THE ROLE OF NON-UTILITY SERVICE PROVIDERS IN SMART GRID DEVELOPMENT: SHOULD THEY BE REGULATED, AND IF SO, WHO CAN REGULATE THEM?

ANDREAS S. V. WOKUTCH*

* J.D., University of Colorado Law School (2011) and Associate Editor, University of Colorado Law Review. I am grateful for the helpful comments of Professor Paul Ohm, Professor Brad Bernthal, and the editorial board of the JTHTL, which benefited this Note. I would also like to thank Professor William Boyd, Eli Quinn, Mark Walker, and David Mohler for serving as soundboards in my search for the topic of this Note. Lastly, this Note is dedicated to Rich, Mary Ellen, Caitlin, and Seema. Without your support and encouragement over the past three years, this Note would not have been possible. Thank you.

INTRODUCTION

Enormous commercial interest surrounds the idea of modernizing the U.S. electric grid[1] via modern digital technology, more commonly known as creating the "smart grid."[2] This interest is evidenced by the staggering amount of capital that continues to flow toward this end. The smart grid market is estimated to grow from $20 billion in 2009, to $42 billion in 2014,[3] and possibly to $100 billion by 2030.[4] Additionally, the federal government has declared the modernization of the grid to be a priority for the U.S.[5] and has allocated $3.4 billion in grants to smart grid development projects.[6] This tremendous public and private investment in the smart grid has led to the development of many products and services that promise to transform and modernize the grid in myriad ways. However, these avenues of modernization significantly complicate the regulation of the electric grid by blurring jurisdictional boundaries that already lack clarity. As a result, regulators are less able to quickly and adequately address issues that arise with smart grid development. This

1. Referred to interchangeably in this Note as "electric grid" or "grid."

2. This paper will refer to modernization of the electrical grid as "smart grid development." *See generally* LITOS STRATEGIC COMMC'N, U.S. DEP'T OF ENERGY, THE SMART GRID: AN INTRODUCTION 2 (2008).

3. *U.S. Hardware and Software Companies Should Prepare to Capitalize on the Smart Grid in the U.S. and in International Markets*, ZPRYME RES. & CONSULTING (Dec. 2009).

4. *Wiser Wires*, ECONOMIST, Oct. 10, 2009, at 71 (citing a prediction by Morgan Stanley); *see also* ELEC. POWER RESEARCH INST., POWER DELIVERY SYSTEM OF THE FUTURE: A PRELIMINARY ESTIMATE OF COSTS AND BENEFITS 5-1 (2004) (stating that investment in the smart grid is likely to reach $165 billion by 2024).

5. Energy Independence and Security Act of 2007 § 1301, 42 U.S.C.A. § 17831 (2010).

6. These funds were made available by the American Reinvestment and Recovery Act of 2009. *Smart Grid Investment Grant Awards*, DEP'T OF ENERGY, http://www.oe.energy.gov/recovery/1249.htm (last visited Feb. 11, 2011).

Note analyzes one such issue: the lack of clear jurisdictional authority to regulate the direct interactions between consumers and non-utility companies that offer smart grid products and services ("non-utility service providers" or "NUSPs"). This lack of regulatory authority is significant because inadequate oversight of these interactions raises substantial security and privacy concerns. Accordingly, this Note analyzes this issue in Part I by giving a brief overview of what smart grid development entails. Part II explains the security and privacy concerns of NUSPs developing the smart grid by interacting directly with consumers, and determines that these concerns are substantial enough to require regulation. Part III explores which entities have authority to regulate these interactions and determines that none do. Lastly, Part IV analyzes which entity should be given authority to regulate NUSP-consumer interactions, and concludes that the most appropriate solution is to extend the Federal Energy Regulatory Commission's ("FERC") current jurisdictional authority.

I. OVERVIEW OF SMART GRID DEVELOPMENT

As stated above, the idea of modernizing the U.S. electric grid via modern digital technology is referred to as creating the "smart grid" or "smart grid development."[7] Although there are wide differences between the seemingly endless number of new and developing smart grid products and services that purport to further this end, each generally involves the application of digital technology to the grid to enable real-time coordination of electric data.[8,9] Additionally, these products and services commonly seek to accomplish one or more recognized goals of smart grid development. These goals were laid out by the Energy Independence and Security Act of 2007 ("EISA") and include: (1) the use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid, (2) integration of distributed resources and electric generation, including renewable resources, (3) deployment of "smart" digital technologies that optimize the operation of appliances and consumer devices through real-time monitoring, automation, and

7. *See supra* notes 1-2.

8. *Smart Grid*, FED. ENERGY REG. COMM'N, http://www.ferc.gov/industries/electric/indus-act/smart-grid.asp (last updated Feb. 2, 2011); *see also* DON VON DOLLEN, ELEC. POWER RESEARCH INST., REPORT TO NIST ON THE SMART GRID INTEROPERABILITY STANDARDS ROADMAP 6 (2009) (defining the smart grid as the "two-way flow of electricity and information to create an automated, widely distributed energy delivery network").

9. It is very difficult to speak about smart grid technologies as a group because there is such a wide range of services, products, and business models currently in use or in development. Invariably some technology falls outside a given generalization. However, this fact should not reduce the value of this Note's findings in relation to those technologies that it does encompass.

user interaction capabilities, and (4) provision of timely electric information and control options to consumers.[10] While these goals add some commonality between different smart grid products and services, the development of an advanced metering infrastructure ("AMI") is considered the keystone to achieving the goals of the smart grid.[11]

AMI is a metering system that almost exclusively uses digital technology to record "customer consumption (and possibly other parameters) hourly or more frequently and provides for daily or more frequent transmittal of measurements over a communication network to a central collection point."[12] Like most methods of modernizing the grid, AMI has many applications. However, two applications have emerged as the predominant foci: first, using advanced metering devices at the distribution level to create better communication between electric utilities and (usually) residential consumers, and second, supplying advanced metering products and services directly to consumers by NUSPs.[13] While both utility and non-utility products and services will likely have a role in the development of the smart grid, non-utility services may create some particularly difficult regulatory issues. Because it is unclear that any entity can effectively and comprehensively regulate interactions between consumers and NUSPs, leading to security and privacy concerns, this second category is the focus of this Note.[14]

II. WHY NUSP-CONSUMER INTERACTIONS SHOULD BE REGULATED

Commentators note that there are many cyber security and privacy concerns related to the development of the smart grid.[15] These concerns

10. Energy Independence and Security Act of 2007 § 1305, 42 U.S.C.A. § 17385 (2010).

11. *See* LITOS STRATEGIC COMMC'N , *supra* note 2, at 11 (describing two-way digital communication as a key function of the smart grid, which is made possible by AMI's ability to allow electricity price-signals to reach consumers); OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, ADVANCED METERING INFRASTRUCTURE 2 (2008).

12. FED. ENERGY REGULATORY COMM'N, ASSESSMENT OF DEMAND RESPONSE AND ADVANCED METERING vi n.2 (2008).

13. *See, e.g.*, *What Is TED?*, ENERGY, INC., http://www.theenergydetective.com/what/overview.html (last visited Feb. 11, 2011); *Products*, ALERTME, http://www.alertme.com/products (last visited Feb. 11, 2011).

14. *See infra* Part II.

15. *See, e.g.*, SMART GRID INTEROPERABILITY PANEL – CYBER SEC. WORKING GRP., NAT'L INST. OF STANDARDS & TECH., GUIDELINES FOR SMART GRID CYBER SECURITY STRATEGY AND REQUIREMENTS 8, 111-12 (2010) [hereinafter NISTIR DRAFT FEB. 2010]; *see also* Investigation of Sec. & Privacy Concerns Regarding the Deployment of Smart Grid Tech., *Order Opening Docket, Establishing Procedures & Dates, & Seeking Comments & Information*, Colo. PUC Dkt. No. 09I-593EG, 2009 WL 2751604, at 2 ¶ 5 (Aug. 12, 2009) [hereinafter Investigation]; Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies* 9-11 (Working Paper Series, 2009).

have largely been evaluated with the presumption that smart grid development would be subject to regulation. However, it is not clear that this is true regarding NUSP-consumer interactions, potentially making these concerns more significant. This Part illustrates the magnitude of the risk associated with inadequate regulation of NUSP-consumer interactions by providing background information on NUSPs and the cyber security and privacy concerns created by their interactions with consumers. Section A explains what NUSPs are and how they provide smart grid products and services directly to consumers. Then, Section B describes the cyber security and personal privacy concerns that emerge when NUSPs provide smart grid products and services to consumers.[16]

A. What are NUSPs and How Do They Interact with Consumers?

NUSPs interact directly with consumers by bypassing a consumer's electric utility and providing smart grid products and services ("non-utility services") directly to the consumers. NUSPs are able to avoid the involvement of the consumer's utility by relying on the consumer to provide electric usage data that the NUSP otherwise would need to obtain from the consumer's electric utility.[17] The two main examples of non-utility services are electric efficiency analysis ("EEA") and energy management, both of which are discussed below. These services are provided by NUSPs to consumers via many interfaces including advanced metering devices, Web portals, software, and home area networks ("HANs").[18,19]

EEA is a non-utility service that provides consumers with an analysis of their electricity usage, and in turn allows consumers to identify and eliminate energy sinks.[20] In effect, EEA provides consumers with the information necessary to correct electrical inefficiencies and

16. While this Note explains the privacy concerns related to NUSPs and details the regulatory framework surrounding them, it does not delve into the issue of how privacy concerns should be treated by NUSPs and regulators.

17. Some NUSPs collect electric usage data from electric utilities. However, this Note focuses on NUSPs that collect electric usage data directly from consumers because these services are less likely to fall under state PUC jurisdiction as they are farthest removed from the electric utility.

18. HANs are defined as the "network[s] between the advanced meter and the home device[s]" within an advanced metering system, which includes advanced meters, the associated hardware, and software and communications systems. PUB. UTIL. COMM'N OF TEX., GLOSSARY 2 (2009).

19. For more information about other non-utility services, *see* Quinn, *supra* note 15, at B-6 to -8 (noting that other uses of electric usage data include insurance premium calculation, marketing research, and national security and law enforcement).

20. Energy sinks are defined as "anything that collects a significant quantity of energy that is either lost or not considered transferable in the system under study." *Flow of Energy*, CONNEXIONS, http://cnx.org/content/m16468/1.3 (last modified Sept. 25, 2009).

lower electric bills. Two examples of EEA are Google's PowerMeter[21] and Microsoft's Hohm, which both provide EEA through a Web portal interface using online software.[22] PowerMeter enables consumers to monitor their electricity usage[23] by allowing them "to view their home's energy consumption from anywhere online."[24] To monitor electricity usage, the software must receive electric usage data from the consumer's home. This could be accomplished by receiving data from a smart meter installed by a consumer's electric utility. However, PowerMeter bypasses the utility by receiving data directly from the consumer. This is done by providing the consumer with a device to install in his or her home that can collect data.[25] Alternatively, EEA can be performed without installing any sort of advanced meter. Microsoft's Hohm accomplishes this by requiring a consumer to manually enter certain energy-related information onto an online software program, which in turn provides efficiency suggestions[26] based on the consumer's "specific household circumstances including home attributes and use of appliances and systems."[27]

The other main non-utility service, energy management, usually includes EEA as part of the service, but takes EEA a step further by also providing a management system for a consumer to control electric usage throughout the residence.[28] Two examples of energy management, among others,[29] are AlertMe.com, Ltd.'s AlertMe Energy ("AlertMe")

21. *Google PowerMeter*, GOOGLE, http://www.google.org/powermeter (last visited Feb. 11, 2011).

22. *Help*, MICROSOFT HOHM, http://www.microsoft-hohm.com/Info/Help.aspx (under "Frequently Asked Questions" select "What is Hohm?") (last visited Feb. 11, 2011).

23. *See Google PowerMeter*, *supra* note 21. Other notable Web-based load management products/services are Silver Spring Network's Greenbox, *see Products*, SILVER SPRING NETWORKS, http://silverspringnetworks.com/products/index.html (last visited Feb. 11, 2011), and Agilewaves' Resource Monitor, *see Products*, AGILEWAVES, http://www.agilewaves.com/products (last visited Feb. 11, 2011).

24. *Google PowerMeter Frequently Asked Questions*, GOOGLE, http://www.google.org/powermeter/faqs.html (last visited Feb. 11, 2011).

25. *See infra* text accompanying notes 33-34; *see also supra* note 13.

26. Software load management serves the same purpose as Web portal load management services except that the software is not located online. Notable companies providing this type of load management include IBM and Cisco Systems who have combined their Tivoli software and EnergyWise company-wide energy management services, respectively. *EnergyWise Technology*, CISCO, http://www.cisco.com/en/US/solutions/ns726/intro_content_energywise.html (last visited Feb. 11, 2011).

27. *Help*, *supra* note 22.

28. "[E]nergy management is the process of monitoring, controlling, and conserving energy . . . ." *The What, Why, and How of Energy Management*, BIZEE ENERGY LENS, http://www.energylens.com/articles/energy-management (last visited Feb. 11, 2011).

29. *See* Jeffrey Lee, *Real Time Feedback*, ECOHOME (Feb. 6, 2009), http://www.ecohomemagazine.com/home-technology/real-time-feedback.aspx (noting Blueline Innovations' PowerCost Monitor and Control4's home controller as other non-utility

and Energy, Inc.'s The Energy Detective ("T.E.D.").[30] Both AlertMe and T.E.D. provide EEA to consumers through the installation of an advanced metering device in a consumer's home, which collects electricity usage data for the residence.[31] After collecting this data, AlertMe, and to a lesser extent T.E.D., helps consumers improve electric efficiency by allowing them to better control energy use in their home.[32] Installation of T.E.D. requires connecting hardware to the residence's circuit breakers and then plugging an LCD display into an electric socket.[33] AlertMe operates differently, requiring attachment of hardware onto the actual electric meter and setting up a broadband hub that collects usage data and transmits it over the Internet.[34] Both of these products bypass the electric utility. Additionally, both companies supplying these products have joined in a partnership with Google,[35] whereby their devices provide consumers with energy management service and Google's PowerMeter provides the EEA.[36]

Lastly, energy management is also provided by a broad category of products referred to as HANs. HANs are networks that come in many forms; one formal definition describes them as the "network[s] between the advanced meter and the home device[s]" within an advanced metering system, which includes advanced meters, the associated hardware, and software and communications systems.[37] HANs are essentially networks within a consumer's home that connect home appliances with heating, cooling, and lighting systems via an interface such as a website, software, or hardware.[38] Through this portal,

energy management service providers); *see also* Katie Fehrenbacher, *How Apple Could Jolt the Smart Home Energy Market*, GIGAOM (Jan. 17, 2010, 5:19 PM), http://earth2tech.com/2010/01/17/how-apple-could-jolt-the-smart-home-energy-market; Katie Fehrenbacher, *Intel Developing Home Energy Management Concept Gadget*, GigaOM (Sept. 24, 2009, 1:01 PM), http://earth2tech.com/2009/09/24/intel-developing-home-energy-management-concept-gadget.

30. *See What Is TED?*, *supra* note 13.

31. *How It Works,* ALERTME, http://www.alertme.com/products/energy/how-it-works (last visited Feb. 11, 2011); *What Is Ted?*, *supra* note 13.

32. *Id.*

33. *How Do I Install TED?,* THE ENERGY DETECTIVE, http://www.theenergydetective.com/what/install.html (last visited Feb. 11, 2011).

34. *Getting Started,* ALERTME, http://www.alertme.com/help/getting-started (last visited Feb. 11, 2011).

35. Katie Fehrenbacher, *Google's PowerMeter Links with AlertMe, UK Utility*, GIGAOM (Oct. 28, 2009, 7:29 AM), http://earth2tech.com/2009/10/28/googles-powermeter-links-with-alertme-uk-utilility.

36. Katie Fehrenbacher, *How Google's PowerMeter Will Affect the Smart Grid Industry*, GIGAOM (Feb. 11, 2009, 12:00 AM), http://earth2tech.com/2009/02/11/how-googles-powermeter-will-affect-the-smart-meter-industry.

37. PUB. UTIL. COMM'N OF TEX., GLOSSARY, *supra* note 18.

38. *Home Area Networks*, BURNS & MCDONNELL, http://www.burnsmcd.com/portal/page/portal/Internet/Service/Electrical_Transmission_and_Distribution1/SmartGrid/Home%20Area%20Network (last visited Feb. 11, 2011).

consumers can obtain real-time information about the total energy use of their home and can make changes to this use in various ways.[39] Examples include automating energy use so that energy will only be used during periods of the day with the lowest prices, and programming appliances, heating, cooling, and distributed generation systems (e.g. solar panel displays) to operate as efficiently as possible.[40] HANs, like other energy management services, rely on obtaining electric usage data from some sort of advanced meter (utility or non-utility installed).[41] Although this meter can be installed by a utility or a NUSP, only HANs that utilize electric usage data gathered from the consumer without involving the consumer's electric utility are relevant to this Note.

B. Cyber Security and Privacy Concerns of NUSP-Consumer Interactions

While the smart grid promises to increase the efficiency and reliability of the electric grid, it may also increase cyber security concerns for the grid and privacy concerns for consumers.[42] This Section outlines the scope of each of these concerns and highlights how they may be exacerbated by NUSP-consumer interactions.

1. Cyber Security Concerns

Understanding cyber security concerns requires a basic understanding of prevailing terminology. Cyberspace is defined as an "interdependent network of information technology infrastructures"[43] including "the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[44] Broadly, cyber security is the protection of these infrastructures.[45] More formally, cyber security is "the protection required to ensure confidentiality, integrity, and availability of the electronic information communication system."[46]

---

39. *Id.*

40. Lynne Kiesling, *Intelligent End-Use Devices Make a Transactive Smart Grid Valuable (Part 3 of 5)*, KNOWLEDGE PROBLEM (Mar. 4, 2009, 7:41 PM), http://knowledgeproblem.com/2009/03/04/intelligent-end-use-devices-make-a-transactive-smart-grid-valuable-part-3-of-5.

41. *Smart Meters and Home Area Networks*, SAN DIEGO GAS & ELECTRIC, http://www.sdge.com/smartmeter/homeAreaNetwork.shtml (last visited Feb. 11, 2011).

42. *See generally* Investigation, *supra* note 15.

43. U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE iii (2003).

44. Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 125 (2009) (quoting DEP'T OF DEF., DICTIONARY OF MILITARY AND ASSOCIATED TERMS 141 (2001)). *See* DEP'T. OF DEF., DICTIONARY OF MILITARY AND ASSOCIATED TERMS 92 (2010).

45. *See* NISTIR DRAFT FEB. 2010, *supra* note 15, at 9-10.

46. *Id.* at 10; *see also* BRUCE S. SCHAEFFER ET AL., CYBER CRIME AND CYBER

Recently, the National Institute of Science and Technology ("NIST") has called for a more inclusive definition of cyber security in relation to the development of the smart grid.[47] The NIST proposes expanding the definition of cyber security in relation to the smart grid to include "both power and cyber system technologies and processes in [information technology] and power system operations and governance."[48] The NIST's desire to develop a more precise definition of cyber security is part of its development of cyber security standards for the smart grid.[49] These standards are recognized as critical to the protection of the U.S. economy, which depends on the proper functioning of the information technology ("IT") infrastructure and power system.[50]

The federal government officially recognized the need for strong cyber security standards in 2003, when such standards were deemed necessary to eliminate the risk of "organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security."[51] In turn, cyber security emerged as a concern with the development of the smart grid because the smart grid relies heavily on software and networks to achieve its goals, which, if not adequately protected, can provide cyber criminals with a way to attack the electric grid and impact its overall safety and reliability.[52] As one FERC commissioner stated, "[t]he significant benefits of Smart Grid technologies must be achieved without taking reliability and security risks that could be exploited to cause great harm to our Nation's citizens and economy."[53] Ironically, because the smart grid seeks to increase the efficiency of the electric grid through the use of modern technology (such

---

SECURITY: A WHITE PAPER FOR FRANCHISORS, LICENSORS, AND OTHERS 1 (2009) (citing another definition of cyber security as "the protection of any computer system, software program, and data against unauthorized use, disclosure, transfer, modification, or destruction, whether accidental or intentional").

47. *See* NISTIR DRAFT FEB. 2010, *supra* note 15, at 10.

48. *Id.*

49. *See id.* at 10, 12.

50. *Id.* at 8 (noting that the need to address cyber security vulnerabilities has been acknowledged by many federal government agencies).

51. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 43, at viii.

52. *Id.* at xiii, 6; *see also* NISTIR DRAFT FEB. 2010, *supra* note 15, at 8-9 (citing one of the EISA's explicit statements of purpose to include "modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure" in relation to the development of the Smart Grid, and noting that "[t]he need to address potential vulnerabilities has been acknowledged across the federal government, including the [NIST], the [DHS], the [DOE], and the [FERC]").

53. *Smart Grid Initiatives and Technologies: Hearing to Examine the Progress on Smart Grid Initiatives Authorized in the Energy Independence and Security Act of 2007, and Funded in the Stimulus Bill, and to Learn of Opportunities and Impediments to Timely Installation of Smart Grid Technologies Before the S. Comm. on Energy & Natural Res.*, 111th Cong. 7 (2009) (prepared statement of Suedeen G. Kelly, Comm'r, Federal Energy Regulatory Commission).

as software and networks), and because software and networks are by their very nature prone to cyber attacks, smart grid development may actually decrease the security of the electric grid. This underscores the importance of prudent smart grid development that understands and adapts to the challenges of cyber security.

The EISA delegated responsibility to the NIST to develop "interoperability and functionality" standards for the smart grid.[54] The NIST has interpreted this authority to include cyber security standards,[55] which the NIST is still developing.[56] These standards currently target the ways that smart grid development may create cyber security risks such as (1) by increasing the complexity of the grid thereby introducing vulnerabilities and increasing exposure to attacks and unintentional errors, (2) by increasingly interconnecting networks, (3) by increasing vulnerabilities to communication disruptions and introduction of malicious software that could result in denial of service or compromising the integrity of software and systems, (4) by increasing the number of entry points and paths for attackers, and (5) by increasing the potential for compromise of data confidentiality.[57] These vulnerabilities are also created by NUSP-consumer interactions.

NUSP-consumer interactions should be considered a cyber security risk equal to other smart grid applications because the non-utility services they provide share the same vulnerabilities as other aspects of smart grid development. Non-utility services exhibit all of the smart grid development vulnerabilities identified above as particularly problematic for assuring the safety of the grid. First, these interactions increase the complexity of the grid by adding an additional layer of functionality to the grid. For example, AlertMe adds a new layer of functionality to the grid by creating an interface where the consumer can tap into his or her electric usage data to perform EEA. This new function complicates the current status of the grid by adding a function currently absent (i.e. the grid currently lacks active participation of the consumer beyond consuming electricity). Second, these interactions increase the interconnection of networks. HANs are good examples of this as they create new networks within a consumer's home to perform EEA, which is in turn connected to the Internet. Third, many of these services increase vulnerability to malicious software and the potential for service disruption because they allow consumers to utilize the Internet to

54. Energy Independence and Security Act of 2007 § 1305, 42 U.S.C.A. § 17385 (2010); *see also* NAT'L INST. OF STANDARDS & TECH., NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS RELEASE 1.0 7 (2010) (interpreting the NIST's EISA authority to include cyber security standards).

55. NAT'L INST. OF STANDARDS & TECH., *supra* note 54.

56. *See* NISTIR DRAFT FEB. 2010, *supra* note 15, at 1.

57. *Id.* at 8.

perform EEA, which creates an additional access point for malicious software to exploit. Fourth, these new access points also create additional entry points that potential attackers can exploit to harm the grid. Finally, non-utility services such as PowerMeter or AlertMe create a risk that data confidentiality will be compromised because an additional party, the non-utility, collects electric usage data from consumers.[58]

Exploitation of poor cyber security related to NUSP-consumer interactions could result in harm to the grid in a variety of ways. As the complexity of interconnection between smart grid technologies and the electric grid increases, a "chain of dependencies" is created that makes the grid more and more vulnerable to cyber attacks.[59] The Department of Energy ("DOE") has explained that these vulnerabilities could be exploited to jeopardize the grid, stating that there is potential for "extreme damage from a cyber attack" on the U.S. electric grid that could result in "destruction of generators, power outages, and grid instability."[60] One way this level of damage could be achieved is by disruption of IT equipment by EM Pulse, EMI, or Geomagnetically Induced Currents.[61] More specifically, the DOE cited a 2009 study of AMI devices and networks to exemplify how a NUSP-consumer interaction could result in such "extreme damage."[62] This study found that when these wireless AMI devices/networks (such as wireless non-utility devices that provide EEA and HANs connected to them) are used by consumers outside of the control of an electric utility, the devices are highly vulnerable to cyber attacks.[63] The study found that if these devices were attacked, the grid would be jeopardized by a cyber attacker extracting data from the memory of a device and modifying the device's memory to insert malicious software.[64] Once the device has been compromised, it can be used to attack other parts of the smart grid by communicating through a network, which can compromise control systems.[65]

58. *See* Quinn, *supra* note 15, at 9-11.

59. Alex Yu Zheng, *Smart Security for a Smart Grid: New Threats on the Horizon*, SMARTGRIDNEWS.COM (Sept. 28, 2009), http://www.smartgridnews.com/artman/publish/Technologies_Security_News/Smart-Security-for-a-Smart-Grid-New-Threats-on-the-Horizon-1226.html.

60. OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, STUDY OF SECURITY ATTRIBUTES OF SMART GRID SYSTEMS – CURRENT CYBER SECURITY ISSUES 2 (2009).

61. ANNABELLE LEE, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST AND THE SMART GRID 32 (2010).

62. OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, *supra* note 60, at 12 (citing Travis Goodspeed et al., Low-level Design Vulnerabilities in Wireless Control Systems Hardware (2009)).

63. *Id.*

64. *Id.*

65. *Id.*

Employees of the FERC have also acknowledged the cyber security concerns that develop due to chains of dependencies between the grid and NUSP-consumer interactions.[66] Joseph McClelland, Director of the Office of Electric Reliability at the FERC, has specifically addressed the danger of non-utility services.[67] McClelland has stated that "a smarter grid would permit two-way communication between the electric system and a large number of devices located outside of controlled utility environments, which will introduce many potential access points."[68] He believes that these access points allow cyber attackers to harm the grid by either manipulating the electric usage data collected by non-utility devices or by manipulating the control systems that manage electricity supply and usage.[69] Additionally, McClelland singles out automated load management, one of the main functions of non-utility services, as a particularly apt avenue for attacking the grid.[70] He explains that an attack on load management could be used to affect the smart grid's AMI, which could result in disconnection of service to a large number of customers and subsequently harm the bulk power system.[71] Reestablishing service could be greatly delayed if a subsequent attack was carried out on the advanced meters themselves.[72] This loss of service can be extremely costly—an estimated $164 billion per year—and should be avoided.[73]

As the DOE findings and McClelland's statements illustrate, the electric grid is vulnerable to damaging cyber security attacks that originate from NUSP-consumer interactions. As explained below, no entity has authority to effectively regulate these interactions.[74] Thus, to avoid this potential harm, it is necessary to create regulatory authority

66. *See Securing the Modern Electric Grid from Physical and Cyber Attacks: Hearing Before the Subcomm. on Emerging Threats, Cybersecurity, & Sci. & Tech. of the H. Comm. on Homeland Sec.*, 111th Cong. 51-52 (2009) (statement of Joseph McClelland, Director, Office of Electric Reliability, Federal Energy Regulatory Commission).

67. *Id.*

68. *Id.* at 52.

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.*

73. CONSORTIUM FOR ELEC. INFRASTRUCTURE TO SUPPORT A DIGITAL SOC'Y, THE COST OF POWER DISTURBANCES TO INDUSTRIAL & DIGITAL ECONOMY COMPANIES ES-3 (2001).

74. *See infra* Part III; *see also* ANNABELLE LEE, NAT'L INST. OF STANDARDS & TECH., SMART GRID CYBER SECURITY STRATEGY AND REQUIREMENTS A-19 (2009) [hereinafter NISTIR DRAFT SEPT. 2009] (describing the cyber security objectives for these interactions, but not going into detail for how they will be applied); Energy Independence and Security Act of 2007 § 1305(d), 42 U.S.C.A. § 17385(d) (2010) (Standards for Interoperability in Federal Jurisdiction: "At any time after the Institute's work has led to sufficient consensus in the Commission's judgment, the Commission shall institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets.").

over the cyber security concerns that arise from NUSP-consumer interactions.

2. Privacy Concerns

While smart grid development may bring many positive benefits due to an improved ability to receive and transmit electric usage information, increased transmission of such information about individual consumers creates privacy concerns.[75] Examples of such concerns include the use of electricity usage data to (1) expose consumer behavior patterns for commercial benefit (e.g. through sale to advertising companies), (2) identify and track consumers for law enforcement purposes,[76] and (3) monitor consumer activities in the home.[77] While each of these capabilities of the smart grid could be used for beneficial purposes, they could also be used for malicious ones. Additionally, although it can be argued that the magnitude of harm that can result from such privacy violations is likely less severe in economic terms than the harm that can result from cyber security breaches,[78] the potential harm an individual consumer could experience through privacy violations is varied and personal. Not only could consumers experience monetary harm or a violation of their legal rights, but they could also be physically harmed through criminal acts made possible by the smart grid's data surveillance capabilities.[79] Accordingly, regulators and commentators have voiced concern that something must be done to protect consumer privacy in the context of smart grid services and products.[80]

As early as 2000, the National Association of Regulatory Utility Commissioners ("NARUC"), which represents the Public Utility Commissions ("PUC") of all fifty states,[81] adopted a resolution "[u]rging the [a]doption of [g]eneral [p]rivacy [p]rinciples [f]or [s]tate [c]ommission [u]se in [c]onsidering the [p]rivacy implications of the [u]se of [u]tility [c]ustomer [i]nformation."[82] Although the NARUC

75. *See* NISTIR DRAFT SEPT. 2009, *supra* note 74, at 8 (stating that there are "many significant privacy concerns and issues" regarding smart grid development); *see also* Quinn, *supra* note 15, at 11; *The Smart Grid and Privacy*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/smartgrid/smartgrid.html (last visited Feb. 11, 2011).

76. Quinn, *supra* note 15, at 11.

77. For more technical information regarding how smart metering accomplishes these feats, *see* Quinn, *supra* note 15, at A-1 to -9.

78. *See supra* note 60 and accompanying text.

79. Quinn, *supra* note 15, at 10 (describing the potential for burglary as a privacy concern created by the smart grid's ability to obtain detailed electric usage data which could be used to ascertain when consumers are away from their homes).

80. *See supra* note 15.

81. *About NARUC*, NAT'L ASS'N OF REGULATORY UTIL. COMM'RS, http://www.naruc.org/about.cfm (last visited Feb. 11, 2011).

82. NAT'L ASS'N OF REGULATORY UTIL. COMM'RS, RESOLUTION URGING THE

identified the privacy issues associated with smart grid development nearly ten years ago, the NIST noted in 2010 that "in general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid" and that a "lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a privacy risk that needs to be addressed."[83] Such statements affirm the need to protect against privacy concerns related to smart grid development and evidence the current lack of such protections.

Finally, while it is unclear that either the NARUC's or the NIST's statements contemplated the role of NUSPs in smart grid development, privacy concerns are not reduced in this context. Instead, privacy concerns may be exacerbated for NUSP-consumer interactions because it is less clear which government entity can regulate such interactions. This uncertainty stems from the legal distinction between a utility-consumer interaction and a NUSP-consumer interaction, the former clearly being under PUC jurisdiction while the latter is a more difficult inquiry.[84] Regardless of this regulatory uncertainty, because privacy concerns related to smart grid development have been identified by regulatory authorities as serious concerns that need to be addressed, regulation of the privacy concerns of NUSP-consumer interactions is also necessary.

III. WHAT ENTITY HAS AUTHORITY TO REGULATE NUSP-CONSUMER INTERACTIONS?

Determining what government entity or entities have authority to regulate the smart grid is complicated. This Part identifies the government entities with regulatory authority over the development of the smart grid, explains the extent of each entity's regulatory authority, and concludes that none of these entities have authority to adequately regulate the cyber security and privacy concerns of NUSP-consumer interactions. Section A explains why no government entity currently has the authority to adequately regulate NUSP-consumer *cyber security* concerns, and Section B explains why the state PUCs and the state analogues of the Federal Trade Commission ("FTC") are the only entities with authority to regulate NUSP-consumer *privacy* concerns.

ADOPTION OF GENERAL PRIVACY PRINCIPLES FOR STATE COMM'N USE IN CONSIDERING THE PRIVACY IMPLICATIONS OF THE USE OF UTILITY CUSTOMER INFORMATION (2000).

83. NISTIR DRAFT SEPT. 2009, *supra* note 74, at 8.

84. *See infra* Part III.

A. No Entity has Authority to Regulate NUSP-Consumer Cyber Security Concerns

Authority to regulate the electric grid was traditionally divided between the FERC and PUCs. The FERC's jurisdiction, as codified in the Federal Power Act ("FPA"),[85] included authority to regulate wholesale sales[86] of electricity in interstate commerce and transmission of electricity in interstate commerce. The PUCs' jurisdiction included authority to regulate retail sales of electricity,[87] local distribution of electricity, and the siting of power plants and transmission lines.[88] Federal legislation has since altered this dual regulatory framework. Specifically, the Energy Policy Act of 2005 ("EPAct of 2005") and the EISA have increased the FERC's regulatory authority and have extended regulatory authority to additional entities such as the Department of Energy ("DOE"), the National Electric Reliability Corporation ("NERC"), the National Institute of Standards and Technology ("NIST"), and the Federal Communications Commission ("FCC") (referred to collectively as "non-traditional entities"). Additionally, the Department of Homeland Security ("DHS") has been delegated some jurisdiction over cyber security concerns. Delegation of regulatory authority to non-traditional entities has been problematic because it has blurred jurisdictional boundaries. Consequently, determining which entity has authority to regulate new developments in the electric industry, such as NUSP-consumer interactions, has become more difficult. This Section analyzes the jurisdictional boundaries of each entity in relation to NUSP-consumer cyber security concerns and concludes that it is unlikely that the FERC, PUCs, or non-traditional entities have authority to adequately regulate them.

1. The FERC—Partial and Inadequate Regulatory Authority

While the FERC's traditional and newly delegated regulatory powers give it a great deal of power to regulate the electric grid, these powers do not include the authority to adequately regulate the cyber security aspects of NUSP-consumer interactions. This Subsection outlines the development of the FERC's authority to regulate the electric grid and explains why its current jurisdiction is not broad enough to

85. Federal Power Act § 201, 16 U.S.C. § 824 (2006).

86. "Wholesale sales" are defined as one between two entities who are not the ultimate users of the electricity. FRED BOSSELMAN ET AL., ENERGY, ECONOMICS, AND THE ENVIRONMENT 590 (3d ed. 2010).

87. "Retail sales" are defined as sales directly to an end user. *Id.*

88. U.S. GEN. ACCOUNTING OFFICE, GAO-03-726R, ELECTRICITY MARKETS: FERC'S ROLE IN PROTECTING CONSUMERS 2 (2003).

allow for adequate regulation of the NUSP-consumer cyber security concerns.

Although the FERC's traditional authority to regulate the transmission and wholesale sales of electricity that occur in interstate commerce has expanded over the years, this authority does not allow for regulation of NUSP-consumer cyber security concerns. The FERC's authority to regulate the transmission and wholesale sales of electricity that occur in interstate commerce has expanded for two reasons: (1) growth in the amount of interstate wholesale sales and transmission of electricity, and (2) judicial recognition of the physical properties of electricity.[89] The first reason for expansion relates to the development of the electric grid. When the FPA was passed, the electric grid had few interstate transmission lines because electricity markets were local.[90] However, as electricity markets grew, interstate interconnection increased, thereby increasing the FERC's regulatory power.[91] The second reason for expansion relates to judicial recognition of the physical properties of electric transmission. Physical scientists have explained, and courts have accepted, that due to the physical properties of electricity, when electricity is transmitted intrastate it should be deemed to be traveling *interstate* if that state's grid connects to another state's grid.[92] Thus, nearly all transmission of electricity is now deemed to be transmission in interstate commerce.[93] Additionally, the FERC's

89. *See* Fed. Power Comm'n v. Fla. Power & Light Co., 404 U.S. 453, 463 (1972) (upholding the FERC's interpretation that its jurisdiction over wholesale sales in interstate commerce includes sales of electricity for resale when that electricity is transmitted via transmission lines that eventually connect to transmission lines of another state due to the physical properties of electricity transmission); *see generally* Brief for Electrical Engineers, Energy Economists and Physicists as Amici Curiae Supporting Respondents, New York v. FERC, 535 U.S. 1 (2002) (No. 00-568), (2001 WL 605124) (explaining that due to the physical properties of electricity, electricity flows at a tremendous pace on the wires of an interconnected grid and is not confined to the artificial boundaries of a state, but instead should be considered to be present at all locations where transmission lines run).

90. *National Electricity Policy: Federal Government Perspectives: Hearing Before the Subcomm. on Energy & Air Quality of the H. Comm. on Energy & Commerce*, 107th Cong. 34 (2001) (prepared statement of Hon. Francis Blake, Deputy Secretary, Dep't of Energy).

91. *See supra* note 89. *See also* Jared M. Fleisher, ERCOT'S JURISDICTIONAL STATUS: A LEGAL HISTORY AND CONTEMPORARY APPRAISAL, 3 TEX. J. OIL, GAS, & ENERGY L. 4, 9-10 (2008) (describing the Supreme Court's "technological transmission test" for determining when electric transmission occurs in interstate commerce as laid out by Conn. Light & Power Co. v. Fed. Power Comm'n, 324 U.S. 515, 529-31 (1954), and how the test has been applied expansively).

92. *See* Fleisher, *supra* note 91, at 9 (describing how Texas, Alaska, and Hawaii are the only states that currently are not regulated by the FERC due to the broad interpretation of electric "transmission in interstate commerce").

93. *See Securing the Modern Electric Grid from Physical and Cyber Attacks*, *supra* note 66. It is also noteworthy that this recognition by the courts was the reason that Texas limited the connection of its transmission lines to those of surrounding states. Thus, Texas has escaped some regulation by the FERC and instead regulates the transmission of electricity within its

authority to regulate wholesale sales of electricity in interstate commerce has grown in proportion to this new interpretation of interstate transmission because wholesale sales are now much more frequently found to be in interstate commerce.[94]

Regardless of the expansion of the FERC's traditional regulatory powers, the FERC does not have authority to regulate NUSP-consumer interactions because these interactions do not involve either the wholesale sale or transmission of electricity. Wholesale sales of electricity are sales of electricity between entities who are not the ultimate users of the electricity.[95] Transmission of electricity is the physical transport or flow of electric energy to end use locations.[96] NUSP-consumer interactions involve the provision of a product or service by NUSPs to consumers that can be used for EEA or load management.[97] These services are performed by gathering a consumer's electric usage data and then analyzing it so that the consumer can make decisions about electricity use.[98] Because NUSP products/services allow consumers to collect and analyze electric usage data, but do not transmit or sell electricity to the consumer, NUSP-consumer interactions do not involve wholesale sale or transmission of electricity, and the FERC cannot regulate them under its traditional regulatory authority. Thus, the FERC must seek another jurisdictional hook if it is to regulate NUSP-consumer interactions.

Fortunately for the FERC, Congress has increased the FERC's range of jurisdictional powers via three major statutes: the EPAct of 2005,[99] the EISA,[100] and the ARRA.[101] Each of these statutes extends partial regulatory authority to the FERC for NUSP-consumer interactions. However, this partial authority is inadequate to properly address NUSP-consumer cyber security concerns.

The EPAct of 2005 changed the traditional electric regulatory framework by giving the FERC authority to regulate the "reliability" of

---

state via its own Electric Reliability Council of Texas (ERCOT). *See ERCOT*, FED. ENERGY REGULATORY COMM'N, http://www.ferc.gov/industries/electric/indus-act/rto/ercot.asp (last updated Jan. 20, 2011).

94. *See* Fed. Power Comm'n v. Fla. Power & Light Co., 404 U.S. 453 (1972).

95. *See* FRED BOSSELMAN ET AL., *supra* note 86.

96. *Electric Power Transmission*, ANSWERS.COM, http://www.answers.com/topic/electric-power-transmission (last visited Feb. 11, 2011) (providing the definition from the McGraw-Hill Dictionary of Scientific and Technical Terms (6th ed. 2003)); *see also* Fleisher, *supra* note 91, at 9.

97. *See supra* Part II.A.

98. *Id.*

99. Codified as an amendment to the Federal Power Act at 16 U.S.C. § 824 (2006).

100. Energy Independence and Security Act of 2007 § 1305(d), 42 U.S.C.A. § 17385(d) (2010).

101. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (to be codified in scattered sections of 42 U.S.C.).

the "bulk power system."[102] To accomplish this, the FERC was ordered to appoint an electric reliability organization ("ERO") that would establish mandatory electric reliability standards.[103] The FERC could then adopt and enforce these electric reliability standards via civil penalties.[104] In 2006, the FERC approved the North American Electric Reliability Corporation ("NERC") to become the ERO, and in 2007 the FERC approved mandatory reliability standards suggested by the NERC.[105] The FERC's authority to regulate the reliability of the grid arguably encompasses the regulation of cyber security concerns related to smart grid development because security violations have the potential to jeopardize the reliability of the grid.[106] However, at best this authority would only be a partial solution to these concerns because its powers would only extend to the "reliability" of smart grid development within the "bulk power system."[107]

Reliability or "reliable operation" as codified in § 215(a)(4) of the FPA is defined as

> [O]perating the elements of the Bulk-Power System within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a Cybersecurity Incident, or unanticipated failure of system elements.[108]

This definition clearly contemplates cyber security as a component of "reliable operation." However, the ability to use this provision to regulate the cyber security concerns of smart grid development is extinguished by the limitation that the FERC may only regulate cyber security when it involves the reliable operation of the "bulk power system."

The "bulk power system" is defined as both "facilities and control systems necessary for operating an interconnected electric energy transmission network" and "electric energy from generating facilities needed to maintain transmission system reliability."[109] The EPAct of 2005 specifically excludes "facilities used in the local distribution of

102. 16 U.S.C. § 824(o)(b)(1) (2006).
103. *Id.* §§ 824(o)(d-e).
104. *Id.*
105. N. AM. ELEC. RELIABILITY CORP., MILESTONES: NERC RELIABILITY STANDARDS 4 (2007).
106. This argument is based on an assumption that the cyber security threats are a consideration for the grid's "reliability."
107. 16 U.S.C. § 824(o)(a)(1) (2006).
108. 18 C.F.R. § 39.1 (2010).
109. *Id.*

electric energy"[110] from this definition. However, it is unclear what is considered a local distribution facility and what is considered part of the bulk power system.[111] Some employees at the FERC have stated that the bulk power system definition excludes nearly all grid facilities in some large cities,[112] while others state that it describes "low-voltage facilities used to deliver energy in one direction to retail end-users."[113] Because general development of the smart grid, such as the provision of smart meters, largely takes place at the local distribution facilities and grid facilities,[114] this development falls outside of the FERC's reliability authority. This is unfortunate because smart meters might be considered "control systems" under the definition of bulk power system. Control systems are defined as "facilities, systems, equipment, services, and diagnostics that provide the functional control capabilities necessary for the effective and reliable operation of the bulk [power] system."[115] Smart meters perform this exact role by providing functional control of electric usage for effective operation of the grid. However, because the EPAct of 2005 specifically excludes local distribution and grid facilities, where smart meters are primarily located, smart meters are likely excluded from the bulk power system definition. Thus, it is likely that the FERC's regulatory authority over grid reliability does not extend to the cyber security concerns of smart grid development taking place at local distribution and grid facilities.

The FERC's reliability authority is even less likely to cover NUSP-consumer interactions. These interactions are presumably outside the scope of the bulk power system definition because these interactions are not similar to large scale control systems. The definition of bulk power system seems to contemplate large scale grid operations such as "facilities and control systems" used for operating a transmission network. NUSP-consumer interactions do not occur on a large scale, but instead are more localized and thus farther removed from the bulk power system than local distribution or grid facilities, which are exempted from the bulk power system definition. In fact, NUSP-consumer interactions take place at the smallest and most local level possible: the consumer's residence. Additionally, it is unclear that NUSP services are control systems used for "operating a transmission network." NERC's reliability standards

110. 16 U.S.C. § 824(o)(a)(1) (2006).

111. BERNARD C. LESIEUTRE ET. AL., TOPOLOGICAL AND IMPEDANCE ELEMENT RANKING (TIER) OF THE BULK-POWER SYSTEM, PRELIMINARY REPORT 7 (2009).

112. *See Securing the Modern Electric Grid from Physical and Cyber Attacks*, *supra* note 66.

113. *Net Metering: Hearing Before the Subcomm. on Energy of the S. Comm. on Energy & Natural Res.*, 111th Cong. 5 (2009) (statement of Kevin A. Kelly, Director, Div. of Policy Dev., Office of Energy Policy and Innovation, Fed. Energy Regulatory Comm'n).

114. *See generally* U.S. DEP'T OF ENERGY, *supra* note 2, at 2.

115. U.S. DEP'T OF ENERGY & U.S. DEP'T OF HOMELAND SEC., ROADMAP TO SECURE CONTROL SYSTEMS IN THE ENERGY SECTOR 5 (2006).

describe one such control system as "[s]ystems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more."[116] NUSP services, however, are used by the consumer in monitoring and augmenting electricity usage—a function that has nothing to do with transmission and which controls electricity usage many magnitudes of scale smaller than 300 MW.[117] Thus, it is likely that the FERC cannot regulate NUSP-consumer interactions to account for cyber security concerns or other larger scale aspects of smart grid development through its EPAct of 2005 reliability authority because these interactions do not meet the definitional criteria over which the FERC has reliability authority.

Although the EPAct of 2005 fails to vest the FERC with the jurisdiction needed to adequately regulate the cyber security concerns of smart grid development and NUSPs, the EISA does provide it with new jurisdiction tied directly to smart grid development.[118] This jurisdiction gives the FERC the power to regulate NUSP-consumer interactions, but because the FERC has interpreted its authority under this act narrowly,[119] the FERC cannot use its EISA authority to adequately address NUSP-consumer cyber security concerns without reinterpreting its jurisdictional authority.

The EISA has changed the traditional electric regulatory framework by directing the NIST to develop standards to ensure smart grid functionality and interoperability.[120] Interoperability is defined as "the capability of systems or units to provide and receive services and information between each other, and to use the services and information exchanged . . . without significant user intervention."[121] Once the NIST has developed these standards, the FERC is required to institute rulemaking proceedings to adopt them, provided they "insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets."[122] The FERC has interpreted this delegation of authority to mean that it may adopt

116. N. AM. ELEC. RELIABILITY CORP., RELIABILITY STANDARDS FOR THE BULK ELECTRIC SYSTEMS OF NORTH AMERICA 2 in Standard CIP–002–1 (2006).

117. According the U.S. Energy Information Administration, in 2008 the average U.S. household used only 11.04 MWh *per year* which equals 0.00126 MW needed each hour of every day (i.e., 11.04 MWh/y ÷ 365 days ÷ 24 hours/day). *Frequently Asked Questions – Electricity*, U.S. ENERGY INFO. ADMIN., http://tonto.eia.doe.gov/ask/electricity_faqs.asp#electricity_use_home (last visited Feb. 11, 2011) (select "How much electricity does an American home use?").

118. Smart Grid Policy, 74 Fed. Reg. 37,098, 37,098 (July 16, 2009).

119. *Id.* at 37,100.

120. *Id.* at 37,099.

121. GRIDWISE ARCHITECTURE COUNCIL, INTRODUCTION TO INTEROPERABILITY AND DECISION-MAKER'S INTEROPERABILITY CHECKLIST VERSION 1.5, 1 (2010).

122. Energy Independence and Security Act of 2007 § 1305(d), 42 U.S.C.A. § 17385(d) (2010).

interoperability standards for "all electric power facilities and devices with smart grid 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 [stated in the act]."[123] Because NUSP devices, such as the TED or AlertMe, are "devices with smart grid features" and are used "directly by retail consumers," the FERC has authority to regulate these devices through NIST standards as long as the standards are necessary for insuring "functionality and interoperability in interstate transmission of electric power, and . . . wholesale electricity markets."[124] This power very nearly gives the FERC the ability to address the cyber security concerns of NUSPs. However, the FERC has interpreted a limitation on this new power that significantly restricts its efficacy: the EISA omits the additional authority for FERC to mandate or enforce these standards.[125] The FERC acknowledged this limitation in its Smart Grid Policy Statement by stating that it "does not [have] authority to . . . enforce [these] standards" or to "direct states to implement any particular retail customer policies or programs."[126] Thus, while the FERC has the authority to enact standards that address NUSP-consumer cyber security concerns, the FERC effectively cannot ensure that these concerns are actually minimized. Accordingly, the only solutions available are for the FERC to reinterpret its interoperability authority or, as suggested by the FERC Commissioner Suedeen Kelly, for Congress to consider additional legislation.[127]

Although the FERC's self-imposed enforcement limitation significantly restricts the efficacy of the interoperability standards, the FERC does have a limited ability to enforce the standards indirectly via its traditional cost-recovery ratemaking powers. Under this alternative, the FERC could bypass the limitation by mandating the adoption of the interoperability standards as a condition of parties recovering costs through rate regulation under the FERC's traditional wholesale sales and transmission in interstate commerce jurisdiction.[128] The FERC has acknowledged its intention to do this in its Smart Grid Policy Statement,[129] explaining that while standards are being developed it will condition cost recovery on principles laid out in its "Interim Rate Policy."[130] This policy requires applicants seeking smart grid cost recovery to (1) demonstrate that "the reliability and security of the bulk-power

123. Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).
124. 42 U.S.C.A. § 17385(d) (2010).
125. *See Smart Grid Initiatives and Technologies, supra* note 53, at 10.
126. Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).
127. *Id.*
128. *Id.* at 37,099.
129. *Id.* at 37,098.
130. *Id.* at 37,110.

system will not be adversely affected by the deployment of smart grid facilities at issue,"[131] (2) show that it has minimized the possibility of stranded costs for smart grid equipment,[132] and (3) share certain information with the DOE Smart Grid Clearinghouse so that the smart grid deployment provides useful feedback for the development of the interoperability standards.[133] This indirect enforcement of the interoperability standards will allow the FERC to bypass its self-imposed jurisdictional limitation. However, it will not allow the FERC to regulate the cyber security concerns of smart grid development related to NUSP-consumer interactions because NUSPs are not utilities that will seek cost recovery, and even if they were, NUSP services would not fall under the FERC's ratemaking authority because they are not wholesale sales of electricity.[134] Thus, these interactions will go unregulated by the FERC.

2. PUCs—No Authority to Regulate

The powers of PUCs to regulate the electric grid are limited by the powers of the FERC, a state's constitution and legislation, and the U.S. Constitution.[135] Under this framework, the powers of PUCs may, at the maximum, extend to all the powers not delegated to the FERC and not precluded by the U.S. Constitution. In reality, PUC powers vary somewhat from state to state.[136] However, a PUC's electric regulatory authority generally includes the power to regulate the facilities, services, and rates of electric utilities operating within that state for the purposes of selling retail electricity and distributing electricity locally.[137] Under this general regulatory authority, a cursory analysis of NUSP-consumer interactions is enough to demonstrate that PUCs do not have the authority to regulate the NUSP-consumer cyber security concerns because NUSP-consumer interactions occur between non-utilities and consumers, and PUCs can only regulate interactions between utilities and consumers.

---

131. *Id.* at 37,111.

132. *Id.*

133. *Id.*

134. *See infra* Part III.A.2.

135. For example, the COLO. CONST., art. XXV, the COLO. REV. STAT. ANN. §§ 40-1-101 to -104 (West 2010), and the COLO. CODE REGS. § 723-1 (2011), lay out the powers of the Colorado PUC.

136. For example, California's PUC can regulate public utilities, including "electrical corporations," defined as any person or corporation owning, controlling, operating, or managing any electric plant for compensation within California "where the service is performed for, or the commodity is delivered to, the public or any portion thereof." CAL. PUB. UTIL. CODE § 216 (West 2010). Whereas in Texas the PUC can regulate public utilities including "electric utilities" defined as "a person . . . that owns or operates for compensation in [Texas] equipment or facilities to produce, generate, transmit, distribute, sell, or furnish electricity" in Texas. 16 TEX. ADMIN. CODE §§ 25.5(41), (92) (2011).

137. *See supra* text accompanying notes 87-88.

In relation to the new powers of the FERC and other new entities, PUCs retain a great deal of control over how the smart grid develops. As the FERC was careful to point out in its Smart Grid Policy Statement, PUCs retain authority to decide (1) what costs utilities may recover from ratepayers for smart grid development when that development relates to retail sales or local distribution of electricity, (2) whether or not to adopt interoperability and functionality standards for the smart grid, and (3) how to regulate retail electric consumers in relation to the smart grid.[138] These powers are strong tools for controlling smart grid development. For example, PUCs can choose to ignore the FERC's interoperability and functionality standards for smart grid devices/services and create their own when those devices/services are only used for the purposes of retail sales or local distribution of electricity.[139] Additionally, PUCs can control smart grid development by using their ratemaking authority to limit the types of smart grid expenditures which may be recovered through rate regulation. Lastly, and most importantly, a PUC can control the policies surrounding retail sales and local distribution of electricity, which encompasses the actual implementation and function of smart grid technologies. Through this power the PUC can determine how advanced meters are installed and how they allow consumers to respond to real-time pricing. Because many aspects of smart grid development depend upon PUC decisions in these three areas, PUCs retain substantial control over how the smart grid develops. However, this control does not extend to NUSP-consumer interactions.

PUCs regulate "public utilities." The definition of "public utility" is derived from English common law,[140] was formally adopted by the Supreme Court in *Munn v. Illinois*,[141] and has been codified in state statutes.[142] The common law defines a public utility as private property "affected with a public interest."[143] In turn, the common law considers private property to be affected with a public interest when it is "used in a manner to make it of public consequence, and affect the community at large."[144] In practice this definition seems difficult to apply. However, states have eliminated the need to use the definition on an ad hoc basis

138. Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).

139. *See Smart Grid Initiatives and Technologies*, *supra* note 53, at 10 (in which FERC Commissioner Suedeen Kelly states that even asserting the full scope of the FERC's powers under the FPA, the FERC's Smart Grid standards will only apply to certain entities, excluding PUCs).

140. Munn v. Illinois, 94 U.S. 113, 126 (1876) (citing Lord Chief Justice Hale's treatise, DE PORTIBUS MARIS, as the source of the definition of public utility).

141. *Id.*

142. *See, e.g.*, COLO. REV. STAT. § 40-1-103(1)(a)(I) (2010) (stating any entity "declared by law to be affected with a public interest" is a public utility).

143. *Munn*, 94 U.S. at 126.

144. *Id.*

by supplying concrete statutory lists of the entities that the state declares to be public utilities.[145] The entities declared to be public utilities in most states are those that "provide[] necessary services to the public, such as telephone lines and service, electricity, and water."[146] Additionally, "[m]ost utilities operate as monopolies" that carry on operations "for the accommodation of the public, the members of which are entitled as a matter of right to use the enterprise's facilities."[147]

A sample of state definitions of public utility suggests that NUSPs are likely not public utilities. For example, in California public utilities include "electrical corporations" defined as any person or corporation owning, controlling, operating, or managing any electric plant for compensation within California "where the service is performed for, or the commodity is delivered to, the public or any portion thereof."[148] Colorado's definition of a public utility is nearly identical, stating that electrical corporations are deemed to be public utilities if they operate for the purpose of supplying the public with use of electricity.[149] Additionally, in Texas, public utilities include "electric utilities" defined as "a person . . . that owns or operates for compensation in [Texas] equipment or facilities to produce, generate, transmit, distribute, sell, or furnish electricity" in Texas.[150] A common thread among these states' definitions is the limitation that for private corporations to be declared public utilities they must provide an electric service related to the *provision* of electricity *to* the consumer. This limitation guides the application of the definition and leaves out corporations such as NUSPs that provide services that are related to the *use* of electricity *by* the consumer. It also clearly leaves out NUSPs that provide products to consumers rather than services.

Even if one believes that it is ambiguous as to whether or not NUSPs fall under a state's public utility definition, NUSPs are unlikely to be deemed public utilities by a state court because they do not meet the underlying limitation guiding decisions as to when a private enterprise should be deemed a public utility. For example, in applying the limitation outlined above to NUSPs such as Energy, Inc. or AltertMe.com, Ltd., neither provides necessary services to the public similar to the provision of electricity or water, neither are monopolies,

145. Colorado defines a "public utility" as "every common carrier, pipeline corporation, gas corporation, electrical corporation, telephone corporation, water corporation, person, or municipality operating for the purpose of supplying the public for domestic, mechanical, or public uses and every corporation, or person declared by law to be affected with a public interest." COLO. REV. STAT. § 40-1-103(1)(a)(I) (2010).

146. BLACK'S LAW DICTIONARY 1686 (9th ed. 2009).

147. *Id.*

148. CAL. PUB. UTIL. CODE § 216 (West 2010).

149. *See* COLO. REV. STAT. § 40-1-103(1)(a)(I) (2010).

150. 16 TEX. ADMIN. CODE §§ 25.5(41), (92) (2011).

and members of the public are not entitled as a matter of right to use either companies' services. Instead, these companies conduct business as for-profit associations, the services they provide are simply beneficial to the consumer but not "necessary," and the members of the public only have a right to use these companies' services upon entering into private contracts with them. Thus, NUSPs are not public utilities, and NUSP-consumer interactions cannot be regulated by PUCs.

3. The DOE—No Authority to Regulate

The EISA charged the DOE with the responsibility of creating a Smart Grid Task Force ("SGTF") to "insure awareness, coordination and integration of . . . Federal Government [activities] related to smart-grid technologies and practices."[151] However, this grant of authority cannot be construed to grant the DOE power to regulate NUSP-consumer cyber security concerns.

The plain language of the EISA indicates that the DOE may create the SGTF for the limited purpose of streamlining federal government smart grid development efforts by allowing the SGTF to advise other agencies on the development of the smart grid.[152] Without more, the DOE cannot interpret this language to permit it to regulate NUSP-consumer interactions because such a delegation of authority is significant enough to necessitate plain statutory language.[153] Moreover, if the DOE attempted to take on this authority it is likely that the very purpose of the SGTF provision would be frustrated because it would inject confusion into the regulation and development of the smart grid by splitting up regulatory authority over the smart grid. Thus, the DOE does not have authority to regulate NUSP-consumer interactions via this provision.

The ARRA also charged the DOE with some responsibility over the development of the smart grid. The ARRA charged the DOE with the responsibility of awarding grants for smart grid projects and developing a smart grid information clearinghouse.[154] Responsibility for

151. Energy Independence and Security Act of 2007 § 1303(b)(2), 42 U.S.C.A. § 17383(b)(2) (2010).

152. *Id.* § 17383(a)(2) (stating the mission of the Smart Grid Advisory Committee, which oversees the SGTF, "shall be to advise the Secretary, the Assistant Secretary, and other relevant Federal officials concerning the development of smart grid technologies, the progress of a national transition to the use of smart-grid technologies and services, the evolution of widely-accepted technical and practical standards and protocols to allow interoperability and inter-communication among smart-grid capable devices, and the optimum means of using Federal incentive authority to encourage such progress").

153. *See generally* YULE KIM, CONG. RESEARCH SERV., STATUTORY INTERPRETATION: GENERAL PRINCIPLES AND RECENT TRENDS 39 (2008).

154. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 405, 123 Stat. 115 (to be codified at 42 U.S.C. § 17384).

developing a smart grid information clearinghouse does not permit the DOE to regulate the cyber security aspects of NUSP-consumer interactions. The DOE has interpreted this responsibility to mean that it must provide "comprehensive and detailed information about the attributes, performance, impacts, costs, and benefits of smart grid technologies, tools, and techniques" through "direct sharing and dissemination of information on knowledge gained, lessons learned, and best practices."[155] Although authority to create the clearinghouse allows the DOE to create an information resource by requiring disclosure of information from smart grid grant applicants, it does not authorize the DOE to do more than collect data and even this power is restricted to entities that apply for a grant award.[156] Thus, this new responsibility does not extend to the DOE the power to regulate NUSP-consumer interactions.

Although the authority to award smart grid grants gave the DOE a small amount of control over NUSP-consumer interactions, the opportunity to exercise this power has passed because the DOE has already issued its grants.[157] The DOE had the responsibility to award smart grid grants, which it interpreted to mean authority to evaluate the cyber security vulnerabilities of proposed smart grid projects and reject those that "cannot provide reasonable assurance that their approach to cyber security will prevent broad based systemic failures in the electric grid in the event of a cyber security breach."[158] It also interpreted this responsibility to allow it to require a potential grant recipient to show that its project would use "open protocols and standards . . . if available and appropriate" to facilitate interoperability by allowing vendors to design and build smart grid equipment and systems that can function in tandem with the approved projects.[159] These interpretations of the DOE's smart grid grant authority allowed the DOE to control the security issues of smart grid grants by rejecting projects that did not meet threshold security standards. However, the DOE has already exercised this grant authority so it cannot further control the security issues related

155. OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, RECOVERY ACT: FINANCIAL ASSISTANCE OPPORTUNITY FUNDING ANNOUNCEMENT 9 (2009), *available at* http://www.bpa.gov/energy/n/smart_grid/docs/1306_Smart_Grid_investment_program_funding_announcement.doc.

156. *See Smart Grid Initiatives and Technologies, supra* note 53, at 5-6.

157. *Will We Get Our Money's Worth? $3.4 Billion in Smart Grid Stimulus Grants Go to 100 Projects*, SMARTGRIDNEWS.COM (Oct. 27, 2009), http://www.smartgridnews.com/artman/publish/Stimulus_News_Digest_News/Will-We-Get-Our-Money-s-Worth-3-4-Billion-in-Smart-Grid-Stimulus-Grants-Go-to-100-Projects-1336.html.

158. OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, *supra* note 155, at 40.

159. Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,113 n.179 (July 16, 2009).

to NUSP-consumer interactions. Thus, unless additional funding is allocated to the DOE under the same authority, the DOE no longer has the ability to regulate NUSP-consumer cyber security concerns via the smart grid grant authority.

4. The FCC—Perhaps Able But Unlikely to Regulate

The ARRA directed the FCC to develop a National Broadband Plan ("NBP") which includes "a plan for use of broadband infrastructure and services in advancing . . . energy independence and efficiency."[160] In turn, the FCC, believing that its role should be to update policies, set standards, and align incentives to maximize broadband use for national priorities, has interpreted this authority to include development of an NBP that takes into consideration the energy sector, smart grid development, and cyber security.[161] Consequently, the FCC has made recommendations in the NBP that seek to modernize the electric grid with broadband so that it is more reliable and efficient and will allow for energy innovation in homes and buildings by making electric usage data readily accessible to consumers.[162]

Although it is difficult to see how the FCC's new authority and agenda fit into the mix of agencies with partial authority over smart grid development, the FCC has interpreted its role to be one of guidance and assistance rather than active involvement. This is evidenced by the FCC's decision to limit its ARRA authority to the narrow meaning of "plan" within its mandate of developing a "plan for use of broadband . . . in advancing . . . energy independence and efficiency."[163] In other words, instead of developing a "plan" that involves active involvement by the FCC, the agency has limited the plan's scope to offering recommendations to the principal agencies, states, and stakeholders that are currently participating in smart grid development.[164] Accordingly, while it is possible for the FCC to adopt a more aggressive interpretation of its role in smart grid development via its ARRA mandate, for the time being it seems likely that the FCC will only have a voice in developing cyber security standards for the smart grid and perhaps NUSPs. Moreover, the FCC may be hesitant to define its role as one of active

160. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 6001(k)(2)(D), 123 Stat. 115 (to be codified at 47 U.S.C. § 1305); *see also* Fed. Commc'ns Comm'n, Comment Sought on the Implementation of Smart Grid Technology, GN Dkt. Nos. 09-47, 09-51, 09-137, NBP Public Notice #2 (2009), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-09-2017A1.pdf.

161. FED. COMMC'NS COMM'N, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 7-11 (2010).

162. *Id.* at xiv.

163. American Recovery and Reinvestment Act of 2009 § 6001(k)(2)(D).

164. *Id.* § 6001(k).

regulation because such a decision would significantly complicate the regulatory landscape by adding another agency to the administrative process. Thus, although the FCC might have regulatory authority to address NUSP-consumer cyber security concerns, it seems unlikely that it will claim this authority.

5. The DHS—No Authority to Regulate

The DHS has some responsibility for addressing the nation's cyber security concerns. However, this responsibility does not extend to the regulation of NUSP-consumer interactions.

The DHS was given responsibility for the cyber security of non-federal entities in the Homeland Security Act of 2002.[165] However, this responsibility was limited to the provision of analysis, warnings, and crisis management support related to threats to, and vulnerabilities of, critical information systems as well as technical assistance (upon request) for "emergency recovery plans for failures of critical information systems."[166] In other words, the DHS has no authority to mandate these standards, but can only suggest them, offer help in implementing them if requested, or help private parties create plans to address cyber security concerns.[167] For instance, the DHS worked with the DOE to create the "Roadmap to Secure Control Systems in the Energy Sector" in 2006.[168] This document outlines a vision of both departments and stakeholders of the electric energy industry in which control systems in the U.S. energy sector will be able to withstand "an intentional cyber assault with no loss of critical function in critical applications."[169] This roadmap merely functions as a framework of goals and milestones for protecting control systems, with no authority to enforce or promote these goals.[170] The roadmap also provides a drawn-out ten-year timetable for accomplishment of these goals.[171] Thus, the DHS does not have

165. Homeland Security Act of 2002 § 223, 6 U.S.C. § 143 (2006).

166. U.S. DEP'T OF HOMELAND SEC., *supra* note 43, at ix; U.S. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 115 (2009) (describing the role of the DHS as "[p]roviding technical assistance to other governmental entities and the private sector with respect to emergency recovery plans").

167. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 43, at 14-15 (describing the narrow way in which the DHS has interpreted its grant of authority under statutes and executive orders, e.g., "[o]ur traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts" and "[b]road regulations mandating how all corporations must configure their information systems could divert more successful efforts by creating a lowest-common denominator approach to cybersecurity.").

168. U.S. DEP'T OF ENERGY & U.S. DEP'T OF HOMELAND SEC., *supra* note 115.

169. *Id.* at 1.

170. *See id.* at 2.

171. *Id.*

authority to regulate NUSP-consumer cyber security concerns on its own. Instead its function is largely one of aiding agencies to develop their own standards.

B. Only PUCs or the FTC's State Analogues Have Authority to Regulate NUSP-Consumer Privacy Concerns

The FERC, the FCC, PUCs, and the FTC and its state analogues are all entities that have some authority to regulate NUSP-consumer privacy concerns. This Section explains why the FERC, the FCC, and the FTC are currently unable to regulate these concerns. It then explains why PUCs and the state analogues of the FTC may be able to do so.

1. The FERC

Under the current regulatory framework, the FERC has authority to adopt the interoperability and functionality standards developed by the NIST.[172] The FERC has interpreted this authority to include the ability to apply these standards to entities all the way down to the retail level.[173] Thus, because the NIST has determined that interoperability and functionality standards should include privacy standards, the FERC has the authority to adopt privacy standards that apply to entities all the way down to the retail level. Further, because NUSPs are retail-level entities that interact directly with consumers, the FERC has the authority to regulate the privacy aspects of NUSP-consumer interactions. However, this regulatory authority is inadequate for proper regulation of NUSP-consumer privacy concerns because it does not include the authority to mandate the adoption of these standards or to enforce them. Accordingly, in order to ensure that the FERC can adequately regulate the privacy aspects of NUSP-consumer interactions, federal legislation must be passed to give the FERC these authorities.

2. The FCC

As noted above, the ARRA gave the FCC new authority to establish an NBP to advance energy independence and efficiency.[174] Although some organizations requested that the FCC take an active role in regulating the privacy aspects of the smart grid via this authority,[175] in

172. *See supra* text accompanying note 118.

173. *See* Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).

174. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 6001(k)(2)(D), 123 Stat. 115 (to be codified at 47 U.S.C. § 1305); *see also* FED. COMMC'NS COMM'N, *supra* note 160, at 1.

175. *See generally* ELEC. PRIVACY INFO. CTR, A NATIONAL BROADBAND PLAN FOR OUR FUTURE (2009) (advocating that the FCC "[s]hould [p]ursue a [w]ide [r]ange of [a]pproaches . . . to [a]ddress [b]roadband [p]rivacy").

the NBP the FCC only noted that "many users are increasingly concerned about their lack of control over sensitive personal data" and warned that "[i]nnovation will suffer if a lack of trust exists between users and the entities with which they interact over the Internet."[176] The FCC then made several recommendations, but, as with cyber security concerns, passed on taking a more active role in regulating privacy concerns with the smart grid.[177] As a result, the FCC will likely not be able to regulate NUSP-consumer privacy concerns unless it takes a more active role under its ARRA authority.

3. The FTC, Its State Analogues, & PUCs

Because the FTC and its state analogues are the primary government agencies with jurisdiction over consumer protection,[178] these are currently the only government entities that may regulate the privacy aspects of NUSP-consumer interactions.

The FTC is charged with protecting consumers from "unfair and deceptive acts or practices in or affecting commerce."[179] The FTC has interpreted this to cover privacy concerns[180] and has recognized the need for protection of consumer privacy at least since 1996.[181] In protecting consumers, the FTC has pursued a policy of self-regulation for cyber commerce in which the only guidelines for regulated entities are the FTC's Fair Information Practice Principles ("FIPPs").[182] These principles require entities to (1) notify consumers of the entity's information practices, (2) receive consent from consumers regarding the information practices, (3) allow consumers to access the information that the entity has on them, (4) secure the consumers' information, and (5) allow consumers to seek redress to enforce the entity's promises regarding the consumers' information.[183] Although the FTC's official policy is self-regulation, the FTC has been actively enforcing the promises of self-regulated entities to consumers through the courts for

176. FED. COMMC'NS COMM'N, *supra* note 161, at 53.

177. *Id.* at 55-57.

178. Some other agencies have a consumer protection role to some extent although it is not their main purpose. For example, the U.S. Environmental Protection Agency controls labeling requirements for pesticides.

179. The Federal Trade Commission Act of 1914, 15 U.S.C. § 45(a)(1) (2006).

180. *See, e.g.*, FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 33 (2000); FED. TRADE COMM'N, PROTECTING CONSUMERS IN THE NEXT TECH-ADE 30 (2008).

181. *See, e.g.*, FED. TRADE COMM'N, ANTICIPATING THE 21ST CENTURY: CONSUMER PROTECTION POLICY IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE 35 (1996).

182. Joseph Turrow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3:3 J.L. & POL'Y FOR INFO. SOC'Y 723, 727-28 (2007).

183. *Fair Information Practice Principles*, FED. TRADE COMM'N, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified June 25, 2007).

over ten years.[184] For example, the FTC has brought suit and obtained settlement from numerous companies that have compromised the financial and/or medical data security of customers.[185] These enforcement actions suggest that the FTC has authority to regulate privacy violations occurring within NUSP-consumer interactions. However, under the FTC's current policy of self-regulation, this authority would not necessarily protect consumers from privacy violations because it would only provide consumers with recourse after their privacy had been violated. In effect, the only protection consumers would receive is some difficult-to-measure degree of protection resulting from the deterrent effect that the threat of suit by the FTC would have on companies. Accordingly, the FTC may have authority to regulate NUSP-consumer privacy concerns. However, it is likely that this level of regulation would be inadequate for preventing privacy violations under the current agency policy of self-regulation.

In addition to the FTC, many states have either a PUC or a separate consumer protection agency enforce state privacy laws.[186] These laws may not be inconsistent with the federal unfair and deceptive trade practice laws that established the FTC. However, the Supreme Court has affirmed the authority of states to establish privacy safeguards that provide stronger consumer protections than federal laws.[187] Accordingly, states may pass laws to regulate NUSP-consumer privacy concerns either through the PUC or the state consumer protection agency. Currently, as found by the NIST through developing interoperability and functionality standards, most state PUCs lack formal privacy policies or standards related to the smart grid, and state privacy laws generally do not address privacy concerns related to the smart grid.[188] Thus, while states have the ability to regulate these privacy concerns, legislation must be passed or regulations must be developed by states to adequately address NUSP-consumer privacy concerns.

184. *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 8, 9 n.17 (2010) (describing enforcement actions taken by the FTC under Section 5 of the Federal Trade Act and listing examples of such cases going back to 1999).

185. *Id.* at 47 & n.20

186. *See* NISTIR DRAFT FEB. 2010, *supra* note 15, at 103.

187. *See* Altria Group, Inc. v. Good, 129 S.Ct. 538, 551 (2008) (holding that state law predicated on a duty not to deceive is not impliedly preempted by various FTC decisions); Am. Bankers Ass'n v. Lockyer, 541 F.3d 1214, 1218 (9th Cir. 2008) (holding that some provisions of a California consumer protection law should be held valid even though other provisions were preempted by federal law).

188. *Id.*

IV. WHICH ENTITY SHOULD REGULATE NUSP-CONSUMER INTERACTIONS?

No government entity has authority to adequately regulate NUSP-consumer cyber security concerns, and although PUCs and the state analogues of the FTC have authority to regulate NUSP-consumer privacy concerns, very few are taking steps to do so.[189] Accordingly, this Part evaluates which government entities would be the optimal choices for regulating NUSP-consumer cyber security and privacy concerns. In making these determinations, the following factors are evaluated as crucial considerations: (1) areas of expertise within government entities, (2) ability to achieve efficiency gains from the streamlining of government functions (e.g. speed in implementing regulation and reduction in regulatory complexity), and (3) likelihood of encountering undesirable side-effects from giving a government entity regulatory authority (e.g. piecemeal regulation and externalities). As such, Section A considers each potential regulator in turn and explains why the FERC should be given authority to regulate NUSP-consumer cyber security concerns. Then, Section B considers each potential regulator in turn and explains why the FERC should also be given authority to regulate NUSP-consumer privacy concerns.

A. The FERC Should Regulate NUSP-Consumer Cyber Security Concerns

1. PUC Regulation Is Not Ideal

While PUCs may have the most expertise for handling localized issues like NUSP-consumer interactions, PUCs are not the best entities to regulate NUSP-consumer cyber security concerns for several reasons: (1) PUC regulation could only be achieved by states individually passing legislation to create this authority, which would not streamline government function and may not be possible due to preemption and Dormant Commerce Clause concerns; and (2) PUC regulation would inevitably lead to undesirable side-effects such as piecemeal regulation and negative externalities between states.

One strong argument for PUC regulation of NUSP-consumer cyber security concerns is that PUCs have the most expertise in handling localized interactions related to the electric grid, such as NUSP-consumer interactions. NUSP-consumer interactions are localized interactions, and PUCs likely have the most expertise in handling localized interactions via experience regulating the retail electricity

189. *See supra* Part II.B.2.

market.[190] This argument assumes that a PUC's knowledge and experience gathered from regulating intrastate retail utility-consumer interactions translates to an advantage in regulating NUSP-consumer interactions. This assumption may be accurate because experience regulating localized interactions is likely to have given the PUC the resources and know-how needed to effectively implement other localized regulations, including regulations related to NUSP-consumer cyber security concerns.[191] Accordingly, it can be argued that regulation by an entity less familiar with localized interactions is likely to be less effective than regulation by a PUC. Less effective regulation could result in delay. It could also result in incomplete, and, consequently, ineffective implementation of regulation, which could lead to completely inadequate cyber security protection. Although this argument is persuasive, it is heavily outweighed by other considerations.

PUCs are poorly suited to regulate NUSP-consumer cyber security concerns because the state statutes that set out PUC regulatory authority do not currently authorize the regulation of these NUSP-consumer interactions,[192] which means that new legislation must be individually passed by states to authorize this regulatory power.[193] This is problematic for multiple reasons. Most importantly states may not have the legal authority to implement such legislation. Congress has already provided the FERC with jurisdiction through the EISA to implement interoperability and functionality standards, which the FERC has interpreted to cover NUSP-consumer interactions.[194] As a result, it is likely that the FERC's interpretation of this delegation may preempt any state legislation that delegates to PUCs the authority to also regulate cyber security concerns under the Supremacy Clause.[195] Additionally, under *Chevron v. Natural Resources Defense Council* a state challenge to the FERC's interpretation of the EISA could easily fail because a reviewing court would give the FERC substantial deference in interpreting the statute if it were held that the statute's language is ambiguous.[196] Lastly, the state would need to be careful in drafting its legislation so that the authority to regulate these interactions did not place undue burden upon out-of-state NUSPs,

190. *See supra* Part III.A.2.

191. *See id.*

192. *See, e.g.,* Joint Comments of the Ctr. for Democracy & Tech. & the Elec. Frontier Found., to the *Order Instituting Rule Making*, RM No. 08-12-009, at 21 (Mar. 9, 2010), *available at* http://www.cdt.org/files/pdfs/20100309_smartgrid_cpuc_comments.pdf (noting that the ability for the California PUC to implement security measures is restricted to "regulable entites" of which this comment posits NUSPs are not).

193. *See supra* notes 135-36 and accompanying text.

194. *See* Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).

195. U.S. CONST. art. VI, cl. 2.

196. Chevron, U.S.A. v. Natural Res. Def. Council, 467 U.S. 837, 843-44 (1984).

thereby potentially violating the Dormant Commerce Clause.[197]

Even assuming that state legislation could be passed and upheld, it is undesirable for states to regulate these interactions because PUC regulation may cause detrimental side-effects. For instance, if PUCs were given regulatory authority over NUSP-consumer cyber security concerns, there would be a risk of creating a piecemeal system of regulation. This could result if not all states decided to create PUC authority over these concerns, or if all states did create this authority but did so at different times or to varying degrees. In such a situation, a piecemeal system of regulation would be created. This is problematic because piecemeal regulation of cyber security could lead to negative externalities between states using an interconnected electric grid. In other words, the decision of one state to regulate NUSP-consumer cyber security concerns could be undermined by the decision of another state to forego such regulation. This could result via a security breach occurring in the state without regulation, which negatively affects the state with regulation due to the nature of an interconnected electric grid. This scenario is particularly relevant to cyber security issues because a person seeking to breach security will invariably seek out the easiest way to do so. Moreover, these issues do not disappear when both states decide to regulate. In such a situation it is still possible, and likely, that the two states will have different amounts of resources and expertise that can be put towards regulating these interactions, which may create the same externalities.[198]

Besides the larger issues already addressed, there are also a variety of practical problems that could result from individual states creating this regulatory authority for PUCs. These include the slow speed of the legislative process, difficulties with party politics, the legislative process's vulnerability to lobbying (which could result in watered-down or ineffective legislation),[199] and statutory language that could unintentionally impede the PUC's regulatory flexibility if drafted too narrowly.[200] Finally, extending the jurisdiction of the PUC to entities that are not public utilities is a step that states may be unwilling to take because states may feel that extending jurisdiction to regulate NUSPs is too much like extending jurisdiction to regulate private businesses. Some states might consider this to be an overreaching of regulatory authority because PUCs conventionally regulate only public utilities.[201]

197. U.S. CONST. art I, § 8, cl. 3.

198. Robert W. Hahn et al., *Federalism and Regulation*, 2004 REGULATION 46, 47.

199. Email from Elias Leake Quinn, Former Senior Policy Analyst, Ctr. for Envtl. & Energy Sec., Univ. of Colo. Law Sch., to author (Jan. 10, 2010) (on file with the Journal on Telecommunications and High Technology Law).

200. *Id.*

201. *See supra* notes 148-50 and accompanying text.

2. DOE Regulation Is Not Ideal

The DOE has significant technical expertise regarding cyber security issues, it has some responsibility to regulate smart grid development, and it is involved with NIST in creating smart grid interoperability and functionality standards.[202] Ultimately, however, the DOE should not be given authority to regulate NUSP-consumer cyber security concerns because (1) this would unnecessarily complicate the electric regulatory framework, and (2) the DOE's technical expertise would be better used for assisting in regulation. Further, the DOE may not want to assume this regulatory responsibility.

The DOE has extensive experience developing security standards for energy control systems.[203] This experience includes: identifying cyber vulnerabilities in energy control systems, working with vendors to develop hardened systems that mitigate cyber security risks, developing more secure communication methods between energy control systems and field devices, developing tools and methods to help utilities assess their security posture, and providing extensive cyber security training for energy owners and operators to help them prevent, detect, and mitigate cyber penetration.[204] This expertise was the reason that the NIST was required to collaborate with the DOE in creating interoperability and functionality standards.[205] However, despite this expertise, it would be undesirable to give the DOE authority to regulate NUSP-consumer cyber security concerns because this would further complicate the electric regulatory framework—something that desperately needs to be streamlined for the smart grid.

Giving the DOE the power to regulate NUSP-consumer interactions would create a new facet to electric regulation outside of the traditional FERC-PUC regulatory scheme and the new interoperability and functionality authority of the FERC. This facet would unnecessarily complicate regulation because the resultant regulatory framework would require the FERC to adopt security standards, but would then charge the DOE with the responsibility to enforce them. This could cause jurisdictional blurring down the road, which, as this Note illustrates, creates uncertainty and can impede regulatory action.[206] Instead of

202. *See Smart Grid Initiatives and Technologies*, *supra* note 53, at 2.

203. *See* U.S. DEP'T OF ENERGY, *supra* note 60, at 2.

204. *Id.*

205. *See Smart Grid Initiatives and Technologies*, *supra* note 53, at 4.

206. *See, e.g.*, Comments of the Nat'l Ass'n of Regulatory Util. Comm'rs, to the *Proposed Policy Statement & Action Plan*, in Smart Grid Policy, Dkt. No. PL09-4-000, at 1 (May 11, 2009), *available at* http://www.naruc.org/Testimony/09%200511_NARUC%20Comments%20on%20FERC%20DRAFT%20POLICY%20STATEMENT.pdf (noting that the FERC's Smart Grid Policy Statement's assertions raise jurisdictional issues that must be resolved to proceed effectively).

creating confusion, uncertainty, and complicating regulation, it would be vastly more beneficial to streamline regulatory authority and jurisdictional boundaries (especially for the already confusing regulatory landscape of smart grid development). Perhaps a more preferable role for the DOE would be one similar to that which it occupies for the NIST standards: the DOE could serve as an adviser to the FERC on technical cyber security issues that may arise during regulation of NUSP-consumer cyber security concerns. Under this scenario the DOE would still be able to offer its expertise to secure the grid from these concerns, but the regulatory framework would not become more complicated.

Lastly, it is possible that the DOE may not want to regulate NUSP-consumer cyber security concerns. The Assistant Secretary for the Office of Electricity Delivery and Energy Reliability at the DOE has testified before the House Subcommittee on Energy and Environment regarding the DOE's "recommended courses of action" for dealing with security issues associated with smart grid development.[207] Nowhere in those recommendations were calls for legislation or delegation of additional authority to the DOE.[208]

3. FCC Regulation Is Not Ideal

Like the DOE and the DHS (as discussed below), the FCC has agency expertise that may be helpful in regulating NUSP-consumer cyber security concerns. However, the FCC has no experience regulating the electric grid. Consequently, it is counterintuitive and out-of-place to put it in charge of regulating these concerns because the FCC's involvement in regulating the grid would lead to increased regulatory complexity and decreased efficiency. Although the FCC may play a role in assisting the more traditional regulatory players via its NBP and ARRA authority, the FCC would not be the optimal choice for regulating NUSP-consumer cyber security concerns.

4. DHS Regulation Is Not Ideal

Although the DHS has some responsibility for addressing cyber security concerns, it is not the proper entity to regulate these interactions because the DHS has expertise in aiding other agencies with cyber security concerns but no experience in implementing cyber security standards. As a result, DHS regulation could lead to ineffective implementation of cyber security standards.

---

207. *See Effectively Transforming Our Electric Delivery System to a Smart Grid: Hearing Before the Subcomm. on Energy & Env't of the H. Comm on Sci. & Tech.*, 111th Cong. 15-16 (2009) (statement of Patricia Hoffman, Acting Assistant Secretary, Office of Electricity Delivery and Energy Reliability, Dep't. of Energy).

208. *Id.*

As noted above,[209] the role of the DHS in developing cyber security standards has largely been one of aiding agencies to develop their own standards rather than controlling the creation and implementation of standards. This is significant because this traditional function likely means that the DHS has significant agency expertise in helping agencies decide what types of standards to implement but no actual expertise in implementing such standards itself. Thus, the DHS would likely require more time to obtain the necessary personnel to adequately regulate NUSP-consumer cyber security concerns than other agencies that already have staffs with such regulatory experience. Consequently, for efficiency and efficacy reasons, it is beneficial to give authority to regulate NUSP-consumer cyber security concerns to a government entity that can assume this responsibility with less effort.

5. FERC Regulation Is Optimal

The FERC should regulate NUSP-consumer cyber security concerns because (1) federal regulation would avoid preemption and piecemeal regulation issues related to state regulation, (2) FERC regulation would contribute to streamlined regulation of the smart grid, which would in turn lead to more efficient and perhaps more effective regulation, (3) the FERC has expertise in implementing and enforcing regulatory standards on the grid via its EPAct of 2005 reliability authority, and (4) FERC regulation would be the simplest option, requiring the passage of minimal legislation or reinterpretation of the FERC's interoperability and functionality standards authority under the EISA.

As noted above, leaving the regulation of NUSP-consumer cyber security concerns to states may not be possible and, if possible, may result in ineffective regulation. Accordingly, federal regulation is more appropriate for NUSP-consumer cyber security concerns. Of the federal entities that could regulate NUSP-consumer cyber security concerns, the FERC is the best suited because it already has experience developing cyber security standards to address these concerns.[210] As a result, the FERC has personnel and resources already allocated to this area, allowing the agency to assume this additional authority with minimal effort.[211]

209. *See supra* Part III.A.5.

210. *See Smart Grid Initiatives and Technologies, supra* note 53, at 4; Smart Grid Policy, 74 Fed. Reg. 37,098 (July 16, 2009).

211. For example, the FERC has a smart grid webpage, a smart grid policy statement, and various other policy documents and congressional testimonies dedicated to addressing the role of the FERC and its involvement in the interoperability and functionality standards, including their cyber security standards aspect. *Smart Grid*, *supra* note 8 (select links under "Quick Links").

Deciding to delegate this authority to the FERC would also concentrate regulatory authority in the FERC instead of unnecessarily dividing it among other agencies. Concentrating authority in the FERC would be beneficial because it would streamline federal regulation of the smart grid, thus creating clearer departmental roles, and, subsequently, increased regulatory efficiency and effectiveness. This may happen because clearer departmental roles reduce uncertainty as to which government agency will regulate. And this, in turn, is beneficial for several reasons. First, it reduces the need for regulators to make difficult and time-consuming jurisdictional decisions. Second, because regulated entities know more quickly and with greater certainty which regulators have authority, regulated entities, too, can act more quickly and with greater faith that they will not face unanticipated regulatory requirements.

Furthermore, streamlining of federal regulation will reduce complexity and confusion in the regulatory framework.[212] The value of this effect has been noted implicitly by the statements of cyber security experts, who caution about the current "lack of transparency and dearth of defined departmental roles and responsibilities in addressing cyber-related issues from a comprehensive national approach."[213] Lastly, streamlining can increase regulatory efficiency by helping to avoid vulnerabilities in regulation caused by inconsistent regulations from multiple agencies.[214] Thus, extending the FERC's jurisdiction to regulate NUSP-consumer cyber security concerns is desirable because it can lead to increased regulatory efficiency and efficacy.

Finally, allowing the FERC to regulate NUSP-consumer cyber security concerns would require less effort than creating a new authority for a different federal agency. To allow the FERC to regulate these concerns would either require the passage of minimal legislation extending the FERC's current interoperability and functionality standards authority under the EISA, or it would require the FERC to

212. Regulatory streamlining is commonly pursued when trying to achieve regulatory efficiency, cost-effectiveness, and regulatory certainty. For instance, streamlining efforts pursued by U.S. federal agencies include streamlining of the regulation of construction, both generally and for nuclear power. *See, e.g.*, NAT'L P'SHIP TO STREAMLINE GOV'T, http://www.natlpartnerstreamline.org (last visited Feb. 11, 2011) (noting enormous cost savings and increased efficiency as a result of streamlining efforts in the regulation of general construction); DEP'T OF ENERGY, THE ECONOMIC FUTURE OF NUCLEAR POWER: A STUDY CONDUCTED AT THE UNIVERSITY OF CHICAGO (2004) (describing streamlining of the nuclear power permitting process).

213. CATHERINE A. THEOHARY & JOHN ROLLINS, CONG. RESEARCH SERV., CYBERSECURITY: CURRENT LEGISLATION, EXECUTIVE BRANCH INITIATIVES, AND OPTIONS FOR CONGRESS 7 (2009).

214. *Id.* at 7-8.

reinterpret this existing authority.[215] These options are simpler to accomplish than passing legislation to create an entirely new function for a different agency.[216] For instance, although numerous factors contribute to the difficulty in passing legislation, it is arguable that extending the regulatory authority of an agency that nearly enjoys this authority already is easier to achieve than obtaining consensus that a bill should be passed to allow an agency with less regulatory authority in that area to have wholly new powers. Thus, for the foregoing reasons, the FERC is the optimal choice for regulation of NUSP-consumer cyber security concerns.

B. The FERC Should Regulate NUSP-Consumer Privacy Concerns

Although the FTC and its state analogues are the traditional government agencies with jurisdiction over consumer protection, and although these entities and PUCs may regulate NUSP-consumer privacy concerns after taking certain steps,[217] the FERC is best suited to regulate these concerns. FERC regulation is the optimal choice because (1) the FERC has more experience regulating the electric grid than the FTC or state analogues, (2) the FERC has experience mandating and enforcing standards from its reliability authority, (3) PUCs are likely to encounter piecemeal regulation issues, and (4) allocating regulatory authority to the FERC will streamline federal regulation of the smart grid. Thus, either the FERC should reinterpret its interoperability and functionality standards authority to include the authority to mandate and enforce the privacy standards for the smart grid being developed by the NIST, or federal legislation should be passed to give the FERC this authority.

The FERC has decades of experience regulating the electric grid, whereas the FTC and its state analogues have no experience regulating the grid.[218] Expertise translates into a better ability to regulate because agencies with expertise better understand what manner of regulation works best. In addition, agencies with expertise do not need to familiarize themselves with an area of regulation, allowing them to implement regulation more quickly than agencies with less expertise.

---

215. *See Smart Grid Initiatives and Technologies*, *supra* note 53, at 2; Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).

216. This argument assumes that political feasibility is lower when legislation with a broad, as compared to a narrow, purpose is needed.

217. As noted in Part III.B.3, the FTC would need to change its policy of self-regulation to actively regulate these concerns, and the states would need to either allow their PUCs to enact regulations to control NUSP-consumer privacy concerns or pass legislation allowing the state's consumer protection agencies to take on that responsibility.

218. *See Students' Corner, What is FERC?*, U.S. FED. ENERGY REG. COMM'N, http://www.ferc.gov/students/whatisferc/history.htm (explaining that FERC regulation dates back to the formation of the predecessor of the FERC, the Federal Power Commission, in 1920) (last visited Feb. 11, 2011).

Because the smart grid is complex and is developing quickly, effective and timely regulation is crucial. Thus, one reason that the FERC is a better choice than the FTC or its state analogues for regulating NUSP-consumer privacy concerns is that it is likely to be better able to keep pace with smart grid development.

It is also preferable to give the FERC authority to regulate NUSP-consumer privacy concerns rather than the FTC or its state analogues because the FERC has related experience mandating and enforcing standards from its reliability authority under the EPAct of 2005.[219] Experience enforcing standards makes the FERC a strong candidate for similar regulatory authority because the FERC could simply adjust its current enforcement practices to include these additional standards. However, the FTC or its state analogues might have more difficulty adjusting to a regulatory role that they are less familiar with fulfilling.

The FERC is a preferable entity for regulating NUSP-consumer privacy concerns because in exercising this authority, the FERC acts as a single entity and therefore will not run into piecemeal regulation issues. Piecemeal regulation is particularly problematic when unified policy is needed for effective regulation. In the case of cyber security, this is a paramount concern because cyber security of the grid is dependent upon effective regulation of the entire grid. It is unclear whether or not piecemeal regulation of NUSP-consumer privacy concerns presents the same degree of danger to the privacy of all users of the grid. However, common sense advises that in deciding how to best regulate these privacy concerns, it is better to err on the side of caution and avoid piecemeal regulation. This may be preferable due to the interconnected nature of the grid and networks that are the hallmark of the smart grid. Additionally, in consideration of the rapid speed of smart grid technology development, it is likely more sensible to seek uniform regulation and avoid needing to re-delegate authority at a later time due to a later-found shortcoming of piecemeal regulation.

Lastly, in the same vein as the analysis of cyber security regulation, it is prudent to consider how tangential authorities are allocated when deciding how to delegate regulatory authority over privacy concerns. The FERC is the optimal choice for regulating NUSP-consumer cyber security concerns via its interoperability and functionality standards authority. However, the interoperability and functionality authority extends to privacy concerns as well. Accordingly, it may be disadvantageous to allow the FERC to regulate the cyber security aspects of NUSP-consumer interactions, but to not regulate these interactions' privacy aspects. For example, a decision to aggregate or streamline

219. *Office of Enforcement*, FED. ENERGY REG, COMM'N, http://www.ferc.gov/about/offices/oe.asp (last updated Feb. 25, 2011).

regulatory authority over the smart grid rather than to divide it among multiple agencies might increase efficiency by reducing regulatory complexity. Complexity not only makes it difficult for regulated entities to understand what authorities they report to, but it also makes it difficult for regulators to act because regulatory actions will require difficult jurisdictional decisions. Thus, in the interest of streamlining the federal government regulation of the smart grid, this authority should be delegated to the FERC.

CONCLUSION

NUSP-consumer interactions pose a danger to the security of the electric grid and to the privacy interests of its users. Because no government entity currently has the authority to effectively regulate these interactions, regulatory authority must be extended to cover them. The FERC is the most attractive candidate to assume this authority because it already has the power to promulgate non-compulsory standards for NUSP-consumer cyber security and privacy concerns under its interoperability and functionality standards authority. Accordingly, either the FERC should reinterpret its interoperability and functionality standard authority to encompass the ability to mandate or enforce the NIST's cyber security and privacy standards, or legislation should be passed to extend this authority to the FERC. Failing to address these concerns will likely result in the continued ineffectual regulation of NUSP-consumer interactions. Such ineffectual regulation could potentially result in the invasion of consumer privacy interests or the endangerment of the electric grid—things that unarguably should be avoided.