaptic transmission onto pyramidal cells in the prefrontal cortex associated with these behavioral changes, suggesting a mechanism by which *in-utero* cellular telephone radiation exposure may lead to the increased prevalence of neurobehavioral disorders.

This is the first study to specifically identify effects of radio-frequency exposure on the mouse fetus. During critical windows in neurogenesis the brain is susceptible to numerous environmental insults; common medically relevant exposures include ionizing radiation, alcohol, tobacco, drugs and stress. The effects of these agents are dependent on dose and timing of exposure. Even small exposures during periods of neurogenesis have a more profound effect than exposure as an adult. Alcohol affects cerebral neurogenesis, patterning of brain development and subsequent behavior. Maternal smoking also affects fetal development; fetal tobacco exposure results in a higher incidence of behavioral and cognitive impairment including ADHD. Similarly, prenatal exposure to cocaine can lead to behavioral disorders. Even prenatal maternal stress can lower intelligence and language abilities in offspring. As demonstrated by these examples, environmental exposures occurring in fetal life can lead to persistent neurological deficits. Exposure to these insults as an adult does not carry the same consequences. It is therefore not surprising that studies exposing adult animals to radiofrequency radiation failed to find similar significant defects in behavior. The exposure to cellular telephones in pregnancy may have a comparable effect on the fetus and similar implications for society as do exposures to other common neurodevelopmental toxicants. While this data demonstrates a clear association between fetal EMR exposure and neurodevelopment, it is important to recognize that the extrapolation of this animal model to humans is limited; the exposures used here are not identical to those experienced by the human fetus.

The molecular and cellular effects of radiofrequency exposure are not yet fully characterized. Multiple targets have been identified *in vitro*. Electromagnetic frequency exposure has been demonstrated to affect cell division and proliferation, both by inducing apoptosis and altering the cell cycle<sup>22</sup>. Electromagnetic radiation may promote the formation of reactive oxygen species (ROS) causing cell damage<sup>23</sup>. One study specifically analyzing the effects of radiofrequency radiation on glioma cells demonstrated altered oxidative stress, a potential mediator of the alterations caused by electromagnetic radiation<sup>24</sup>. Electromagnetic frequency radiation has also been found to activate ERK and p38 MAPK signaling<sup>25</sup>. Although the precise molecular mechanisms that led to altered glutamatergic synaptic transmission in the prefrontal cortex identified in this study are not yet fully known, here we provide the first evidence that links changes in neuronal circuitry centered on layer V pyramidal neurons in the PFC with impaired memory and cognitive behaviors in animals exposed to radiation from cellular phone use. Our results indicate that the release of glutamate from the nerve terminals on PFC neurons and response of PFC neurons to glutamate are impaired in mice prenatally exposed to cell phone radiation. These results are consistent with previous reports that compromised glutamatergic transmission onto PFC neurons underlies impaired memory and cognitive functions in animals<sup>26,27</sup>. Our results also imply that the effects of prenatal exposure to radiation on the brain might be global, since glutamatergic transmission onto neurons in another area of the brain (i.e., the VMH) was decreased as well. The effects of prenatal exposure to cell phone radiation may have more profound effects on brain functions than reported in this study. However, the effect was not identical; there are likely to be cell type specific or regional variations in susceptibility. Alternatively, the depth of the VMH may have shielded this region from maximal exposure.

Given the recent advancements in the technology of cellular telephones (i.e. smart phones), they are now used in a capacity beyond that of a basic telephone. For many, cellular telephones are used as a bedside alarm clock and personal organizer. Cellular telephone usage can reach 24 hours/day, leaving users increasingly exposed to the potentially harmful effects of radiofrequency radiation exposure. Our findings indicated significant electrophysiological and behavioral changes in mice exposed *in-utero* to radiation. The significant trend between the groups treated for 0, 9, 15, and 24 hours/day demonstrates that the effects are directly proportional to usage time, and suggests that safety limits, particularly for pregnant women, can be established. Though it is difficult to translate these findings to human risks and vulnerability, we identify a novel potential contribution to the increased prevalence in hyperactive children, one that is easily prevented. However, it is important to note that hyperactivity and anxiety are closely related and my confound one another.

In this study we used cellular telephones as a source of EMR to mimic human exposure. However there are several limitations to this study that include lack of a defined exposure from a traditional EMF generator. Further we did not measure the level of exposure and the distance to the source was not fixed; mice were free to move within the confines of the cage. Power density measurements with respect to orientation, polarization, reflection, and interference were not considered. In order to determine the maximal effects and potential risks associated with exposure, the mice were exposed from conception to birth, however mouse brain development is incomplete at birth and distinct from that of humans. While neurological effects were found here, future studies should focus on a more narrow gestational age of exposure, use EMF generators to more precisely define exposure, and limit variation in the distance from the source. Definitive studies in humans are required prior to extrapolating these behavioral findings to humans.

In summary, we demonstrate that fetal radiofrequency radiation exposure led to neurobehavioral disorders in mice. We anticipate these findings will improve our understanding of the etiology of neurobehavioral disorders. The rise in behavioral disorders in developed countries may be, at least in part, due to a contribution from fetal cellular telephone radiation exposure. Further testing is warranted in humans and non-human primates to determine if the risks are similar and to establish safe exposure limits during pregnancy.

## Methods

**Exposure and Behavioral Tests.** Over five separate experiments, a total of 27 breeding cages were set-up each containing 3 CD-1 female mice and 1 CD-1 male mouse (13 experimental cages and 14 control cages). Each experimental cage was equipped with a muted and silenced 800–1900 Mhz cellular phone with a SAR of 1.6 W/kg placed over the feeding bottle area at a distance of 4.5–22.3 cm from the mice. The cellular phones were then placed on an active call for 24 hours per day and the 33 experimental female mice were exposed throughout gestation (days 1–17). An additional six females were exposed to an active phone for either 9 or 15 hours per day. Each control cage was equipped with a deactivated phone and was kept under the same conditions. To assure equal exposure time independent of the variable length of gestation (18–20 days), at the end of day 17 all phones were removed. On day 18 all female mice were separated and placed in their own cage yielding a total of 39 exposed pregnant females and 42 unexposed pregnant females. Throughout the experiment, both the control and experimental mice were fed and given water *ad libitum*. The mice were maintained on a 12 hour light/dark cycle (07:00 on) and all procedures were approved by the Yale University Animal Care and Use Committee.

Memory was evaluated using a standard object recognition memory test. A total of 161 pups were tested (82 experimental mice and 79 control mice) at 8, 12, and 16 weeks. The test consisted of two learning days (Day 1 and 2) and one test day (Day 3). On Day 1 four opaque exploration chambers were set-up in the exam room at a luminosity of 420–440 Lux. Prior to conducting each test, the mice were placed in the testing room and allowed 1 hour to acclimate to the light. Two identical objects were then placed in each of the four chambers and a single mouse was placed in each chamber to explore the two identical objects for 15 minutes. Before repeating the experiment, the objects and the chambers were cleaned thoroughly with a detergent solution to remove any scents or odors. On Day 3 a video camera was placed over all 4 chambers and the objects were rearranged so that each chamber had one familiar object and one novel object. The mice were then allowed to explore both objects and were filmed for 5 minutes. Upon completing the experiment, 3 observers, blinded to

the treatment regimen, viewed the first 2 minutes of footage to determine the time spent exploring the novel object. Exploration of the new object was defined as sniffing at less than 1 cm. A preference index was then calculated by dividing the time spent exploring the new object by the total exploration time multiplied by one hundred. The percent time spent idle - not exploring either of the objects was also calculated in order to ensure that our findings are in fact due to memory deficits and not distractibility or hyperactivity.

The light-dark box test was conducted using a light-dark box, constructed of black and white Plexiglass (45×27×27 cm). The dark compartment (18×27 cm) was made of black Plexiglass with a black Plexiglass cover and the light compartment (27×27 cm) was made of white Plexiglass and remained open. The light compartment was kept at a luminosity of 420–440 Lux. An opening (7.5×7.5 cm) was located in the wall between the two chambers allowing free access between the light and dark compartments. A video camera was then placed over the box for filming. Prior to conducting each test, the mice were placed in the testing room and allowed 1 hour to acclimate to the light. A single mouse was then placed in the light chamber and was allowed to explore the box for 5 minutes while being filmed. Before repeating the experiment, the chambers were cleaned thoroughly with a detergent solution to remove any scents or odors. Three observers, blinded to the treatment regimen, then viewed the footage and recorded the total time spent in the dark as well as the total number of transitions. This data was then interpreted as described in the text to analyze anxiety and hyperactivity.

The Step Down Assay was performed to determine fearful behavior by placing a mouse gently on a platform (96 well plate) and recording the time on the platform. The timer was stopped once the mouse stepped off the platform with all four paws. Before repeating the experiment, the platform was cleaned thoroughly with a detergent solution to remove any scents or odors.

**Corticosterone Measurement.** Gestational stress was analyzed by collecting serum on Day 12 of gestation from 6 exposed and 6 unexposed pregnant females. Serum samples were tested for corticosterone levels using an enzyme immunoassay kit (Assay Designs, Ann Arbor, MI) as recommended by the manufacturer.

**Electrophysiology.** Mice from control and cell phone-exposed groups were anesthetized with ether and then decapitated. The brains were rapidly removed and immersed in an oxygenated cutting solution at 4°C containing (in mM): sucrose 220, KCl 2.5, CaCl<sub>2</sub> 1, MgCl<sub>2</sub> 6, NaH<sub>2</sub>PO<sub>4</sub> 1.25, NaHCO<sub>3</sub> 26, and glucose 10, and adjusted to pH 7.3 with NaOH. Coronal cortical slices (300 μm thick) were prepared from the prefrontal area of the brain and the ventral medial hypothalamus (VMH) using a vibratome. After preparation, slices were maintained in a holding chamber with artificial cerebrospinal fluid (ACSF) (bubbled with 5% CO<sub>2</sub> and 95% O<sub>2</sub>) containing (in mM): NaCl 124, KCl 3, CaCl<sub>2</sub> 2, MgCl<sub>2</sub> 2, NaH<sub>2</sub>PO<sub>4</sub> 1.23, NaHCO<sub>3</sub> 26, glucose 10, pH 7.4 with NaOH, and were transferred to a recording chamber constantly perfused with bath solution (33°C) at 2 ml/min after at least a 1 hr recovery.

Whole-cell voltage clamp (at –60 mV) was performed to observe miniature excitatory postsynaptic currents (mEPSCs) in layer V cortical neurons with a Multiclamp 700 A amplifier (Molecular devices, CA). The patch pipettes (tip resistance = 4–6 MΩ) were made of borosilicate glass (World Precision Instruments) with a pipette puller (Sutter P-97) and back filled with a pipette solution containing (in mM): K-gluconate 135, MgCl<sub>2</sub> 2, HEPES 10, EGTA 1.1, Mg-ATP 2, Na<sub>2</sub>-phosphocreatine 10, and Na<sub>2</sub>-GTP 0.3, pH 7.3 with KOH. mEPSCs were recorded in pyramidal neurons under voltage clamp (at –60 mV) in the presence of tetrodotoxin (TTX, 0.5 μM) and a GABA-A receptor antagonist picrotoxin (50 μM). Both input resistance and series resistance were monitored constantly during experiments. The series resistance (between 20 and 40 MΩ) was partially compensated by the amplifier and only recordings with stable series and input resistance throughout experiments were accepted. All data were sampled at 3–10 kHz and filtered at 1–3 kHz with an Apple Macintosh computer using Axograph X (AxoGraph Scientific). mEPSC events were detected and analyzed with AxoGraph X and plotted with Igor Pro software (WaveMetrics, Lake Oswego, OR) as described previously by Rao, et al (2007). Linear correlation was performed with the software GB-STAT (Dynamic Microsystems, Inc, Silver Spring, MD).

1. American Psychiatric Association: *Diagnostic and Statistical Manual of Mental Disorders* (2000) Fourth Edition, Text Revision. Washington, DC, American Psychiatric Association.
2. Barkley, R. Behavioral Inhibition, Sustained Attention, and Executive Functions: Constructing a Unifying Theory of ADHD. *Psychol Bull* 121, 65–94 (1997).
3. Rappley, M. Attention deficit-hyperactivity disorder. *N Engl J Med* 352, 165–73 (2005).
4. Sowell, E. R. Cortical abnormalities in children and adolescent with attention-deficit hyperactivity disorder. *Lancet* 362, 1699–707 (2003).
5. Castellanos, F. X. Development trajectories of brain volume abnormalities in children and adolescents with attention-deficit/hyperactivity disorder. *JAMA* 288, 1740–48 (2002).
6. Castellanos, F. X. & Tannock, R. Neuroscience of attention deficit/hyperactivity disorder: the search for endophenotypes. *Nat Rev Neurosci* 3, 617–28 (2002).
7. Fukuda, K. & Vogel, E. K. Human variation in overriding attentional capture. *J Neurosci* 29, 8726–33 (2009).
8. Singh, I. Beyond polemics: science and ethics of ADHD. *Nat Rev Neurosci* 9, 957–64 (2008).



9. Brasset-Harknett, A. & Butler, N. Attention-deficit/hyperactivity disorder: an overview of the etiology and a review of the literature relating to the correlates and lifecourse outcomes for men and women. *Clin Psychol Rev.* **27**, 188–210 (2007).
10. Biederman, J. & Faraone, S. V. Attention-deficit hyperactivity disorder. *Lancet* **366**, 237–248 (2005).
11. Divan, H., Kheifets, L., Obel, C. & Olsen, J. Prenatal and postnatal exposure to cell phone use and behavioral problems in children. *Epidemiology* **19**, 523–529 (2008).
12. Measuring the Information Society: The ICT Development Index. International Telecommunication Union. p108. (2009).
13. Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz). International Commission on Non-Ionizing Radiation Protection. *Health Phys.* **74**, 494–522 (1998).
14. Bourin, M. & Hascoet, M. The mouse light/dark box test. *Eur J Pharmacol.* **463**, 55–65 (2003).
15. Corbetta, S. *et al.* Hyperactivity and novelty-induced hyperactivity in mice lacking Rac3. *Behav Brain Res* **186**, 246–255 (2008).
16. Arnsten, A. F. Stress signalling pathways that impair prefrontal cortex structure and function. *Nat Rev Neurosci* **10**, 410–22 (2009).
17. Ungless, M. A., Whistler, J. L., Malenka, R. C. *et al.* Single cocaine exposure in vivo induces long-term potentiation in dopamine neurons. *Nature.* **411**, 583–587 (2001).
18. Rao, Y. *et al.* Prolonged wakefulness induces experience-dependent synaptic plasticity in mouse hypocretin/orexin neurons. *J Clin Invest.* **117**, 4022–33 (2007).
19. López, M. *et al.* Hypothalamic AMPK and fatty acid metabolism mediate thyroid regulation of energy balance. *Nat Med.* **16**, 1001–8 (2010).
20. Xu, Y. *et al.* PI3K signaling in the ventromedial hypothalamic nucleus is required for normal energy homeostasis. *Cell Metab.* **12**, 88–95 (2010).
21. Koehl, M., Lemaire, V., Le Moal, M. & Abrous, D. N. Age-dependent effect of prenatal stress on hippocampal cell proliferation in female rats. *Eur J Neurosci.* **29**, 635–40 (2009).
22. Panagopoulos, D. J., Chavdoula, E. D., Nezis, I. P. & Margaritis, L. H. Cell death induced by GSM 900-MHz and DCS 1800-MHz mobile telephony radiation. *Mutat Res.* **626**, 69–78 (2007).
23. Zmyslony, M. *et al.* Acute exposure to 930 MHz CW electromagnetic radiation in vitro affects reactive oxygen species level in rat lymphocytes treated by iron ions. *Bioelectromagnetics.* **25**, 324–8 (2004).
24. Cao, Y. *et al.* 900-MHz microwave radiation enhances gamma-ray adverse effects on SHG44 cells. *J Toxicol Environ Health A.* **72**, 727–32 (2009).
25. French, P. W., Penny, R., Laurence, J. A. & McKenzie, D. R. Mobile phones, heat shock proteins and cancer. *Differentiation* **67**, 93–97 (2001).
26. Jentsch, J. D. *et al.* Dysbindin modulates prefrontal cortical glutamatergic circuits and working memory function in mice. *Neuropsychopharmacology.* **34**, 2601–8 (2009).
27. Rubino, T. *et al.* The depressive phenotype induced in adult female rats by adolescent exposure to THC is associated with cognitive impairment and altered neuroplasticity in the prefrontal cortex. *Neurotox Res.* **15**, 291–302 (2009).

## Acknowledgements

The authors thank Arie Kaffman and Richard Hochberg for critical reading of the manuscript and thank Neil Odem, Michael Lee and Yuzhe Feng for their technical assistance and analysis of behavioral test results. Supported by grants from EHHI and NICHD (HD052668).

## Author contributions

TSA treated the mice, performed the behavioral studies, analyzed the data and wrote the manuscript. GG and XBG performed and analyzed the electrophysiology studies. HST designed the experiment, analyzed the data and edited the manuscript.

## Additional information

**Competing financial interests:** The authors declare no competing financial interests.

**License:** This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivative Works 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/>

**How to cite this article:** Aldad, T.S., Gan, G., Gao, X. & Taylor, H.S. Fetal Radiofrequency Radiation Exposure From 800-1900 Mhz-Rated Cellular Telephones Affects Neurodevelopment and Behavior in Mice. *Sci. Rep.* **2**, 312; DOI:10.1038/srep00312 (2012).