THE SMART GRID: THE COMPLEXITIES AND IMPORTANCE OF DATA PRIVACY AND SECURITY

H. Russell Frisby, Jr.[†] & Jonathan P. Trotta[‡]

I. INTRODUCTION

Over the last several years, the nation has become fixated by the wide range of possibilities afforded by what has become known as the Smart Grid. In concept, the Smart Grid has the potential not only to significantly improve the reliability of the electric grid, but also to change the way electric utilities interact with their customers. Smart Grid technologies can aid in combating climate change by promoting energy independence, and by helping to improve electric system reliability and efficiency. The Smart Grid has also been envisioned as a means to spur technological innovation, encourage broadband deployment, and serve as a catalyst for economic development.[1] The Smart Grid, which will

[†] Yale Law School, J.D. 1975. Mr. Frisby is a Partner in the Energy and Telecommunications Group at Stinson Morrison Hecker LLP. He is the former Chairman of the Maryland Public Service Commission and is past President of the Competitive Telecommunications Association. Mr. Frisby is also a member of the Administrative Conference of the United States.

[‡] Suffolk University Law School, J.D. 2007. Mr. Trotta is an attorney in the Energy and Telecommunications Group at Stinson Morrison Hecker LLP. Previously, he was an attorney-advisor with the Federal Energy Regulatory Commission.

[1] The promise of the Smart Grid is enormous and includes improved reliability, flexibility and power quality, reduction in peak demand, reduction in transmission congestion costs, environmental benefits gained by increased asset utilization, increased security, increased energy efficiency, and increased durability and ease of repair in response to attacks or natural disasters. *See* Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy, DOE Request for Information, 75 Fed. Reg. 26203 (July 12, 2010) [hereinafter DOE Data Access RFI]. *See also* FED. COMMC'NS COMM'N, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 265 (2010), *available at* http://www.broadband.gov/download-plan [hereinafter NATIONAL BROADBAND PLAN].

cost billions of dollars to build,[2] represents the long-awaited convergence of energy and telecommunications in technology and policy.[3] In our Smart Grid future, companies such as Google may play as important a role in providing energy services as traditional electric utilities do today.[4] Consequently, The American Recovery and Reinvestment Act of 2009 devoted 4.5 billion dollars to accelerating standardization and deployment of the Smart Grid as part of a new national policy.[5]

Once deployed and implemented, Smart Grid technologies will "introduce millions of new intelligent components" into this nation's "electric grid that communicate in much more advanced ways" than were previously possible.[6] According to Thomas Friedman, in the future world of the Smart Grid

> [i]t would feel like all the power systems in your home were communicating with all the information systems in your home and that they had all merged into one big seamless platform for using storing, generating, and even buying and selling clean electrons. It would feel like the information technology revolution and the energy technology revolution, IT and ET, had merged into a single system.[7]

Regardless of the benefits, this future world is not without its dangers. The Smart Grid will generate and permit worldwide access to an unprecedented amount of confidential, personally-identifiable customer energy usage data ("CEUD"), which could enable significant invasions of consumer privacy.[8]

---

[2] ELECTRIC POWER RES. INST. (EPRI), REPORT TO NIST ON THE SMART GRID INTEROPERABILITY STANDARDS ROADMAP 12 (Aug. 10, 2009), *available at* http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf.

[3] *See* H. Russell Frisby, Jr., *The National Broadband Plan,* ELECTRIC PERSPECTIVES, July/August 2010, at 22, *available at* http://www.stinson.com/Publications/Image_Files/Frisby_ElectricPerspectivesArticle.aspx. It is important to note that electric utilities have made extensive use of communications networks and services (both private and commercial) for over 100 years and are significant providers of wholesale telecommunications facilities. *See* UTILITIES TELECOM COUNCIL (UTC), A STUDY OF UTILITY COMMUNICATIONS NEEDS: KEY FACTORS THAT IMPACT UTILITY COMMUNICATIONS NETWORKS BY THE UTC 5 (2010) [hereinafter UTC STUDY].

[4] *See* Martin LaMonica, *Google Crashes the Smart-Grid Party*, CNET NEWS (Feb. 10, 2009, 10:13 AM), http://news.cnet.com/google-crashes-the-smart-grid-party/.

[5] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, div. A, title IV, 123 Stat. 115 (2009).

[6] ANDREAS DREHER & ERIC BYRES, BELDEN, INC.,GET SMART ABOUT ELECTRICAL GRID CYBERSECURITY 2 (2010), *available at* http://www.belden.com/pdfs/techpprs/PTD_Cyber_SecurityWP.pdf; *see also* SMART GRID INTEROPERABILITY PANEL CYBERSECURITY WORKING GROUP (SGIP), NISTIR 7628, GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 14-15 (Aug. 2010) [hereinafter NISTIR 7628 VOL. 2 PRIVACY GUIDELINES], *available at* http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf (describing how "smart appliances" will be able to communicate "directly to utilities, consumers, and other entities").

[7] THOMAS L. FRIEDMAN, HOT, FLAT, AND CROWDED: WHY WE NEED A GREEN REVOLUTION—AND HOW IT CAN RENEW AMERICA 217 (Farrar, Straus & Giroux New York 2008).

[8] DOE Data Access RFI, *supra* note 1, at 26203, 26205.

According to the Department of Energy ("DOE"),

> many of the benefits of the Smart Grid could be reduced or delayed and avoidable harms caused unless the Smart Grid adequately respects consumers' reasonable—and often widely differing—expectations of privacy, expectations that could be compromised if detailed household energy consumption data is made too readily available, too inaccessible, or incorrectly anonymized.[9]

Until recently, insufficient thought has been given to questions of controlling access to this information—and if so, how to do so—because much of this information was either never accessible or simply did not exist.

As a result, the deployment of Smart Grid technologies raises a number of complex, but extremely important, issues that policymakers must carefully consider to ensure the long-term success of the Smart Grid. The present Administration,[10] various federal agencies,[11] and a range of state regulatory bodies[12] have undertaken a close review of these issues and solicited input from a wide range of industry participants. While much of what is being studied involves technical or policy issues, the Smart Grid also implicates many regulatory issues which must be addressed. This article will provide an overview of the Smart Grid, review federal and some state efforts to date, and finally discuss a number of regulatory issues relating to Smart Grid data access, privacy and security.

II. OVERVIEW OF THE SMART GRID

A. What is the Smart Grid?

For better or worse, there is no firm definition of the "Smart Grid"–nor is there a universal understanding of the technologies and applications it encompasses. Often, the Smart Grid is described not in terms of what it is, but rather in terms of its capabilities. This ambiguity has caused a great deal of confusion, particularly among consumers and regulators.

The Smart Grid is generally understood to enable the "two-way flow of elec-

---

[9] *See id.* at 26203 ("The information provided by smart meters and other smart grid technologies is unique in both its dep't.h and breadth. If its collection and dissemination goes unchecked, such information has to [sic] potential to enable significant invasions into consumer privacy.").

[10] Office of Science and Technology Policy, Consumer Interface with the Smart Grid and OSTP Request for Public Comment, 75 Fed. Reg. 7526 (Feb. 19, 2010) [hereinafter OSTP Request].

[11] *See* NATIONAL BROADBAND PLAN, *supra* note 1, at 247 (describing efforts by the FCC, NTIA, and DOE in considering policies regarding the Smart Grid).

[12] *See* U.S. DEP'T. OF ENERGY, DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES 54-56 (Oct. 5, 2010) [hereinafter DATA ACCESS & PRIVACY REPORT] (describing legislation in California, Pennsylvania and Texas), *available at* http://www.gc.energy.gov/documents/Broadband_Report_Data_Privacy_10_5.pdf.

tricity and information to create an automated, widely distributed energy delivery network."[13] However, in real-world application, parties define the Smart Grid very differently. As the DOE has recognized, "[d]efining the Smart Grid is in itself tricky business. Select six stakeholders and you will likely get at least six definitions."[14] Rather than defining the Smart Grid, Congress has identified the Smart Grid in the context of at least ten characteristics.[15]

For its part, and perhaps to avoid the definitional quandary, DOE has stated that five fundamental technologies will drive the Smart Grid: integrated communications, sensing and measurement technologies, advance components, advanced control methods, and improved interfaces and decision support.[16] However, the DOE in its third Request for Information on Smart Grid issues, and in recognition of the great potential for confusion and miscommunication,[17] sought comment on whether using the EISA description was the best

---

[13] NATIONAL BROADBAND PLAN, *supra* note 1, at 267.

[14] U.S DEP'T. OF ENERGY, WHAT THE SMART GRID MEANS TO YOU AND THE PEOPLE YOU SERVE, (prepared by Litos Strategic Communication 2009) [hereinafter LITOS REPORT].

[15] Energy Independence and Security Act (EISA), Pub. L. No. 110-140 § 1301, 121 Stat. 1492, 1783-1784 (2007) (codified at 42 U.S.C. §§ 17001 *et seq.*). EISA § 1301 outlines the following characteristics of a Smart Grid:

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

42 U.S.C. § 17381 (Supp. I 2007-2008).

[16] DEP'T. OF ENERGY, THE SMART GRID: AN INTRODUCTION, 29 (2008), *available at* http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf.

[17] For example, as discussed below, the Smart Grid is more than just a collection of smart meters and any regulatory cost benefit analysis which solely focuses on the meters is doomed to be inadequate. *See* discussion *infra* Part II. A (defining the Smart Grid); U.S. DEP'T. OF ENERGY, THE SMART GRID: AN INTRODUCTION, 14 (2008), *available at* http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages5281%29.pd

way to define the Smart Grid.[18] In addition, the DOE correctly sought guidance on what significant policy challenges might remain unaddressed, or what risks might emerge, if the EISA definition were used.[19]

According to others, the primary components of the Smart Grid system are: intelligent home area networks ("HANs"), advanced metering infrastructure ("AMI") and smart meters, two-way communication between a customer's network and its utility, system visualization or wide area situational awareness about generation, distribution and transmission systems, and increased system controls for electricity load management.[20]

From the utility perspective, "Smart Grid" is perhaps a misnomer because the electric grid is already "smart": traditional infrastructure and technologies allow utilities to detect outages and to manage power flows. What these new features describe is an effort to develop an even "Smarter Grid."[21] While AMI and smart meters have piqued the public's attention, the earliest benefits of the Smart Grid may be realized from the deployment of technologies that will strengthen and improve transmission and distribution systems.[22] Unfortunately, this has led state regulators to question the long-term efficacy of the Smart Grid, thereby potentially delaying the implementation of much needed Smart Grid projects.[23]

Perhaps the Smart Grid is best viewed as an intelligent energy platform enabled by "communications, information and systems control technologies" that permits the integration of a wide variety of new applications into the power grid.[24]

---

f. *See also* discussion *infra* Part IV-V (emphasizing that Smart Grid regulation must account for consumer privacy, security, and control expectations).

[18] U.S. Dep't. of Energy, Addressing Policy and Logistical Challenges to Smart Grid Implementation, 75 Fed. Reg. 57006, 57008 (Sept. 17, 2010).

[19] *Id.*

[20] *See* AMERICAN PUBLIC POWER ASS'N, SMART GRID ESSENTIALS: A PUBLIC POWER PRIMER 6 (Burns & McDonnell 2009); MILES KEOGH, THE NAT'L ASS'N OF REGULATORY COMMISSIONERS, THE SMART GRID: FREQUENTLY ASKED QUESTIONS FOR STATE COMMISSIONS 3 (May 2009).

[21] *See* Litos Report, *supra* note 14, at 4 ("A smarter grid refers to the current state of transformation [of the grid], one in which technologies are being deployed today or in the near future.").

[22] These benefits will include optimizing asset utilization and efficient operation, enhancing reliability, improving power quality, reducing widespread outages, and reducing vulnerability to man-made and natural disasters. *See* Litos Report, *supra* note 14 at 5-6.

[23] *See, e.g.*, In the matter of the Application of Baltimore Gas and Electric Co. for Authorization to Deploy to a Smart Grid Initiative and to Establish a Surcharge for the Recovery of Cost, Order No. 83410, Case No. 9208, Pub. Serv. Comm'n. *See also Petition of Massachusetts Electric Company and Nantucket Electric Company, each d/b/a National Grid for Approval of a Smart Grid Pilot Program,* D.P.U. 09-32 (July 27, 2010).

[24] Re: Smart Grid RFI: Addressing Policy and Logistical Challenges to Smart Grid Implementation, *Comments of Edison Electric Institute*, at 3-4 (Nov. 1, 2010) [hereinafter *EEI*

B. Who Will Benefit from the Smart Grid?

Apart from definitional issues, a host of questions arise as to what the Smart Grid may mean for the consumer. A number of third-party service providers[25] have started to provide energy-related services that will take advantage of smart meter data, while other services are currently in development.[26] These new third-party market entrants will strategically position themselves between the customer and the utility, resulting in what has been termed "customer disintermediation"–an occurrence in which vendors offer attractive energy products and services to customers that will allow customers to bypass their local utility.[27] Much of the focus has been on energy management applications that permit users to monitor and control their energy use.[28] Facilitated by broadband networks and the Internet, consumers can access these applications through their smart phones or computers, permitting the automation of electric consumption decisions through control of energy-consuming devices, as well as demand response.[29] HANs can connect and control a wide variety of appliances such as water heaters, washers/dryers and lights, and can be monitored both directly and remotely. At the same time, smart meters allow consumers and third party service providers to monitor not only historical energy consumption data, but also near real-time data (including price and demand data), and to make economic decisions regarding energy usage. This is particularly true in jurisdictions where electric utilities are permitted to implement time-

---

Comments], *available at* http://www.oe.energy.gov/DocumentsandMedia/EEI_-_DOE_SG_RFI.PDF.

[25] Third party service providers are entities, other than incumbent electric utilities which provide energy services to consumers. The services which they provide include but are not limited to merchant energy and demand response offerings. *See, e.g., Shop for Energy Suppliers*, STATE OF NEW JERSEY BD. OF PUBLIC UTILITIES, http://www.nj.gov/bpu/commercial/shopping.html#5 (last visited May 14, 2011) (providing an example of New Jersey's plan to allow consumers to "shop around for the best price on their energy supplies.").

[26] For a good description of the consumer Smart Grid services that will be available in the future *see* FRIEDMAN, *supra* note 7, at 217 *et. seq.* (describing consumer Smart Grid services that will be available in the future).

[27] JESSE BERST, GLOBAL SMART ENERGY, SUMMARY OF JUNE 2010 EEI SMART GRID SCENARIO WORKSHOPS 8 (2010). Products offered to customers might include energy management options on the customer-side of the meter, as well as options to purchase energy from distributed resources. *See* Lou Jahn, Edison Electric Institute, EEI Smart Grid Scenario Project Update, slide 9 (2010); *see also Rogers Sees Third Party Energy Service Firms as a Big Potential Threat*, RESTRUCTURING TODAY, May 20, 2011, at 1.

[28] NATIONAL BROADBAND PLAN, *supra* note 1, at 273.

[29] LYNNE KIESLING, THE KNOWLEDGE PROBLEM, LEARNING, AND REGULATION: HOW REGULATION AFFECTS TECHNOLOGICAL CHANGE IN THE ELECTRIC POWER INDUSTRY, STUD. EMERGENT ORDER, VOL. 3, 149-171 (2010); MILES KEOUGH, NARUC, THE SMART GRID: FREQUENTLY ASKED QUESTIONS FOR STATE COMMISSIONS, (May 2009) *available at* http://www.naruc.org/Publications/NARUC%20Smart%20Grid%20Factsheet%205_09.pdf.

based or dynamic pricing. The Smart Grid will also be essential to the integration of electrical vehicles into the power grid, which will take advantage of lower cost and off-peak capacity and will provide grid support during periods of peak demand.[30]

Furthermore, well-known corporations such as General Electric and Whirlpool have developed a host of "smart appliances" such as Smart Grid-compatible refrigerators and clothes dryers, while others have developed programmable thermostats and in-home energy displays. Companies such as Microsoft and Google have released Internet visualization tools and web portals to help consumers monitor and manage their energy use.[31]

These and similar appliances and applications, which allow customers to access Smart Grid data, will create new energy services markets on both the utility and customer-facing sides of the meter. Customers will be able to spot and control (if not replace) energy inefficient appliances, determine when to use appliances, exhibit greater control over energy bills, participate more effectively in demand-side management programs, and ultimately facilitate competition in the energy marketing and energy services arenas. These applications are essentially "edge services"[32] and will ultimately be provided by electric and gas utilities, as well as third party service providers in competition with one other. The cost and efficiency implications of these services and applications, while difficult to quantify at this stage of the game, likely will be tremendous over the long term. As the Federal Communications Commission ("FCC") aptly noted in its National Broadband Plan ("NBP"), "[m]aybe energy transactions, not just energy management and efficiency, will be the next killer application of the Internet."[33]

Smart Grid data will also enable electric utilities to improve network reliability and utilization at the transmission and distribution levels,[34] and will assist utilities in their performance of more traditional operational and billing functions by allowing utilities to communicate with smart meters and receive usage data automatically. Ultimately, the Smart Grid may stimulate a change in the structure of the electric utility industry. On the retail side, today's electric utility industry is characterized by the traditional vertically integrated compa-

---

30 Litos Report, *supra* note 14, at 29, 31; *see* NATIONAL BROADBAND PLAN, *supra* note 1, at 250-251.

31 *See Google PowerMeter*, GOOGLE, http://www.google.com/powermeter/about/about.htm; NATIONAL BROADBAND PLAN, *supra* note 1, at 272; *see also* ELIAS L. QUINN, SMART METERING & PRIVACY: EXISTING LAW AND COMPETING POLICIES, A REPORT FOR THE COLORADO PUBLIC UTILITIES COMM'N, at B-3, B-4 (2009).

32 QUINN, *supra* note 31, at B-1.

33 NATIONAL BROADBAND PLAN, *supra* note 1, at 274.

34 *See* AMERICAN PUBLIC POWER ASSOCIATION, SMART GRID ESSENTIALS A PUBLIC POWER PRIMER 5-6 (2009).

nies[35] and wires companies.[36] While these companies will continue to exist, they may have less contact with retail customers and will be joined by the previously described third party service providers.

Smart Grid technologies and applications offer many benefits, but can also prove to be the proverbial double-edged sword. Smart Grid data can be so highly granular as to detect the use of household appliances, water heaters or showers.[37] If left unchecked, those with access to Smart Grid data–including law enforcement officials, commercial entities, thieves and con artists–could gain insight into individual behavior including arrival and departure patterns and daily use of appliances. At a minimum, the marketing and research data that could be mined from Smart Grid data would be very valuable and could be easily misused.[38] Additionally, malicious access to Smart Grid services could provide a means to disrupt grid functionality.[39]

Questions arising in part from a desire to facilitate the deployment of Smart Grid technologies, and in part from concerns about the impact that these technologies will have on customers, have led to a number of Federal and state proceedings examining Smart Grid-related issues and Smart Grid legislation. The following section describes this complex regulatory framework.

III. A COMPLEX REGULATORY FRAMEWORK

Smart Grid development presents a variety of novel practical and legal is-

---

[35] Vertically integrated companies are those that own transmission, distribution and generation plant and facilities and provide service to retail customers. *See Electric Power Industry Overview 2007*, U.S. ENERGY INFORMATION ADMINISTRATION, http://www.eia.doe.gov/cneaf/electricity/page/prim2/toc2.html.

[36] Wires companies do not own generation plant but do own transmission and distribution plant, and provide service to retail customers. *See* PUBLIC UTILITY COMM'N OF TEXAS, STUDY REGARDING THE PROVISION OF ELECTRICITY DURING A NATURAL DISASTER OR EMERGENCY 7-8 (2009) (detailing how wire companies carry power for end users, without selling them power).

[37] *See* Jon Froelich ET AL., *Disaggregated End-Use Energy Sensing for the Smart Grid*, 10 IEEE PERVASIVE COMPUTING 28-29, 31 (2011).

[38] QUINN, *supra* note 31, at B-6, B-7. For example, insurance companies could monitor Smart Grid data from consumers to adjust insurance prices based on energy usage factors. Quinn suggests that auto companies may adjust premiums if they discovered that you have averaged below average sleep levels each night for a month, thereby placing you in a greater risk category for an accident. *Id.* at B-7.

[39] *See, e.g.*, SMART GRID INTEROPERABILITY PANEL CYBER SECURITY WORKING GROUP (SGIP), INTRODUCTION TO NISTIR 7628 GUIDELINES FOR SMART GRID CYBERSECURITY 6 (Sept. 2010), *available at* http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf; Melissa Hathaway, *Power Hackers: The U.S. Smart Grid is Shaping Up to be Dangerously Insecure*, HARVARD-BELFER CTR FOR SCIENCE AND INT'L AFFAIRS, http://belfercenter.ksg.harvard.edu/publication/20424/power_hackers.html (last visited May 14, 2011).

sues that involve a multitude of regulatory jurisdictions, federal departments and agencies, and state authorities. The federal government's efforts in the Smart Grid area have been particularly broad, mandated in part by statute[40] and in part by policy considerations.[41] These efforts have encompassed many agencies including the Office of Science and Technology Policy ("OSTP") within the Executive Office of the President, as well as many operational units within the DOE, FCC, Federal Energy Regulatory Commission ("FERC"), National Institute of Standards and Technology ("NIST"), and the National Science and Technology Council Committee on Technology's Subcommittee on the Smart Grid.[42] This section will review these efforts in somewhat sequential order because at first blush many of the efforts appear to overlap.

A. EISA

The Energy Independence and Security Act of 2007 ("EISA")[43] established a national policy for modernizing the nation's electric transmission and distribution systems in order to maintain a reliable and secure energy infrastructure capable of meeting future growth in electricity demand and achieving numerous goals to advance the Smart Grid.[44] As laid out above, EISA section 1301 sets forth ten characteristics and goals for the Smart Grid, including cybersecurity and improved consumer energy information and control.[45] To meet these objectives, EISA sets out numerous directives and guidance for Smart Grid development, and creates important roles for several federal departments and agencies.

EISA vests in DOE an obligation to establish a Smart Grid Advisory Committee ("SGAC") comprised of representatives from various industries who have "experience and expertise to represent the full range of smart grid technologies and services, to represent both private and non-Federal public sector stakeholders."[46] The purpose of the SGAC is to inform Federal officials of the

---

[40] Energy Independence and Security Act (EISA), Pub. L. No. 110-140 § 1301, 121 Stat. 1492, 1783-1784 (2007) (codified at 42 U.S.C. §§ 17001 *et seq.*).

[41] *National Science and Technology Council Establishes Subcommittee on Smart Grid*, NAT'L SCIENCE AND TECH. COUNCIL COMM. ON TECH., (July 12, 2010), http://www.smartgrid.gov/news/nstc_subcommittee ("The Smart Grid is a vital component of President Obama's comprehensive energy plan, which aims to reduce harmful greenhouse gas emissions and U.S. dependence on oil, create jobs, and help U.S. industry compete in global markets for clean energy technology.").

[42] *See* DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 1.

[43] Energy Independence and Security Act (EISA), Pub. L. No. 110-140 § 1301, 121 Stat. 1492, 1783-1784 (2007) (codified at 42 U.S.C. §§ 17001 *et seq.*).

[44] *See* EISA § 1301 (codified at 42 U.S.C. § 17381) (detailing U.S. policy goals for the modernization of the electricity infrastructure for Smart Grid).

[45] EISA § 1301(2),(8) (codified at 42 U.S.C. § 17381(2),(8)).

[46] EISA § 1303(a) (codified at 42 U.S.C. § 17383(a)(1)).

ongoing efforts to develop Smart Grid technologies, charting the progress towards a national transition to use of a full range of Smart Grid technologies and services.[47] The SGAC is also charged with advising DOE and other Federal representatives on the evolution of interoperability standards to enable communications between Smart Grid devices.

The EISA also charges the DOE to create a Smart Grid Task Force ("SGTF") that consists of representatives from DOE's Office of Electric Delivery and Energy Reliability ("OEDER") who are tasked with the transition to Smart Grid technologies, as well as representatives from FERC and NIST.[48] The SGTF is responsible for the federal role in the transition toward use and development of Smart Grid technologies, and for "insure awareness, coordination and integration of the diverse activities of . . . the Federal Government related to smart-grid technologies and practices."[49] Namely, this includes oversight of both Smart Grid research and development, and the creation of Smart Grid standards and protocols. The SGTF is also responsible for undertaking a careful review of the relationships between Smart Grid technologies and practices and utility regulation, infrastructure development, and system security and reliability, as well as a variety of other electricity elements including supply, demand, transmission and distribution.[50] EISA further ensures collaboration between the SGAC, SGTF and other Federal offices.

Under EISA, the DOE is the entity primarily responsible for funding Smart Grid research and development efforts, as well as regional demonstration projects to exhibit the potential benefits of Smart Grid investments. At a regional level these efforts might include, for example, advanced power grid sensing and communications.[51] An underlying objective of these Smart Grid demonstration projects is to facilitate the transition to, and integration of, new Smart Grid technologies in existing electric systems, with a goal of improving system performance, power flow control and reliability. These efforts are also critical to achieve an understanding of important regional and regulatory differences relevant to effective implementation of the Smart Grid.[52]

DOE is also responsible for developing and establishing procedures for Smart Grid investment grants. EISA section 1306 includes nine types of investments that qualify for DOE Smart Grid grants, most of which reference equipment, appliances or software that engage in, or enable, "Smart Grid func-

---

47 EISA § 1303(a)(2) (codified at 42 U.S.C. § 17383(a)(2)).

48 EISA § 1303(b) (codified at 42 U.S.C. § 17383(b)(2)).

49 EISA §1303(b)(2) (codified at 42 U.S.C. § 17383(b)(2)).

50 *Id.*

51 *See* EISA § 1304(b) (codified at 42 U.S.C. § 17384(b)(1)) (describing the Smart Grid Regional Demonstration Initiative).

52 EISA § 1304(b)(2)(E) (codified at 42 U.S.C. § 17384(b)(2)(e)).

tions" or coordination.[53] EISA also defines "Smart Grid functions" to mean any of the following:[54]

- The ability to develop, store send and receive digital information concerning electricity use, costs, prices, time of use, nature of use, storage, or other information relevant to device, grid, or utility operations to or from or by means of the electric utility system, through one or a combination of devices and technologies.

- The ability to develop, store send and receive digital information concerning electricity use, costs, prices, time of use, nature of use, storage, or other information relevant to device, grid, or utility operations to or from a computer or other control device.

- The ability to measure or monitor electricity use (*i.e.*, time of day use), power quality characteristics (*i.e.*, voltage levels), or generation type, and the ability to "store, synthesize or report that information by digital means."

- The ability to sense and localize disruptions or changes in power flows on the grid, and communicate such information instantaneously and automatically to enable automatic protective responses to sustain reliable and secure grid operations.

- The ability to detect, prevent, respond to or recover from system security threats (e.g., cybersecurity threats; terrorism), and the ability to communicate regarding such threats, using digital information, media and devices.

- The ability of any appliance or machine to respond to such signals or communications automatically or in a manner programmed by an owner/operator without independent human intervention.

- The ability to use digital information to operate functionalities on the electric utility grid that were previously electro-mechanical or manual.

- The ability to use digital controls to manage and modify electricity demand, enable congestion management, assist in voltage control, provide operating reserves, and provide frequency regulation.

EISA vests in NIST the responsibility to "coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems."[55] A goal of this directive is to enable all components of the Smart Grid to utilize effective two-way communications, by establishing a common set of interop-

---

53 EISA § 1306(b)(1)-(9) (codified at 42 U.S.C. § 17386(b)(1)-(9)).
54 EISA § 1306(d) (codified at 42 U.S.C. § 17386(d)).
55 EISA § 1305(a) (codified at 42 U.S.C. § 17385(a)).

erability standards and protocols. This includes enabling all electric resources, including demand response and other demand-side resources, to participate in an efficient and reliable electric system.

NIST's role in achieving these objectives is one of coordination, and involves working with numerous standards development organizations to reach a common set of standards. EISA instructs NIST to seek input and collaborate with FERC, DOE's OEDER and the SGTF, the SGAC and other relevant Federal and state agencies.[56] Private organizations and standards development entities also have an important role in NIST's Smart Grid interoperability framework under EISA. NIST is to work closely with entities interested in interoperability standards and protocols, including the GridWise Architecture Council, the International Electrical and Electronics Engineers, the North American Electric Reliability Corporation, and the National Electrical Manufacturer's Association.[57]

The intended result of this collaborative process is a uniform framework of Smart Grid interoperability standards that is technologically neutral and sufficiently flexible such that it may accommodate traditional forms of generation and transmission resources, as well as consumer distributed resources such as distributed generation. A framework of standards under EISA must also accommodate renewable resources, energy storage and energy efficiency, as well as demand response. EISA further stresses the importance of flexibility in design, and requires interoperability standards to account for regional and organizational differences, as well as technological innovations.[58] EISA contemplates development of voluntary uniform standards for certain consumer-level electric appliances. These "smart" appliances would have the ability (at the customers' election, and consistent with applicable state and Federal laws) to respond to electric grid emergencies and demand response signals through load reduction, adjust the load to provide ancillary services to the grid, and provide short-term load shedding to help maintain grid reliability in the event of a reliability crisis that threatens an outage.[59]

EISA secures a role for Federal approval of the interoperability standards developed through the NIST standards development process. FERC is required to initiate rulemaking proceedings to formally adopt NIST's interoperability standards "as may be necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets."[60] Importantly, FERC is only to initiate such rulemak-

---

56 EISA § 1305(a)(1) (codified at 42 U.S.C. § 17385(a)(1)).
57 EISA § 1305(a)(2) (codified at 42 U.S.C. § 17385(a)(2)).
58 EISA § 1305(b) (codified at 42 U.S.C. § 17385(b)).
59 EISA § 1305(b)(3) (codified at 42 U.S.C. § 17385(b)(3)).
60 EISA § 1305(d) (codified at 42 U.S.C. § 17385(d)).

ings once it is satisfied that the NIST efforts have led to "sufficient consensus" on interoperability standards. FERC has interpreted this mandate to mean that it has "the authority to adopt a standard that will be applicable to all electric power facilities and devices with [S]mart [G]rid features, including those at the local distribution level and those used directly by retail customers so long as the standard is necessary for the purpose" outlined in EISA section 1305(d).[61]

Relevant to the states, EISA creates two new standards for state regulatory commission consideration under Title I of the Public Utility Regulatory Policies Act ("PURPA").[62] These standards would require electric utilities to demonstrate that they considered investing in Smart Grid Equipment based on "appropriate factors," including costs and cost effectiveness, improved reliability, security, system performance and societal benefit.[63]

States are also charged with developing cost recovery methodologies for Smart Grid deployment, as they must consider treatment of aging infrastructure that will be replaced by Smart Grid technologies. Often replacement of such existing equipment will result in stranded costs for companies. The EISA PURPA provisions recognize the need to address the potential for stranded costs to promote investment in new Smart Grid equipment. Finally, EISA's PURPA standards call for states to consider requiring utilities to provide retail customers with access to Smart Grid information, including energy prices and customer usage statistics. EISA's PURPA amendments require state regulators to consider these standards, but do not require states to adopt specific Smart Grid-related standards.

B. Federal Energy Regulatory Commission

FERC is actively engaged in supporting the development and adoption of Smart Grid interoperability standards, and incentivizing investments in Smart Grid technologies. In July 2009, FERC issued a Smart Grid Policy Statement that, among other things, interpreted its EISA authority to adopt Smart Grid interoperability standards and provided guidance on the development of key priorities to achieve interoperability and functionality of Smart Grid systems and devices.[64] In October 2010, FERC received the initial five groups of NIST Smart Grid interoperability standards, which it is currently reviewing in ad-

---

[61] Smart Grid Policy, 74 Fed. Reg. 37098, 37101 (Jul. 27, 2009) (to be codified at 18 C.F.R. chap. I). FERC reaches this conclusion based in part on the fact that EISA section 1305(d) does not exclude facilities used in local distribution, or otherwise limit FERC authority to approve standards.

[62] *See* EISA § 1307 (amending Section 111(d) of PURPA (16 U.S.C. § 2621(d)).

[63] EISA § 1307(a).

[64] Smart Grid Policy, 74 Fed. Reg. 37098, 37102 (Jul. 27, 2009) (to be codified at 18 C.F.R. chap. I).

vance of a potential rulemaking. In addition, FERC, in January of 2011, engaged industry stakeholders in a technical conference on Smart Grid interoperability standards.[65]

1. Smart Grid Policy Statement

FERC's Policy Statement provides a good deal of insight into the Commission's forward thinking with regard to its role in the development and adoption of industry-wide Smart Grid interoperability standards. Under EISA, FERC is charged with the formal review of Smart Grid standards once the Commission is satisfied that NIST's efforts have led to sufficient industry consensus. Once satisfied, FERC is directed to initiate a rulemaking to adopt the NIST standards and protocols. In its Policy Statement, FERC interpreted this EISA mandate to give the Commission authority to adopt a standard that will be applicable to

> all electric power facilities and devices with [S]mart [G]rid features, including those at the local distribution level and those used directly by retail customers so long as the standard is necessary . . . for [S]mart [G]rid functionality and interoperability in interstate transmission of electric power, and in regional and wholesale electricity markets.[66]

FERC noted, however, that its adoption of any Smart Grid standard under EISA does not make the standard mandatory, nor does EISA give FERC authority to require the development of any Smart Grid standard.[67] Any Commission authority to make Smart Grid standards mandatory, or to allow rate recovery of Smart Grid costs must derive from its existing authority under the FPA.[68] In addition, FERC's EISA authority does not change the scope of the Commission's ratemaking or reliability jurisdiction under FPA sections 205, 206 or 215, nor does it give FERC any authority to direct states to implement any particular retail customer policies or programs.[69] The Commission added that adoption of national standards for Smart Grid technologies and standards should enhance policy choices available to states, and should not interfere with states' abilities to adopt certain advanced metering or demand response programs.[70]

FERC's Policy Statement outlined certain Smart Grid functions and characteristics aimed at addressing challenges to transmission system reliability, and

---

[65] *Smart Grid Interoperability Standards*, Notice of Technical Conference-FERC, (issued 12/21/10), *available at* http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=12516141.

[66] Smart Grid Policy, 74 Fed. Reg. 37098, 37101, ¶ 22 (Jul. 27, 2009) (to be codified at 18 C.F.R. chap. I).

[67] *Id.* ¶ 23.

[68] *Id.*

[69] *Id.* ¶¶ 23-25.

[70] *Id.* ¶ 27.

adopted six key priorities for Smart Grid interoperability standards development,[71] including two cross-cutting issues—system security (*i.e.*, cybersecurity) and inter-system communication and coordination—and four key grid functionalities—wide-area situational awareness,[72] demand response, electric storage, and electric transportation.[73] According to FERC, addressing these priorities could support Smart Grid goals, expedite the development of important energy functions, and support state programs such as renewable portfolio requirements.[74] NIST accepted these priorities in preparing its Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 ("NIST Framework"),[75] and added two additional priorities: advanced metering and distribution system automation.[76]

According to FERC, the Smart Grid could create opportunities for malicious access to Smart Grid devices, which could be used to disrupt grid functionality. FERC therefore required NIST-proposed standards to contain "sufficient cybersecurity protections . . . including, where appropriate, a . . . standard applicable to local distribution-related" Smart Grid components.[77] FERC also acknowledged that development of standards for communicating and coordinating across inter-system interfaces is critical to supporting Smart Grid goals such as improved system efficiency and reliability.[78] The Policy Statement concluded that wide-area situational awareness will provide tools to enhance system reliability by promoting increased knowledge of available resources, load and transmission, and allowing additional system automation and improved response to reliability events.[79] FERC also introduced a series of interim rate incentives available to utilities making early investments in Smart Grid technologies.[80] Noticeably lacking from the Policy Statement, however,

---

71 *Id.* at 37099, ¶ 6

72 Wide-area situational awareness is defined as "the visual display of interconnection-wide system conditions in near real time at the reliability coordinator level and above." *See id.* at 37105, ¶¶ 55-56.

73 *Id.* at 37102, ¶¶ 28-29.

74 *Id.* ¶ 28.

75 U.S. DEP'T. OF COMMERCE, NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS, RELEASE 1.0, OFFICE OF THE NAT'L COORDINATOR FOR SMART GRID INTEROPERABILITY 8-9 (Jan. 2010), *available at* http://nist.gov/public affairs/releases/upload/smartgrid interoperability final.pdf.

76 *Id.*

77 Smart Grid Policy, 74 Fed. Reg. 37098, 37103 ¶ 40-42 (Jul. 27, 2009).

78 *Id.* at 37104, ¶ 51.

79 *Id.* at 37105, ¶ 61.

80 *Id.* at 37009, ¶ 6. FERC's rate policy applies to the interim period prior to formal adoption of interoperability standards, and allows recovery of FERC-jurisdictional Smart Grid costs where an applicant demonstrates that (1) the Smart Grid equipment advances the goals of EISA section 1301; (2) the equipment will not adversely impact bulk-power system reliability or cybersecurity; (3) the applicant has minimized the possibility of stranded costs through use of technologies with upgradeable components to prevent the need for future

was any discussion of Smart Grid data access and privacy.

2. FERC's Ongoing Smart Grid Activity and Adoption of NIST Interoperability Standards

FERC is actively engaged in ongoing NIST efforts to reach industry consensus on Smart Grid interoperability standards and in the cybersecurity efforts of the NIST Cybersecurity Working Group ("CSWG").[81] FERC is also committed to working with states on Smart Grid issues and has formed a federal-state collaborative with NARUC to address Federal and state regulators' concerns regarding Smart Grid functionality, data privacy and security.

In July 2010, FERC staff issued an update on NIST development of Smart Grid interoperability standards and on FERC's industry outreach activities and presented the Commission with recommendations to facilitate the adoption of Smart Grid interoperability standards.[82] FERC Staff advised that the NIST process will result in continued development of, and modification to interoperability standards, and that FERC should initiate periodic rulemakings proposing to adopt standards identified by NIST as ready for FERC consideration.[83] Staff identified three areas for consideration for each proposed standard: (1) demonstration that sufficient industry consensus has been reached with respect to any given standard;[84] (2) demonstration that a standard is necessary for Smart Grid functionality and interoperability in interstate transmission of electric power and regional and wholesale electricity markets;[85] and (3) demonstra-

---

wide-scale replacements; and (4) the applicant agrees to share the results of its early adoption experiments with DOE's Smart Grid Clearinghouse. This approach allows utilities that make Smart Grid investments to recover the costs of these investments early, offering some certainty for jurisdictional entities and encouraging near-term deployment of technologies. Once industry-wide interoperability standards are in effect, the risks associated with Smart Grid investments will likely be reduced. *Id.*

81 *See* Fed. Energy Regulatory Comm'n, Smart Grid Standards Adoption: Staff Update and Recommendations, slide 1 (July 15, 2010), *available at* http://www.ferc.gov/legal/staff-reports/07-15-10-smart-grid.pdf (explaining FERC's recommendations for Smart Grid standards adoption through new policy).

82 *Id.*

83 *Id.* at slides 5-8.

84 *Id.* at slide 7. Staff advised the Commission, in determining "sufficient consensus," to rely on the National Technology Transfer and Advancement Act ("NTTAA"), in addition to comments received through the FERC rulemaking process. The NTTAA, a Federal law outlining the use of standards by the Federal government, recognizes "voluntary consensus bodies" to possess "attributes of openness, balance of interest, due process, an appeals process, and a consensus process." *Id.* According to Staff, NTTAA compliance may be established through use of an American National Standards Institute ("ANSI") accredited standards development process. *Id.*

85 *See id.* at slide 8. Staff recommended that the Commission look to NIST reports and documentation, as well as rulemaking comments, to determine whether a standard is neces-

tion that the standard poses no known cybersecurity risks.[86] Presumably FERC will look to these areas when proceeding with future rulemakings addressing interoperability standards.

In October 2010, NIST for the first time filed with the Commission five suites of Smart Grid interoperability standards for regulatory consideration.[87] In response, FERC established a new Docket No. RM11-2-000.While FERC's actions suggest the potential for a future rulemaking, pursuant to EISA section 1305(d),[88] to address the NIST standards, FERC has yet to determine what "sufficient consensus" might mean in the context of EISA, much less whether "sufficient consensus" exists for the five groups of standards.[89] It is unclear if FERC will institute a formal rulemaking proceeding to consider these or other Smart Grid interoperability standards.[90]

On November 14, 2010, FERC and NARUC jointly convened a technical conference to address the NIST Smart Grid interoperability standards submitted for FERC consideration.[91] The conference featured a NIST briefing on the five suites of standards, the standards development process, and issues related to their adoption. As part of this effort, NSTC and NARUC have formed a Smart Grid Working Group and have identified three areas for collaboration: (1) Technical Assistance to the States, (2) Consumer Engagement, and (3) Technology Labs.[92]

On January 31, 2011, FERC convened a technical conference to discuss the five groups of NIST standards and to inform the Commission on whether "sufficient consensus" exists for FERC to consider the standards in a rulemaking proceeding.[93] Discussion at the conference focused on the NIST process used to review and select the five groups of interoperability standards, and the ex-

---

sary for Smart Grid functionality and interoperability.

[86] *See id.* at 6. On this front, Staff advised the Commission to consider cybersecurity guidelines developed by the CSWG, as well as rulemaking comments.

[87] *See* Smart Grid Interoperability Standards, 75 Fed. Reg. 63462 ¶¶ 2-3 (Oct. 15, 2011).

[88] *Id.*

[89] *See* FERC, Smart Grid Interoperability Standards, Supplemental Notice Requesting Comments at 2-3 (2011), available at http://www.ferc.gov/EventCalendar/Files/20110228084004-supplemental-notice.pdf.

[90] Smart Grid Interoperability Standards, 75 Fed. Reg. 63462 ,¶¶ 1-2 (Oct. 15, 2011).

[91] *Id.*

[92] *See* George Arnold & Jessica Zufolo, Presentation at the NARUC Annual Convention, NTSC Smart Grid Subcomm.: Overview & Goals for Ongoing Federal/State Collaboration, slide 9 (Nov. 14, 2010), *available at* http://www.naruc.org/meetingpresentations.cmf?7 . Previously NARUC had formed its own Smart Grid Working Group. *See generally* NAT'L ASSOC. OF REGULATORY UTILITY COMMC'NS (NARUC), http://www.naurc.org/News?default.cfm?pr=211 (last visited May 14, 2011).

[93] *See* FERC Smart Grid Interoperability Standards, Notice of Technical Conference (Dec. 12, 2010), available at http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=12516141

tent and diversity of stakeholder participation in that process, as well as the interoperability standards development process going forward. FERC continues to explore these issues and sought stakeholder comment on, among other things, the NIST process, defining and determining "sufficient consensus," and the implications of potential enforceability of standards.[94]

C. Federal Communications Commission

While the FCC has played but a minor role in the energy arena, this changed to some degree on March 16, 2010 when the FCC delivered to Congress its long-awaited National Broadband Plan entitled *Connecting America: The National Broadband Plan.*[95] Unlike the prototypical FCC report, the NBP extensively discussed the use of broadband to promote energy efficiency and independence as well as competition in the energy sector.[96] Described by the FCC as a 21st century roadmap for connecting America to the Internet communications network of the future, the Plan found that while broadband access and use had increased, the nation must do more to connect all individuals and the economy—including the energy sector—to broadband's transformative benefits.[97] According to the FCC, the nation has failed to harness the power of broadband to transform delivery in, among other areas, energy conservation.[98]

1. The National Broadband Plan

In theory, the Plan is a non-binding report which was drafted by FCC staff, adopted by the FCC and sent to Congress. The NBP is the result of an American Recovery and Reinvestment Act mandate that the FCC develop a plan to ensure that every American has access to broadband capability including a detailed strategy for the use of broadband infrastructure and services to advance, among other things, energy independence and efficiency.[99] The NBP contained over fifty recommendations and goals for action by the FCC, Congress, several other federal agencies including FERC and DOE, and the states on a nationwide broadband strategy. [100]

---

[94] *See* Supplemental Notice Requesting Comments (Feb. 16, 2011), *available at* http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=12566111

[95] *See* NATIONAL BROADBAND PLAN, *supra* note 1, at xi-xv (detailing new FCC initiatives in energy policy).

[96] *Id.*

[97] *See generally id.*

[98] *See id.* at xi-xiv, 11 (explaining how "the country will need to modernize the electric grid with broadband and advanced communications").

[99] *See* NATIONAL BROADBAND PLAN, *supra* note 1, at 3.

[100] Paradoxically, while the NBP was unanimously adopted by the FCC, not every Commissioner agreed with every proposal in the Plan. *See, e.g.* Statement of Comm'ner

From the outset, the Plan linked energy and telecommunications, and argued that the successful efforts in the last century to electrify America must serve as a model for action in both the broadband and related energy markets. NBP Chapter 2, ambitiously titled "Goals for a High-Performance America," recommended that to ensure America leads in the clean energy economy, the country should establish a long-term goal that "every American should be able to use broadband to track and manage their real-time energy consumption."[101] In what the FCC described as an attempt to unleash innovation in homes and buildings and to promote an open competitive marketplace, the Plan made significant proposals which, if implemented, will assist in the deployment of the Smart Grid but will also dictate the nature of utilities' future interaction with their customers.[102] Chapter 12 of the NBP, entitled "Energy and the Environment," introduced a series of recommendations on how to promote energy independence by making smart data more accessible and increasing utilities' access to spectrum.[103]

The particularly long and complicated NBP drafting process began in April 2009 with the issuance of the thirty-one FCC notices.[104] As part of this proceeding, on September 4, 2009, the FCC issued a Public Notice on the "Implementation of Smart Grid Technology" in which it sought comment on the sustainability of communications networks, access to "real-time data," the role of third party application developers, and privacy and security requirements.[105] During the course of the proceeding, the FCC hired a separate staff to draft the Plan, reviewed 74,000 pages of comments, and held thirty-six public hearings, including several on utility issues.[106]

Although energy is not the primary focus of the Plan, the energy-related issues examined in the Plan were not completely new to the FCC, which has longstanding jurisdiction over utility spectrum[107] and pole attachment matters.[108] Likewise, the FCC previously determined that Broadband over Power

---

Mignon Clyburn, *A National Broadband Plan for our future,* GN Docket No. 09-51 (Mar. 16, 2010), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296890A1.pdf (issuing a statement regarding the National Broadband Plan that both supports its initiative in bringing the country up to speed, as well as criticizes the plan over its failure to show how it is to successfully support the nation's public interest goals, the lack of preparation for competition, and assurance that all Americans will benefit).

[101] NATIONAL BROADBAND PLAN, *supra* note 1, at 11.

[102] *See id.* at 253, 255 (describing how Smart Grid policy will stir innovation in use amongst customers and third parties).

[103] *See generally id.* at 245-262.

[104] *Id.* at ix.

[105] Comment Sought on the Implementing of Smart Grid Technology, NBP Public Notice # 2, *Public Notice*, 24 F.C.C.R. 11747, 11748-51 (Sept. 4, 2009).

[106] NATIONAL BROADBAND PLAN, *supra* note 1, at ix.

[107] *See id.* at 251 (discussing utilities' use of licensed spectrum).

[108] *See* 47 U.S.C. § 224(b)(1) (2006) (granting the Commission authority to "regulate the

Lines ("BPL") Internet Access Service is subject to its ancillary jurisdiction.[109] Furthermore, in its Open Internet Rulemaking, the FCC inquired whether an offering such as a Smart Grid should be defined or categorized as a "managed or specialized service" and, if so, what rules, if any, should apply.[110] Finally, the FCC has specific expertise in dealing with data access and privacy issues related to consumers and third-party service providers (i.e. Customer Proprietary Network Information "CPNI" rules).[111]

The FCC's effort was coordinated with other federal agencies and Congress. While the FCC completed the NBP, the White House OSTP simultaneously conducted a proceeding to determine how consumers should interface with the Smart Grid.[112] The very day after the FCC released the NBP, Congressman Markey introduced the "e-KNOW Act," which would enact into law many of the Plan's Smart Grid data access recommendations.[113]

2. The Smart Grid Provisions of Chapter 12

In Chapter 12, the NBP makes four specific recommendations regarding Smart Grid. In making these proposals, the FCC recognized that broadband and advanced communications infrastructure can play an important role in achieving national goals of energy efficiency, that energy transactions may be the "next killer application" of the Internet, and that the unlocking of energy data by utilities is key to integrating broadband into the Smart Grid.[114] The recommendations sought to promote energy efficiency by integrating broadband into the Smart Grid in order to unleash innovation and to "ensure greater competition and innovation in broadband-enabled Smart Grid information services and related devices by providing secure access to digital electric information for consumers and authorized third part[y]" service providers.[115] The four recommendations are as follows.

In NBP Recommendation 12.7, the FCC urged states to require electric utilities to provide consumers access to, and control of, their own digital energy information; including real-time information from smart meters, historical con-

---

rates, terms and conditions for pole attachments . . . .").

[109] *See In re* United Power Line Council's Petition for Declaratory Ruling Regarding the classification of Broadband Over Power Line Internet Access Service as an Information Service, *Memorandum Opinion and Order*, 21 F.C.C.R. 13,281, 13,291 (Nov. 3, 2006).

[110] *In re* Preserving the Open Internet Broadband Industry Practices, *Notice of Proposed Rulemaking*, 24 F.C.C.R. 13064, 13116-36117, ¶ 150 (Oct. 22, 2009).

[111] *See generally* 47 C.F.R. §§ 64.2001-64.2011 (2011).

[112] OSTP Request, *supra* note 10, at 7526, 7527.

[113] *See generally* Electronic Consumer Right to Know Act (e-KNOW), H.R. 4860, 111th Cong. (2010).

[114] NATIONAL BROADBAND PLAN, *supra* note 1, at 249-256.

[115] *Id.* at 30, 247.

sumption data, and price and bill data over the Internet. It further indicated that if the states failed to develop reasonable policies over the next eighteen months, Congress should consider national legislation to cover consumer privacy and the accessibility of energy data.[116]

The Commission posited that its proposed data access and control regime was necessary if end-users were to have the better and timelier energy usage information to maximize energy and cost savings.[117] The FCC recognized that broadband-enabled smart meters are the key to the energy efficiency effort because these instruments generate real-time data, which in turn enables consumers to select from a growing number of the energy-saving products and services described. The FCC asserted that strong action was required because, despite the wide variety of potential uses for the smart meter information, only 35% of the 17 million of deployed meters will provide customer access to this type of data and that less than 1% of customers have real-time access to data today.[118] The FCC believed that, under such circumstances, innovation would lag in the absence of a policies that promote customer access to energy data and their authorized third party service providers. [119]

Consequently, the FCC proposed that consumers, "and their authorized third party service providers must be able to get secure, non-discriminatory access to energy data in granular, standardized, machine-readable formats . . . in as close to real-time as possible."[120] It recommended that state commissions mandate such data accessibility as part of Smart Grid cases and that utilities be required to adopt policies clearly articulating how consumers might authorize third party service providers. The FCC further recommended that by year-end 2010, every state commission should require that by year-end 2011 its regulated IOUs provide historical consumption, price and bill data over the Internet, in machine readable, standardized formats. The agency urged Congress to pass legislation to the extent that the states fail to act.[121]

The FCC's other recommendations regarding the Smart Grid were essentially a sub-set of Recommendation 12.7. In Recommendation 12.8, the FCC indicated that the FERC "should adopt consumer digital data accessibility and control standards as a model for states."[122] In Recommendation 12.9, the FCC urged DOE to "consider consumer data accessibility policies when evaluating Smart Grid grant applications, report on the states' progress toward enacting

---

[116] *Id.* at 256.
[117] *Id.* at 253.
[118] *Id.* at 254-255.
[119] *Id.* at 253-256.
[120] NATIONAL BROADBAND PLAN, *supra* note 1, at 256.
[121] *See id.* at 256 (noting that Congress "should monitor the issue and consider national legislation if states fail to act").
[122] *Id.*

consumer data accessibility, and develop best practices guidance for states."[123] In Recommendation 12.10 the FCC stated that "the Rural Utilities Services (RUS) should make Smart Grid loans to rural electric cooperatives a priority, including integrated Smart Grid broadband projects and that RUS should favor Smart Grid projects from states and utilities with strong consumer data accessibility policies."[124]

These recommendations recognize the need for open and non-proprietary standards, the ongoing NIST standardization process, and the important roles of the DOE and FERC in Smart Grid implementation. Additionally, the recommendations seek to leverage the authority of FERC, DOE and RUS to force states and companies to adopt the data accessibility and control regime proposed in Recommendation 12.7.

D. Broader Efforts of the Obama Administration

Even before the FCC's release of its Smart Grid recommendations, the Obama Administration initiated a series of comprehensive efforts to develop a national Smart Grid policy with a significant focus data access, privacy and security. As noted previously, these efforts were coordinated through an administrative consortium of the OSTP, DOE, the National Institute of Standards (NIST) and the National Science and Technology Council (NSTC).

1. Office of Science and Technology Policy

On February 19, 2010 (almost one month before the release of the NBP) the Office of Science and Technology Policy within the Executive Office of the President released a Request for Public Comment seeking input regarding the consumer interface with the Smart Grid.[125] Among the questions asked were (1) whether it would be "technically and commercially feasible for consumers and their authorized third party service providers to access [Smart Grid] data easily and in real time" and (2) "[w]ho owns the home energy usage data"[126]

2. Department of Energy

Within two months of the release of the FCC's NBP, and in partial response

---

[123] *Id.* at 256-257.

[124] *Id.* at 257.

[125] *See* OSTP Request, *supra* note 10, at 7526-7527 ("The Executive Branch is considering ways to ensure that the consumer interface to the Smart Grid achieves the desired goal of providing all consumers with the information they need to control and optimize their energy use in a manner that ensures ease of use, widespread adoption, and innovation.").

[126] *Id.* at 7527.

to the NBP, DOE released the first two of ultimately three Smart Grid Requests for Information.[127] The first RFI, entitled "Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy" closely paralleled the OSTP inquiry in that it focused on questions pertaining to access to CEUD (real-time or otherwise), state and utility data access and collection policies, access to data by third-party service providers, consumer control over the data, and developing guidelines for policymakers.[128] DOE sought input on the following questions, among others:

- Who owns the energy consumption data?
- Who should be entitled to privacy protections relating to the data?
- What privacy practices should be implemented to protect the data?
- What third-party service providers should have access to the data, and how should they gain access?
- What standards should the DOE apply to third-party service providers to assist in protecting the data?
- What types of data should consumers and third party service providers have access to and should access be in real-time?
- What should be the role of DOE versus that of the states and other Federal agencies? [129]

---

[127] *See* DOE Data Access RFI, *supra* note 1, at 26203. *See also,* Implementing the National Broadband Plan by Studying the Communications Requirements of Electric Utilities to Inform Federal Smart Grid Policy, DOE Request For Information, 75 Fed. Reg. 26206 (July 12, 2010). In this latter RFI, DOE sought to collect information about electricity infrastructure's current and projected communications requirements. This latter RFI was unique in that it did not deal with data access, privacy and security issues.

[128] *See* DOE Data Access RFI, *supra* note 1, at 26203. ("As Smart Grid programs are rolled out across the country, utilities and their consumers will need to reach agreements on how detailed energy data should be collected, reported, managed, shared and disclosed in a way that allows utilities to maximize their investments in the smart Grid while continuing to respect consumers' privacy and security. This RFI will help to collect information, open a dialogue on how to best achieve that balance, and form the basis for best practices that can be distributed to states, public utility commissions and others."). *See also DOE Takes Steps to Implement the National Broadband Plan*, U.S. DEP'T. OF ENERGY, OFFICE OF THE GENERAL COUNSEL (May 11, 2010), http://www.gc.energy.gov/1574.htm.

[129] *See, e.g.,* Re: Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy, *Comments of the American Public Power Association*, at 4-5, 15 (July 12, 2010) [hereinafter *APPA Comments*], *available at* http://www.publicpower.org/files/PDFs/APPAcommentsonDOERFISmartGridprivacyquestions710.pdf; RE: Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy, *Comments of Exelon Corp.*, at 2 (July 12, 2010) [hereinafter *Exelon Comments*], *available at* http://www.gc.energy.gov/documents/Exelon_Comments_DataAccess.pdf; *EEI Comments*, *supra* note 24, at 29; Re: Smart Grid RFI: Addressing Policy and Logistical Challenges to Smart Grid Implementation, *Comments of Edison Electric Institute*, at 3-4 (Nov. 1, 2010),

Numerous parties filed comments and reply comments.[130] On some issues there was agreement, but on many issues there was none. For example, although there was consensus that consumers should have access to their individual data,[131] some consumer groups, such as the National Association of State Consumer Advocates ("NASUCA"), argued that consumers owned their individual CEUD.[132] In contrast, utilities asserted ownership control over consumption data that the utilities collected.[133] Other parties stated that CEUD should be co-owned by the utility and the consumer.[134] Still others stated that the issue of ownership was a complex one due to variance in state laws and regulatory structures and, that the key issue was not ownership of the data, but the actual *use* of this data.[135]

Most parties agreed that third-party service providers should have access to some energy consumption data, provided they have consumer consent.[136] However, the parties disagreed over certain access issues, including: (1) the scope of the data that should be accessible to third party service providers, (2) how third party service providers should gain access to the data or obtain consumer consent to access, (3) whether third party service providers should be required to be certified by the states prior to receipt of the data, (4) what obligations third party service providers should have to disclose to consumers, and (5) whether third-party service providers should be responsible for the costs incurred by utilities in developing the systems and infrastructure necessary to provide third party service providers with access to the data.[137] As telecommu-

---

available at http://www.oe.energy.gov/DocumentsandMedia/EEI_-_DOE_SG_RFI.PDF.

[130] *See supra* note 125. For a list of the comments and reply comments *see Smart Grid Information*, DEP'T. OF ENERGY, http://www.gc.energy.gov/1592.htm (last visited May 14, 2011).

[131] *See* DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 51.

[132] *See* RE: Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use and Privacy, *Comments of the National Association of State Utility Consumer Advocates* (NASUCA), at 7, 16 (July 12, 2010) [hereinafter *NASUCA Comments*], *available at* http://www.nasuca.org/archive/NASUCADOEComments17-12-10.pdf (stating that a customer "must own her or his home energy usage data").

[133] *See, e.g., Exelon Comments*, *supra* note 129, at 2 (clarifying that information collected by a utility about a customer's use is owned by the utility).

[134] *APPA Comments*, *supra* note 129, at 4-5 (suggesting that utilities and customers "co-own" smart meter data by allowing utilities to use it for business functions and consumers for ownership of consumption data).

[135] *EEI Comments*, *supra* note 24, at 4-5 (stating that the complexities of the Smart Grid require all major stakeholder groups, including state and federal regulators, to work together, and customer education is essential to maximize participation).

[136] *See* DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 50 (providing a content summary of comments, including comments from *APPA*, *Cleco*, *DTE*, and the *EEI*).

[137] *Id.* at 3-4 (providing that most parties concur that third-party service providers have a

nications precedent dictates, such consumer privacy issues should be addressed prior to the full development of the Smart Grid market.[138]

There was also a variety of opinions regarding the appropriate role of the federal government, and DOE in particular, versus that of the states. Some parties recognized that DOE and the federal government have important national leadership roles to play,[139] while others adamantly argued that federal agencies should not intrude upon traditional state authority over energy data access issues.[140]

3. National Science and Technology Council/Department of Energy

As part of the Obama Administration's ongoing efforts to address Smart Grid issues, the NSTC's Committee on Technology established a Smart Grid Subcommittee to guide the development of the Administration's Smart Grid policy.[141] Led by senior officials at DOE, the White House, and high-level officials from various other agencies,[142] the subcommittee's goals were to (1) ar-

---

right to some energy consumption data given consumer consent but parties disagreed over other third-party access issues).

[138] For example, at one point, it was possible to find numerous Web sites advertising the sale of personal telephone records for a price. *See In re* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP Enabled Services, *Report and Order and Further Notice of Proposed Rulemaking*, 22 F.C.C.R. 6927, 6928-6929, ¶ 2 (Apr. 2, 2007) [hereinafter *CPNI Order*]. Without proper controls regarding data access and disclosure, there would be little to stop the disclosure of similar energy related information by unscrupulous third parties.

[139] *See EEI Comments*, *supra* note 24, at 27 (noting that the government plays an important role in "issues such as communications, technical standards, and broad public education about the uses and benefits of the Smart Grid"). *See, e.g.*, Re: National Broadband Plan (NBP) Request for Information: Data Access, *Comments of Whirlpool Corp.*, at 4 (July 12, 2010) [hereinafter *Whirlpool Comments*], *available at* http://www.gc.energy.gov/documents/Whirlpool_Comments_DataAccess.pdf (preferring federal programs and standards to encourage scale economies and consumer adoption) ; *NASUCA Comments*, *supra* note 132, at 20 (arguing for the development of minimum federal standards in order to promote uniformity and ease of market entry).

[140] *See, e.g., Exelon Comments, supra* note 129 at 4 (arguing for the DOE to defer to states); NBP RFI: Data Access, Third Party Use, and Privacy, *Comments of Utilities Telecom Council,* at 12 (July 12, 2010) [hereinafter *UTC Comments*], *available at* http://www.gc.energy.gov/documents/UtilitiesTelecom_Comments_DataAccess.pdf (preferring state regulatory authority because smart grid development and implementation are expansions of typical utility operations).

[141] *National Science and Technology Council Establishes Subcommittee on Smart Grid*, SMARTGRID.GOV (July 12, 2010), http://www.smartgrid.gov/news/nstc_subcommittee.

[142] The Chair of the Subcommittee is Patricia Hoffman (Principal Deputy Assistant Secretary (PDAS) for the Office of Electricity and Energy Reliability at the United States DOE), and the Vice Chair is George Arnold (National Coordinator for Smart Grid Interoperability). Other members of the Subcommittee's Steering Committee include Aneesh Chopra (Chief Technology Officer, Assistant to the President of the United States and Associate

ticulate a vision for Smart Grid and the core priorities and opportunities for its development, (2) facilitate a strong, coordinated effort across federal agencies to develop Smart Grid Policy, and (3) develop a framework for administration Smart Grid policy related that will be described in a public report.[143]

As part of the subcommittee's efforts to draft the aforementioned public report, the DOE released its third and longest Smart Grid RFI—this time addressing "policy and logistical challenges" to Smart Grid implementation.[144] The DOE released the RFI "on behalf of the Administration and in consultation with key stakeholders from state regulatory bodies," in order to assure that Smart Grid deployments benefit consumers and to inform NSTC's analysis of policy challenges and possible solutions.[145] Although not its primary focus, the RFI asked a number of questions related to data access, privacy and security issues.[146]

4. DOE's Data Access and Privacy Report

On October 5, 2010, the Department of Energy released its *Data Access and Privacy Report* examining the manner in which legal and regulatory schemes have evolved to protect consumer privacy and choice while advancing the development of energy-management services and technologies that rely on granular energy-usage data.[147] Starting with the fundamental proposition that,

---

Director of Technology), Philip J. Weiser (Senior Advisor to the National Economic Counsel) and Jason Bordoff (Associate Director for Energy and Climate Change at the White House Council on Environmental Quality). *See* George Arnold & Jessica Zufolo, Presentation at the NARUC Annual Convention, NTSC Smart Grid Subcomm.: Overview & Goals for Ongoing Federal/State Collaboration (Nov. 14, 2010), *available at* http://www.naruc.org/meetingpresentations.cmf?7; *see George W. Arnold Biography,* NIST.GOV, http://www.nist.gov/smartgrid/arnold.cfm.

[143] *See* George Arnold & Jessica Zufolo, Presentation at the NARUC Annual Convention, NTSC Smart Grid Subcomm.: Overview & Goals for Ongoing Federal/State Collaboration (Nov. 14, 2010), *available at* http://www.naruc.org/meetingpresentations.cmf?7.

[144] Addressing Policy and Logistical Challenges to Smart Grid Implementation, DOE Request for Information, 74 Fed. Reg. 57005-57006 (Sept. 17, 2010).

[145] *Id.* at 57006-57007.

[146] *See, e.g., id.* at 57008 ("Are steps necessary to make participation easier and more convenient . . .reduce risks, or otherwise better serve consumers? Moreover, what role do factors like . . . consumer control . . . play in shaping consumer participation . . . ?"). *See also id.* at 57010 ("What is the role of federal, state, and local governments in assuring smart grid technologies are . . .maintained in a manner that ensures cybersecurity?").

[147] *See generally* DATA ACCESS AND PRIVACY REPORT, *supra* note 12. At the same time the Department also issued a second report, entitled *Informing Federal Smart Grid Policy: Communications Requirements of Smart Grid Technologies*, examining how the communications needs of utilities and the electrical grid are likely to evolve as Smart Grid technologies become more widely used. *See generally* DEP'T. OF ENERGY (DOE), COMMUNICATIONS REQUIREMENTS OF SMART GRID TECHNOLOGIES Oct. 5, 2010 [hereinafter COMMUNICATIONS REQUIREMENTS REPORT], *available at*

when properly balanced by regulators and understood by the public, privacy and access are complementary values, not conflicting goals,[148] the DOE made a number of key findings and recommendations related to Smart Grid data access, privacy and security.[149] Unsurprisingly, the DOE found that many Smart Grid technologies can generate highly-detailed or "granular" energy-consumption data that should receive privacy protections because of its sensitive or potentially useful nature. In doing so, the DOE recognized that while CEUD can be a powerful tool that enables utilities and third-party service providers to engage consumers in realizing the benefits of energy efficiency, numerous important privacy implications exist because it "is the energy usage data itself *and* the ability to tie that data to an individual or household that makes the data particularly sensitive."[150] Fundamentally, the Department found that all classes of electric utility customers, both residential and commercial, should be entitled to protect the privacy of their own individual energy-usage data.[151] Moreover, consumers should be able to access CEUD and (to decide whether third-party service providers are entitled to access CEUD for purposes other than providing electrical power.[152] The DOE found that a critical goal of implementing Smart Grid technologies should be providing consumers with access to "actionable" data, which will allow consumers to alter their energy-use patterns to reduce their overall energy costs. It also found agreement among commenters that consumers should decide whether and for what purposes third party service providers should be authorized to access or receive CEUD. Finally, the DOE found that consumer control of third-party service provider access to CEUD would promote the development of a competitive, open, transparent, and innovating marketplace for the use and management of energy-consumption data.[153] To facilitate this, the Department urged states to

---

http://www.gc.energy.gov/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf.

[148] *See* DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 2-3. Congress and the FCC came to a similar conclusion with regard to customer proprietary network information when coming to grips with similar privacy and access issues in the context of opening the telecommunications market. *See CPNI Order*, *supra* note 138, ¶ 4.

[149] In addition to these findings DOE also concluded that consumer education and flexibility in both technology and pace of deployment will be critical to the long-term success of Smart Grid technologies. *Id.* at 4, 7. While important, this only tangentially affects the access privacy issues.

[150] *Id.* at 9-10. Even so, DOE also concluded that utilities should continue to have access to CEUD and be able to use that data for utility-related business purposes like managing their networks, coordinating with transmission and distribution-system operators, billing for services, and compiling it into anonymized and aggregated energy-usage data for purposes like reporting jurisdictional load profiles. *Id.* at 10.

[151] *See* DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 3, 12-13.

[152] *Id.* at 11.

[153] DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 11-12.

carefully consider the conditions under which consumers can authorize third party service provider access to CEUD.[154]

In particular, the DOE recommended to the states that utilities should not disclose CEUD to third party service providers unless a given consumer has consented to such disclosure affirmatively, through an opt-in process that reflects and records the consumer's informed consent. It further stated that jurisdictions designing such opt-in authorization processes should require a valid authorization that specifies the purposes for which the third party service provider is authorized to use CEUD, define the term during which the authorization will remain valid, and identify the means through which consumers can withdraw such authorizations. It also proposed that third party service providers authorized to receive CEUD should be required to protect the privacy and the security (including integrity and confidentiality) of CEUD that they receive and to use it only for the purposes specified in the authorization. Finally it urged states to enact laws or rules that define the circumstances, conditions, and data that utilities should disclose to third party service providers.

There were a number of issues relating to third-party service provider access about which DOE found there was no consensus. The Report noted that these issues need to be addressed when Smart Grid technologies are deployed and that the answers might vary between jurisdictions. The DOE further attempted to describe the questions involved, identify varying approaches and assess the record.[155]

Utilities generally argued that third party service providers should be subject to the same types of data privacy obligations as utilities.[156] Further, utilities argued that in light of the costs involved real-time reporting should not be mandatory and, so as not to burden consumers who do not subscribe to various services, third party service providers should bear the costs of providing the data to themselves.[157] Not unexpectedly, third party service providers took contrary positions. In some instances the DOE recommended a position; in others it did not. For example, on the question of whether consumers should authorize third party service access to CEUD by written or electronic means, the DOE recommended that states consider transitioning from written to online authorization.[158]

5. National Institute of Standards and Technology

---

[154] *Id.* at 14-21.
[155] *Id.* at 3-4, 8.
[156] *Id.* at 15-16.
[157] *EEI Comments*, *supra* note 24, at 35-36 (July 12, 2010).
[158] DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 17 (Oct. 5, 2010).

EISA section 1305 directs NIST to coordinate the development of a framework to achieve interoperability of Smart Grid devices and systems.[159] In furtherance of this responsibility, NIST has engaged in considerable outreach to identify standards for potential inclusion in a Smart Grid interoperability framework, and has provided a good deal of guidance for industry stakeholders and regulators as they collectively move forward with the development, consideration and adoption of Smart Grid Interoperability standards. [160]

NIST has been equally active on the Smart Grid data privacy front. Volume two of NISTIR 7628 addresses privacy issues introduced by Smart Grid implementation, with a particular focus on privacy issues within personal dwellings. According to NIST, the privacy concerns raised by the Smart Grid are diverse, and include privacy of personal information (i.e., when, where, how, to whom and to what extent CEUD is shared), privacy of the person (i.e., control over bodily integrity), privacy of personal behavior (i.e., protection of personal activities from unauthorized disclosure), and privacy of personal communications (i.e., freedom to communicate in a secure fashion).[161]NIST concluded that Smart Grid technologies and information create unique privacy risks and challenges that are not addressed by existing laws and regulations, or existing practices of utilities or third party service providers.[162] According to NIST, both utilities and third party service providers should follow recognized privacy protection policies, and should evaluate existing policies.[163] The NISTIR 7628 went on to acknowledge that the goal of widespread Smart Grid participation will only occur "when effective and transparent privacy practices are consistently implemented, followed, and enforced within the Smart Grid."[164]

To combat these novel privacy exposures, and to cultivate the trust of Smart Grid participants, NIST identified a series of recommended privacy practices.[165] NIST's recommendations, while not official standards, are highly relevant to the Smart Grid and offer a reference for policymakers, utilities and third party service providers as they update existing privacy policies and practices. As discussed further below, NIST recommended that entities conduct privacy impact assessments ("PIA") and develop formal privacy policies and

---

[159] *See* Energy Independence and Security Act of 2007 (EISA), Pub. L. No. 110-140 § 1305(a), 121 Stat. 1492, 1783-84 (2007) (codified at 42 U.S.C. § 17385(a)).

[160] *See* Smart Grid Interoperability Standards, 75 Fed. Reg. 63462 ¶¶ 2-3 (Oct. 15, 2011).

[161] *See generally* NISTIR 7628 VOL. 2 PRIVACY GUIDELINES, *supra* note 6, at 1-39.

[162] *Id.* at 2-3.

[163] *Id.* at 40.

[164] NISTIR 7628 Vol. 2 Privacy Guidelines, *supra* note 6, at 40 (Chapter 5).

[165] *Id.* at 40-42.

practices.[166] According to NIST, entities should limit their collection, scope, use and retention of CEUD, while also allowing individual customers to access their CEUD.[167] Entities should also limit disclosure of data to other parties, and protect all data collected.[168]

E. Smart Grid Efforts at the State-Level

Various states have taken steps to implement Smart Grid programs and policies, including policies addressing Smart Grid data access and privacy issues such as data collection and third party service provider use of information. In California and Texas, for instance, lawmakers have started to address these issues through laws applicable to jurisdictional electric utilities.[169]

In California, legislation has been enacted that shifts liability to third party service providers once there is a transfer of Smart Grid data from a utility to a third party service provider. Under California Senate Bill 1476,[170] third party service providers would be held to the same standards as utilities.[171] In December 2008, the California Public Utilities Commission ("CPUC") instituted a rulemaking to determine policy in California's development of a Smart Grid system under EISA.[172] In its decision, the CPUC required investor-owned utilities to provide authorized third party service providers with access to a customer's real-time or near real-time usage information no later than the end of 2011.[173]

On May 6, 2011 the CPUC issued a Proposed Decision to protect the privacy and security of customer usage data generated by Smart meters deployed by Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company.[174] The decision also adopts policies

---

166 *Id.*

167 *Id.* at 40-41.

168 *Id.* at 41.

169 NISTIR 7628 VOL. 2 PRIVACY GUIDELINES, *supra* note 6, at 9-10.

170 *See* California S.B.1476 (2010) (Chapter 497, Statutes of 2010).

171 DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 55.

172 *See Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's Own Motion to Actively Guide Policy in California's Development of a Smart Grid System,* Decision 09-12-046 in Docket R.08-12-009 (Cal.Pub.Util.Comm., 2009).

173 *Id.* at 51, 65, 78.

174 *Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's Own Motion to Actively Guide Policy in California's Development of a Smart Grid System, Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company,* Proposed Decision of President Peevy Mailed May 6, 2011 in Docket R.08-12-009 (Cal.Pub.Util.Comm., 2011).

to govern access to customer usage data by customers and auathorized third parties and adopts a framework to allow customers to authorize third parties who agree to comply with the adopted privacy and security rules to reciev usage data directly from utilities.[175]

Several other states have taken steps to address Smart Grid data access and privacy issues, and to establish appropriate policies. The State of Texas requires utilities employing advanced metering to use industry standards in providing secure access to customer data, and to provide customers with access to their energy usage data. Texas and California also specifically prohibit the sale of customer-specific data.[176] California, New York, Pennsylvania and Texas each have established statutes or policies to ensure that consumers have access to energy information directly from Smart Grid technology.[177]

Colorado has initiated a proceeding to investigate security and privacy concerns related to Smart Grid deployment.[178] The Michigan Public Service Commission formulated "collaborative policies for Smart Grid privacy, data collection and third party" service provider data usage.[179] The Florida Public Service Commission has implemented policies and practices consistent with existing Florida customer privacy laws that preclude utilities from releasing customer-specific usage data to third party service providers without customer consent, unless otherwise provided by Florida or Federal law or pursuant to a valid subpoena.[180] The Louisiana Public Service Commission issued a General Order, effective September 22, 2009, implementing its *Rule for Approval and Cost Recovery for Advanced Metering System and Demand Response Programs.*[181]

---

[175] *Id.* at 2-3.

[176] *See* DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 55 (summarizing multiple comments filed in response to the DOE's request for information).

[177] Demand Response and Smart Grid Coalition, *Comments of the Demand Response and Smart Grid Coalition* 10 (Jul. 12, 2010), http://www.gc.energy.gov/documents/DRSG_Comments_DataAccess.pdf.

[178] *In re* The Investigation of Security and Privacy concerns regarding the Development of Smart-Grid Technology, Colorado Public Service Comm'n, *Order Seeking Comments and Information*, Docket 09I-593EG (Feb. 24, 2010).

[179] Re: U.S. Dep't. of Energy RFI Implementing the Nat'l Broadband Plan by Empowering Customers and the Smart Grid: Data Access, Third Party Use, and Privacy, *Comments of DTE Energy*, at 6 (July 12, 2010).

[180] Re: U.S. Dep't. of Energy RFI Implementing the Nat'l Broadband Plan by Empowering Customers and the Smart Grid: Data Access, Third Party Use, and Privacy, *Comments of Florida Power & Light Co.* (FPL), at 11 (July 12, 2010) [hereinafter *FPL Comments*], *available at* http://www.gc.energy.gov/documents/FloridaPowerLight_Comments_DataAcess.pdf.

[181] Louisiana Public Service Commission, *General Order*, Docket No. R-29213, R-29213 Subdocket A (consolidated) (Sept. 29, 2009); *see* Re: U.S. Dep't. of Energy RFI Implementing the Nat'l Broadband Plan by Empowering Customers and the Smart Grid: Data Access, Third Party Use, and Privacy, *Comments of Cleco Power, LLC.*, at 1 (July 12, 2010), *available at* http://www.gc.energy.gov/documents/clecopower_data.pdf.

General Order section 3.7 introduces provisions on the release of consumer data:[182]

> The utility is prohibited from transferring any customer-specific information from any AMS outside the customer-utility working relationship without prior [LPSC] approval. Summary data for reporting purposes to governmental, regulatory, and industrial groups in which individual customer data is clearly indivisible from the total would not apply to this restriction.

Some states are also relying on more generally applicable laws to address data privacy issues associated with the Smart Grid. California, Pennsylvania and Texas, for instance, require consumer consent before utilities can release consumer information to a third party service provider even in the absence of Smart Grid-specific legislation.[183] The District of Columbia limits the use of customer information to the use for which the information was originally acquired unless the customer consents in writing.[184] Rules established by the Michigan Public Service Commission governing electric and gas utilities generally, as well as Michigan's identity theft protection Act and Social Security Number Privacy Act could also be relevant to Smart Grid data privacy issues.

Several states have also implemented consumer protections against unfair and deception practices and privacy protections for customer data in other contexts. Numerous states have enacted anti-hacking statutes that prohibit unauthorized access to computers, including smart meters.[185] In addition, forty-five states have in place security breach notification laws that require notification of unauthorized access to personally identifiable information.[186] Similar laws are also in place in the District of Columbia, Puerto Rico and the United States Virgin Islands.[187]

IV. REGULATORY ISSUES

Policymakers and regulators recognize that the long-term success of the Smart Grid depends upon understanding and respecting consumers' reasonable

---

[182] Louisiana Public Service Commission, *General Order*, Docket No. R-29213, R-29213 Subdocket A (consolidated), (Sept. 29, 2009).

[183] *See* CHRISTOPHER WARNER, ET AL, CONSUMER PRIVACY POLICY (CPUC Smart Grid Rulemaking R.08-12-009 Consumer Privacy & Access Workshop) (Oct. 25, 2010) (providing a summary of various public utility codes that provide disclosure protections for the customer); *see* DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 16, 55; *see* CAL. PUB. UTIL. CODE § 8380(b)(1) (West 1994, Supp. 2011).

[184] D.C. Code § 34-1509(B)(1) (West 2006).

[185] *See, e.g.*, Cal. Penal Code §502(a) (2011); Ind. Code §35-43-2-3(b) (2011); Kan. Stat. Ann. §21-3755(b)(1)(A) (2011); Md. Code Ann. Crim. Law §7-203(c) (2011); Or. Rev. Stat. §164.377(2) (2009); Wis. Stat. §943.70(2) (2010).

[186] GINA STEVENS, CONG. RESEARCH SERV., R234120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS 2 (2010).

[187] *Id.*

expectations of privacy, security, and control over who has access to potentially revealing energy usage data.[188] Indeed, the practical impact of a Smart Grid depends on its ability to encourage and accommodate innovation while making usage data available to consumers and certain third party service providers in a responsible manner, and respecting individual consumer choices in how to balance the benefits of access to usage data against the protection of personal privacy and security.[189]

As the DOE recognized in its Data Access and Privacy Report, "privacy and access, in the context of a Smart Grid, must be viewed as complementary values rather than conflicting goals."[190] Although privacy is of tremendous importance to electricity consumers, so is access to the usage data which will enable them to understand their energy use, and thus become more efficient consumers of energy.[191] At the same time, access to the same consumer data is important to utilities' third party service providers for business and operational purposes and to achieve national energy and reliability goals that will be advanced by Smart Grid technologies.[192]

In attempting to maintain the proper balance between Smart Grid related privacy and access concerns, regulators and policymakers must address variations of three fundamental questions: First, who should have access to Smart Grid data? Next, how should the data be accessed? Finally, how should the privacy of the data be protected?

In wrestling with these questions, regulators and policymakers should be guided by five basic principles. First and foremost CEUD is entitled to privacy protection. Second, consumers must have access to and some control over the disclosure of their CEUD. Third, consumers are entitled to "timely, useful, and actionable information about how much energy is used, and what it costs."[193] Fourth, utilities and third party service providers have an obligation to protect CEUD from unauthorized and improper disclosure and use. Fifth, some form of this energy usage data should be available to third party service providers.

These principles, however, can only serve as the starting point in any analysis. There are several issues which in particular must be resolved to ensure the success of the Smart Grid and deployment of Smart Grid technologies on a

---

188 DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 2.

189 *Id.*

190 *Id.*

191 *Id.* at 2-3.

192 *Id.*

193 This is not meant to imply that the FCC was correct when it recommended that consumers have access to this data on a "real-time" basis. *See* DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 18. Because of the costs which are involved, that is a decision which is probably best made on a situational basis in the context of a state regulatory proceeding. *See* NATIONAL BROADBAND PLAN, *supra* note 1, at 11.

timely basis. Without proper regulatory guidance, consumers and businesses will be reluctant to disclose and share usage data,[194] and third party service providers will be limited in the services that they can provide.[195] Many of these issues are best addressed at the state level given the regulatory structure of the electric industry; however there is merit in achieving some degree of national uniformity on certain key issues.

Below is a discussion of some of the more fundamental, broad-based questions that would benefit from national guidance.

A. Who "Owns" Energy Consumption Data and Is the Issue of "Ownership" Relevant to Smart Grid Privacy?

Ownership of energy consumption data in the context of the Smart Grid presents a complex question that extends beyond "ownership" as a property right, and pertains more to issues of data access and usage. Importantly, "[d]ata ownership is traditionally governed by state law and varies on a state-by-state basis", distinguished by varying state regulatory structures.[196] In states with restructured energy markets, competitive service providers offering unbundled service options are required to meet established criteria prior to accessing customers' energy usage information.[197] States that retain a traditional vertically-integrated utility structure often take a different approach to data access issues. Varying regulatory structures raise different issues of data ownership, as do differing utility business models employed in different states.

Based on state regulatory structures, utility business models, the nature of the relationship between a utility and its customer, and the nature of the energy usage data itself, there are varying interests in consumption data. Energy usage data results from a contractual relationship between a utility and a customer based on the provision of energy service, and the interests between these parties must be fairly balanced. Energy usage data is initially collected by utilities who invest in infrastructure to deliver energy services to a customer, and utilities have, by statute, regulation or practice ownership interests in detailed electricity usage data resulting from this relationship. In addition, utilities undertake the risk and invest the capital to capture and manage energy usage data and therefore have an interest in the economic value of that data. Utilities also incur ongoing operating costs to transmit, manage and verify energy usage data. By enhancing and validating this data, utilities derive some sort of owner-

---

194 DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 8-9.
195 NATIONAL BROADBAND PLAN, *supra* note 1, at 256.
196 *See EEI Comments*, *supra* note 24, at 4.
197 *Id.*

ship interest in enhanced and validated customer-specific energy usage data,[198] as well as aggregated non-customer specific energy usage data.

On the other hand, customers have privacy rights associated with their individual customer-specific usage data. As important, they should have the right to use the data for their own purposes and benefit, including either providing to or allowing for the provision of the data to third parties. Moreover, the FCC is correct that while disruptive, competition from third parties will be beneficial and that third party access to data is important to facilitate this competition.[199]

These varying ownership interests and regulatory issues reveal that "ownership" of energy usage data is a difficult concept to parse, and one that will likely complicate efforts at the DOE and Federal and state agencies to reach conclusions on important privacy issues and to develop a framework for Smart Grid policy. Moreover, ownership of consumption data is not a critical issue for Smart Grid development. Regardless of who owns the energy consumption data, customers and their authorized third party service providers should have timely access to data from smart meters. The important policy issues for Smart Grid development is access to, usage and disclosure of energy consumption data, and involves such questions as what, how, when and to whom data should be made available; what privacy protections should apply; and how costs should be recovered.

B. What Rights Should Consumers Have to Access Energy Usage Data?

1. Right to Data Access and Privacy

Generally, all consumers of electricity should be able to easily and efficiently access their individual usage data from their electric utility reflecting the energy services they receive. While the nature of energy usage data provided to a consumer may vary depending on the technologies employed by that consumer, there is general consensus is that providing consumers with "actionable" data (*i.e.*, data that can be used to alter consumers' energy-use patterns to reduce their overall energy costs) is critical to implementation of Smart Grid technologies such as advanced metering.[200]

This right of access is best incorporated into customers' terms and conditions of service as developed by individual utilities pursuant to state regulatory

---

[198] "Customer Specific Energy Usage Data" includes all data specific to an individual customer's energy use (*i.e.*, total and time-differentiated energy and capacity use). *Id.* at 2, n.3.

[199] *See* NATIONAL BROADBAND PLAN, *supra* note 1, at 255.

[200] DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 11.

requirements or by voluntary industry frameworks.[201] Consumers access to usage information should include all information that their utility or metering authority collects (*i.e.*, kW, kWH, kVAR, etc.), and in the same validated (*i.e.*, billing-quality) form that the utility uses it. One issue in need of close consideration is whether the provision of raw, unaudited usage data should be made accessible to consumers directly from their meters. While direct consumer access to this form of usage data carries potential advantages, providing raw data to consumers could lead to billing confusion and introduce additional privacy and security issues.

Beyond this, there is also consensus is that all classes of consumers are entitled to privacy protections related to their individual energy usage data, as ensured under state consumer and privacy protection statutes.[202] Energy usage data can potentially disclose detailed information about behavior and activities of a particular household. As the DOE has recognized, "collection of this data raises privacy implications that should be acknowledged and respected."[203]

In most instances, privacy protection of energy information is mandated by state codes of conduct for utility practices. Consumers are entitled to have their utilities maintain the confidentiality of their account records, including information supplied voluntarily by consumers establishing service, and information related to a utility's supply of energy service as measured by the utility's meter. In addition, consumers that wish to maintain the privacy of data produced by consumer-supplied devices and appliances within their premises should have a right to undertake such privacy measures as appropriate for those purposes.

As discussed above, all classes of consumers must be assured that their energy usage data is adequately protected and will not be released to third party service providers without consumers' express approval. A recent survey of electric utility consumers concluded that "46 percent of respondents believe it is 'very important' that their electricity usage be kept confidential, 29 percent believe it is 'somewhat important,' and 79 percent believe only customers and their utilities should have access to smart meter information."[204] The importance of protecting consumers' energy usage data, then, cannot be overlooked

---

[201] The Administration recently endorsed a similar concept of using voluntary industry frameworks in its Cybersecurity Legislative Proposal. The proposal called for an approach under which "[c]ritical infrastructure operators would develop their own frame works for addressing cyber threats." *See* White House Fact Sheet: Cybersecurity Legis lative Proposal 3 (May 12, 2011), *available at* http://www.whitehouse.gov/sites/default/files/fact_sheetadministration_cybersecurity_legislative_proposal.pdf.

[202] *Id.* at 12.

[203] *Id.* at 9.

[204] *See EEI Comments*, *supra* note 24, at 9; Edison Electric Institute, *Public Opinion On Customers' Information Privacy* (June 9, 2010).

by policymakers or utilities. Consumer confidence in the protection of usage data from unauthorized third party service providers is critical to successful implementation of the Smart Grid, and necessary to avoid any potential consumer backlash which could derail, if not significantly delay, the implementation of the Smart Grid.

Different consumers will likely have different privacy needs. Some will be more sensitive about providing energy usage data to third party service providers, and will demand greater privacy protections. Other consumers will be more amenable to providing individual energy usage information to third party service providers to take advantage of one or more third party service provider Smart Grid applications and services. Privacy protections must be considered for more general consumer information and data that may be generated not only by smart meters, but also by HANs and devices connected directly for third party service provider access. Devices on a consumer's premises, which may be potentially connected to HANs, meters and the Internet raise additional concerns for consumers and regulators.

Similarly, the privacy needs of commercial and industrial consumers will differ based on the nature and size of their businesses. Commercial and industrial consumers will likely require confidentiality of energy usage information, so as to avoid potential competitive harm that might arise from the unauthorized dissemination of energy consumption and cost information. For these reasons, as discussed below, consumers' energy usage data and other proprietary information must only be properly disclosed to *authorized* third party service providers, with consumer consent, and through accepted and secure methods of data transportation. In all instances, however, the need for protecting consumer privacies must be carefully balanced with the need for promoting innovation of Smart Grid technologies.

2. Right to Control Use and Distribution of Usage Data

Consumers should decide whether and for what purposes any third party service provider should be authorized to access or receive energy usage information. As noted by DOE, "[c]onsumer control of third-party access to [energy usage information] would promote the development of a competitive, open, transparent, and innovating marketplace for the use and management of energy-consumption data.[205]

This arrangement translates into the right of consumers to decide on an individual and case-by-case basis which parties, if any, may receive their data. A similar process is seen in the FCC's rules regarding use of, and access to

---

[205] DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 11.

CPNI.[206] The FCC has created rules which allow customers to "opt in " to third party access for telephone and Internet companies, in addition to rules for accessing CPNI information.[207] The FCC further mandates specific notice requirements prior to certain uses of CPNI.[208] Such rules of procedures enable customers to make reasonable and informed choices about access to, and use of CPNI. Applying a comparable process to manage access to consumers' energy usage information would benefit the protection of potentially sensitive data.

As noted above, different consumers will likely desire different degrees of access to usage data: some may permit access by multiple parties to broad portions of their data, including HAN data, while other customers may prefer to be more restrictive in granting data access. Similarly, some states and their consumers may wish to allow third party service providers to transmit data from the meter to other devices. To provide adequate safeguards empowering consumers' rights to control the use and distribution of energy data, and to account for different degrees of data access, an "opt-in" approval process for information sharing with third party service providers may be the most effective approach for protecting consumer privacy interests. Notably, however, consumer rights to control data use become increasingly complicated once data leaves a utility meter en route elsewhere than to a utility. In these instances it is unclear whether state regulators or utilities will be able to control how such data is subsequently used or distributed.

3. Relevant Privacy Standards and Utility Obligations

Robust standards and requirements that both ensure consumer access to energy information and protect consumers' expectations of privacy are essential to a successful and vibrant Smart Grid. Different types of usage data demand

---

[206] *See* 47 C.F.R. § 64.2007 (2009). CPNI means:

(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.

See 47 C.F.R. § 64.2003(g). Pursuant to FCC rules, RBOCs "may use disclose, or permit access to CPNI for the purpose of providing . . . service offerings among the categories of service . . . to which the customer already subscribes from the same carrier, without customer approval." 47 C.F.R. § 64.2005(a) (2009).

[207] *See* 47 C.F.R. § 64.2007 et seq. (2009). *See EEI Comments, supra* note 24, at 23.

[208] *See* 47 C.F.R. § 64.2008(a) (stating the notice requirement "for use of customer proprietary network information").

different privacy practices and standards, and may be subject to different regulations at the Federal Trade Commission ("FTC") and other agencies. NIST has undertaken a review of how different types of data are treated by various parties, including regulatory agencies and industry stakeholders.[209] In developing privacy standards, access to certain types of data and related custodial duties must be consistent. For these reasons, it makes sense to establish a clear definition of "data" as it relates to "energy consumption data." NIST's guidance and recommendations may be a useful starting point for regulators, to prevent development of standards or definitions that might be inconsistent with other data treatment practices.

Often, the "front line" for energy information and privacy protection is at the utility level, where energy usage data is collected and used by utilities to carry out their core business of safely and reliably providing energy services. Utilities typically employ stringent data privacy practices as required under state regulation, and under corporate governance requirements of the Securities and Exchange Commission and Sarbanes-Oxley.[210] However, certain additional protections at the utility level are warranted to safeguard the privacies and energy usage information of electric utility customers.

Comprehensive protections for use of energy usage data should be developed, as well as safeguards on disclosure of data. Energy usage information from smart meters should only be shared with third party service providers with customer consent, and through accepted and secure methods of data transportation. To effectuate these levels of privacy, utilities should develop policies for treatment of energy usage data that are available to utility customers. Utilities should also protect against loss, theft and unauthorized access of usage data, and should not release data to third party service providers absent affirmative customer authorization. In addition, third party service providers with customer authorization to receive energy usage data should be required to obtain explicit customer approval prior to reselling or distributing that data. To the extent possible, these privacy protections should follow the usage data, and authorized third party service providers should equally be responsible for protecting data, and liable for unauthorized access or intellectual property infringement that may occur.

Monitoring and compliance programs at the utility level are essential to ensure compliance with data policies, and assign responsibilities to appropriate personnel with sufficient authority to ensure that data policies are documented, followed and updated as needed, and that internal training and other awareness activities are conducted regularly. Such utility-implemented programs must

---

[209] SGIP GUIDELINES, *supra* note 167, at 8-17.

[210] Sarbanes-Oxley Act, 15 U.S.C. § 7241(a)(4) (2006).

also be consistent with applicable regulatory requirements. To protect consumers' privacy interests in usage data, third party service providers should be subject to similar obligations to ensure consistent treatment of data and privacy protections.

Prior to disclosure of usage data, consumers should be provided with certain information to allow for reasoned and intelligent choices about how their energy usage data is accessed. Consumers should be informed of the types of information that will be collected, from what devices and for what specific purposes; the frequency with which a utility will take meter readings; and the retention period for all information collected and for what purposes. Consumers should also be provided with educational information, such as an explanation of the details of possible information that could be provided to a third party service provider after customer authorization.

To protect consumer privacies, consistent procedures for verification of third party service providers must be developed, as well as clear policies for obtaining customer authorization for release of information to authorized third party service providers. State regulatory agencies are well-positioned to develop such standards, and should look to FCC rules guidance. In particular, the FCC rules establish safeguards for use of customer-specific information including, among other things, records retention requirements for all CPNI disclosures to third party service providers.[211] The FCC also mandates safeguards against unauthorized disclosure of CPNI, and requires telecommunications carriers to take "reasonable measures" to discover and protect against unauthorized disclosures.[212]In addition, the FCC instituted procedures for notifying law enforcement in the event of unauthorized access to CPNI.[213]

As noted above, pursuant to EISA, NIST has evaluated existing privacy standards, principles and practices, and new privacy exposures that may be created in Smart Grid environments, and has identified practices to best meet these new exposures. NIST's work and recommendations are documented in Chapter 5 ("Privacy and the Smart Grid") of NISTIR 7628. The NISTIR includes a series of recommendations for all entities that participate within the Smart Grid:[214]

---

[211] *See* 47 C.F.R. § 64.2009 (2009). The FCC requires records of disclosure or access to be kept for a minimum of one year, and contain specific information.

[212] *See* 47 C.F.R. § 64.2010. The FCC further requires "telecommunications carriers [must] properly authenticate a customer prior to disclosing CPNI" to that customer. The FTC struck a similar approach with its Fair Information Practice ("FIP") Principles. *See* FTC STAFF REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[213] *See* 47 C.F.R. § 64.2011(a) (2009).

[214] NISTIR 7628 VOL. 2 PRIVACY GUIDELINES, *supra* note 6, at 40-42 (Chapter 5).

(1) Conduct a privacy impact assessment ("PIA") upon making the decision to deploy and/or participate in the Smart Grid to identify privacy risks/exposures. Update the PIA whenever major changes may affect privacy;

(2) Develop and document formal privacy policies to:
   a. Assign staff responsible for privacy policy implementation;
   b. Notify customers, before data collection, what data is being collected and how it will be used;
   c. Describe to customers their choices in collection and use of their data;
   d. Ensure that only data necessary for purposes indicated in the customer notification is collected;
   e. Ensure that customer information is only used for the purposes it was collected, only retained as long as needed for those purposes, and is not shared with other parties without explicit customer consent;
   f. Ensure customers' ability to access, update and correct their own data;
   g. Ensure that customer-specific information is protected from loss, theft, unauthorized access, inappropriate disclosure, etc.;

(3) Employ privacy use cases to address identified exposures or problems;

(4) Educate consumers about privacy exposures and privacy protection options;

(5) Share among utilities and commissions solutions to common privacy problems;

(6) Limit data collection by smart appliances and other devices to only data needed for purposes of smart device operation.

These NIST recommendations offer a useful starting point. Ultimately, transparency and coordination of privacy standards between utilities, state regulators, federal agencies and other various parties is critical for successful implementation of Smart Grid data access and privacy standards and, in turn, long-term success of Smart Grid technologies. Privacy issues must also be addressed in a way that balances the need for data privacy with utility obligations to serve consumers safely and reliably.

Smart Grid services and technologies are evolving, and it remains uncertain precisely what types of services will be available to consumers. Different types of Smart Grid technologies will demand different mechanisms to empower customers to make reasonable privacy choices. For example, as the HAN market develops, either a utility-offered HAN solution, or a solution offered through the open market may develop. Mechanisms empowering consumers would vary greatly based on how and where HAN markets develop. Therefore, to decide on specific mechanisms for privacy and data access preferences at

this stage in the game would be premature. While consumer privacy is critical to a successful Smart Grid, rigid requirements to accomplish privacy goals are not in the public interest. A priority should be to develop privacy practices that are transparent for consumers, third party service providers and utilities, and that facilitate, rather than impede, Smart Grid development.

C. What Rights Should Third-Party Service Providers Have to Access Smart Grid Data and What Obligations Should Be Imposed Upon Them Regarding the Protection and Use of the Data?

The question of how "the interaction between third-party firms and regulated utilities be structured to maximize the benefits to consumers and society" is a critical one.[215] This however is not the first time that this nation's utilities and their regulators have had to deal with questions of regulating competitive entry in a manner that protects consumers but does not stifle either competition or innovation. In the electric industry fourteen states have "retail choice" laws and regulations permitting energy service companies to provide local service.[216] Similarly, in telecommunications entry by competitive local exchange companies ("CLECs") is widespread.[217]

Typically, these companies are required to be certified by state public service commissions which inquire into an entity's integrity, background, and financial stability. Many times this examination, while thorough, is less than what is required of companies applying to be full service utilities. Moreover, while somewhat onerous, obtaining certification in the fifty states plus the District of Columbia and Puerto Rico is feasible.[218] Once certified, with a consumer's authorization, these companies are permitted to access and use customer data as part of their provision of service. In general, incumbents are not permitted to favor their own affiliates.

As noted by DOE, there is broad consensus that when authorized by consumers, third party service providers should have access to at least the same type of CEUD that is available to the consumer.[219] To do otherwise would at a minimum potentially stifle innovation.[220]

---

[215] *See* Addressing Policy and Logistical Challenges to Smart Grid Implementation, DOE Request for Information, 75 Fed. Reg. 57006, 57010 (Sept. 17, 2010).

[216] *See, e.g.*, Md. Code Ann., Pub. Utils. § 7-507 (LexisNexis 2010) (engagement in the business of electricity supplier, limitations).

[217] For a description of competitive entry in the telecommunications market *see* H. Russell Frisby, Jr. & David A. Irwin, *The First Great Telecom Debate of the 21st Century*, 15 COMMLAW CONSPECTUS 373 *et. seq.* (2007).

[218] DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 22-23.

[219] *Id.* at 11.

[220] This article will not address potential antitrust concerns, particularly in light of the U.S. Supreme Court's decision in Verizon Commc'ns. Inc. v. Law Offices of Curtis V. Trin-

The previous section discussed how consumers may control the use and distribution of data and the obligations of utilities to protect the data. Once consumers have authorized third party service providers to access their data and this information is in the possession of the third party service providers, these entities should be subject to the same requirements regarding the protection and use of the data as are incumbent utilities.[221] As NIST correctly pointed out, "regardless of data ownership, the management of energy data that contains or is combined with personal information or otherwise identifies individuals, and the personal information derived from such data, remains subject to...privacy considerations."[222] Under such circumstances the "custodian of energy data" regardless of whether the entity is a utility or a third party service provider has an obligation to manage and safeguard the data.[223]

As noted previously, almost all utilities follow data access, disclosure and protection policies either in accordance with or mirroring state codes of practice.[224] There is no reason why third party service providers should not follow or be subject to the same requirements. This would in no way hinder their ability to compete in a state. It would be dangerous, if not pure folly, to subject utilities to one strict set of standards and third party service providers to a more "general" standard.[225] This is particularly the case because the Internet permits providers to access this information from anywhere in the world.

To the extent that a public service commission has authority to require third party service providers to be certified prior to offering service, it could subject the providers to the appropriate privacy rules. Otherwise, federal guidance either through collaboration or otherwise will be necessary.[226]

No discussion of third party service provider access to Smart Grid data would be complete without addressing the issue of third party service provider responsibility for the utility's costs of processing and providing the data to them. In this regard, DOE asks two important questions. First "[c]an utilities charge a fee for providing third party service provider access to CEUD?"[227] Second "[i]s it more appropriate to spread the costs associated with providing third party service provider access to CEUD among all utility customers, or only among those customers who authorize third party service provider access

---

ko, LLP, 540 U.S. 398, 410 (2004).

221 DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 15.

222 NISTIR 7628 VOL. 2 PRIVACY GUIDELINES, *supra* note 6, at 9.

223 *Id.*

224 *See* discussion *supra* Part IV.B. *See also* DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 55-56.

225 *See, e.g.*, DATA ACCESS AND PRIVACY REPORT, *supra* note 12, at 15.

226 *Id.* at 23.

227 *Id.* at 21.

to CEUD?"[228] Since as noted previously, there is no clear answer to the question of who owns the data, it is entirely appropriate that to the extent that third party service providers cause additional costs to be incurred, and then use the data for their commercial purposes, they pay an appropriate share of the costs.

In its discussion of this issue, DOE correctly noted that "[s]ound economics and public policy suggest that an entity causing particular costs should pay for those costs so that these entities do not demand the good without appreciating its true cost."[229] This reflects the well established principle in utility ratemaking that a regulatory body "treats consumers and investors fairly and equitably when it allocates cost to those who have caused the costs to be incurred."[230] The cost of the information is not "free" to consumers, but is included in utility rates.[231] To the extent that third party service providers are not required to cover any additional costs resulting processing third-party service provider authorizations and providing data to them, then these costs would be passed on to all utility ratepayers regardless of whether they used the services of the provider. Consequently, in answer to DOE's second question, it is inappropriate to spread the costs associated with providing third-party service provider access to CEUD among all utility customers. Instead, those costs should be borne by the third party service providers and their customers. This result is fair to consumers, particularly those populations which may prove to be late adopters of Smart Grid services for economic and other reason. Moreover, appropriately regulated by state commissions, this will not stifle either market entry or innovation.

V. CONCLUSION

As noted at the outset of this article, the deployment of Smart Grid technology offers tremendous potential in a wide variety of areas. At the same time this deployment also raises a number of complex privacy issues. If the potential of the Smart Grid is to be realized it is important that a national consensus be reached early on with regard to a number of fundamental data access, privacy and security issues.

Policymakers and regulators should be driven by five fundamental principles. First, CEUD is entitled to privacy protections. Second, consumers should

---

[228] *Id.* at 22.

[229] *Id.*

[230] LEONARD S. GOODMAN, THE PROCESS OF RATEMAKING VOL. 1, 380 (Public Utilities Reports, Inc. 1998).

[231] A utility's cost of service "encompasses all cash and non-cash outlays for the operations of the regulated business" including costs "involved in creating or performing a service-related activity or function." *Id.* at 279, 280. Consequently utilities are entitled to recover for the costs of service-related activities such as processing and providing data.

have access to and control over the disclosure of their energy usage data. Third, consumers are entitled to timely, useful, and actionable information about how much energy is used, and what it costs. Fourth, usage data should be protected from unauthorized and improper disclosure and use. Fifth, some form of this usage data should be available to third party service providers.

In the context of these principles, the question of who owns the data is irrelevant. Instead, the fundamental questions ask who has access to the data, how the data is accessed and used, and how the data is protected. Consumers, utilities and authorized third party service providers should have controlled access to the Smart Grid data. In particular, except for data needed for utility operational purposes, consumers should have the right to control disclosure of their CEUD. Further, utilities and authorized third party service providers should have a mandatory obligation to protect consumer privacy and to control unauthorized disclosure and use of the information. To this end, the FCC's CPNI rules provide a useful model. Finally, along with the right to access data, must come the obligation for third party service providers to use and protect the data in a manner similar to the obligations imposed on utilities, as well as pay the appropriate costs. Hopefully, with these principles in place, as a nation we can quickly and safely enjoy the benefits of the Smart Grid.