**LSU Journal of Energy Law and Resources**

Volume 5 | Issue 2
*Journal of Energy Law & Resources -- Spring 2017*

# Smart Home Alone: The World's Gateway to More Efficient Use of Energy and Mayhem

Chanse J. Barnes

# Smart Home Alone: The World's Gateway to More Efficient Use of Energy and Mayhem

## INTRODUCTION

The future is finally here; the possibility of automated toasters and dishwashers is right around the corner. Currently, homes are undergoing an amazing technological transformation—one aimed at making lives more convenient and manageable. Perhaps the best part of this transformation are the environmental benefits it provides, making each home an efficient consumer of energy with little to no effort by its inhabitants. Welcome to the world of the Internet of Things (IoT) and Cyber-Physical Systems (CPS),[1] the technology behind this amazing transformation. This particular technology has led to improvements in the U.S.'s power grid[2] and advances within our homes collectively known as the "Smart Grid."

The technology used to make homes "smarter" both helps consumers save on their energy bills and reduce stress on the power grid. Modern homes are outfitted with appliances like a smart thermostat, which learns consumer habits and automatically adjusts the temperature of the home based on factors including whether one is home, awake, or sleeping. This technology also allows the smart thermostat to connect and control other smart appliances in the home, including smart lamps, washers, and dryers.

Unfortunately, this technology has a dark side that has not been sufficiently addressed. Looming issues involve the dangers that lurk when consumers, industry leaders, and legislators leave the smart home alone.

---



1. For a detailed discussion of the terms IoT and CPS, *see infra* Part I.B. There is disagreement regarding the relationship between IoT and CPS. The three possibilities include: (1) IoT is a form of CPS; (2) Both terms refer to the same concept and are interchangeable; or (3) IoT and CPS are distinct but similar concepts. This debate is outside the scope of this article, but this comment will treat IoT as a form of CPS. *See generally* Ivan Sojmenovic, *Machine-to-Machine Communications with In-Network Data Aggregation, Processing, and Actuation for Large-Scale Cyber-Physical Systems,* 1 IEEE INTERNET OF THINGS J. 122 (2014), ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6766661 [https://perma.cc/P74P-LXC6]; Eric Simmon et al., *Designing a Cyber-Physical Cloud Computing Architecture*, 17 IT PROFESSIONAL 40 (2015), ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7116443 [https://perma.cc/MXY7-U8XV]; David Sousa Nunes et al., *Survey on Human-in-the-Loop Applications Towards an Internet of All*, 17 IEEE COMM. SURVEYS & TUTORIALS 944 (2015), ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7029083 [https://perma.cc/G9MU-WGW3].

2. The power grid refers to the U.S. electricity delivery system, which generates electricity and transmits it to customers. *See* STAN MARK KAPLAN, CONG. RESEARCH SERV., R40511, ELECTRIC POWER TRANSMISSION: BACKGROUND AND POLICY ISSUES 1–2 (2009).

Imagine that within the smart thermostat, which connects to all smart devices synced to Wi-Fi in your home, the sensor device that determines whether you are home malfunctions. That malfunction, which causes the system to think no one is home, triggers the thermostat to turn off the entire home. This occurs despite the fact that the homeowner is screaming at the thermostat to turn the lights back on. The homeowner is now forced to spend the evening in darkness because his home lacks the ability to manually operate the light switches.

Now, imagine that all of these malfunctions have occurred because someone hacked into the smart home; not a single device, but the entire home. One hacker uses the smart thermostat to determine when the homeowner is not home so he can plan the perfect time to snoop. Another hacker is more nefarious and uses that same smart thermostat to connect to your smart meter. That hacker uses your thermostat-meter connection as a pathway into the Smart Grid itself. He manages to shut down the entire power grid in the region just as that region is going through the worst drought in its history. This means no water, no power, and no electricity. Unfortunately, this hypothetical catastrophe is much more possible than one may first assume.

Modernizing the power grid and homes through IoT and CPS increases the connectivity of many devices which creates pathways for cyber attack. Thus, the continued development of the grid undermines important security concerns that must be considered in preventing a kinetic cyber attack, such as the one presented in the hypothetical above. Any progress made in addressing these concerns will be undone by the inadequate security of smart devices in the home and insufficient oversight by technological developers. The weakest link in the current Smart Grid infrastructure, the "smart home," must become a priority for Smart Grid policy makers in developing a more secure power grid. Such a priority requires more direction and control over developers and service providers involved in the smart home. Securing the smart home will be crucial for security of the entire power grid.

Part I of this Comment provides a brief overview of the current regulatory environment, explains the technology behind the Smart Grid and the smart home, and details the new business developing around the smart home. Part II discusses how the security risks associated with IoT and CPS technology can lead to an attack, not only of the home, but on the power grid as a whole. Part III analyzes how the current regulatory regime fails to adequately address important issues related to the security of the smart home. In light of those issues, Part IV presents a solution to make smart home security a priority in the continuing development of the Smart Grid.

## I. BACKGROUND

Although poorly defined, the Smart Grid can best be understood as "an intelligent energy platform . . . that permits the integration of a wide variety of new applications into the power grid."[3] More concretely, the Smart Grid is the continuing evolution of an electrical power grid that involves implementing various technologies on current or traditional grid infrastructure in an effort to promote more efficient generation, distribution, and use of energy.[4] The new Smart Grid is being built upon the traditional grid infrastructure in a technical and legal sense.[5] The Smart Grid also represents a convergence of energy and telecommunications in technology and policy[6] and includes many benefits.[7]

The Smart Grid's infrastructure consists of four parts: (1) power generation; (2) transmission; (3) distribution; and (4) end-use.[8] The smart home represents the "end-use" portion of the infrastructure.[9] Although ill-defined like the Smart Grid, the smart home can be understood as the aggregate of the technological improvements and advancements being made in the traditional home.[10] The smart home is very important to the Smart Grid infrastructure for many reasons, particularly because of the smart home's role in the Smart Grid's advanced metering infrastructure.[11]

---

3. H. Russell Frisby, Jr. & Jonathan P. Trotta, *The Smart Grid: The Complexities and Importance of Data Privacy and Security*, 19 COMMLAW CONSPECTUS 297, 301 (2011).

4. *See, e.g.*, *id.*; Symposium, *Cyber-Physical Systems: A Security Perspective*, 2015 20th IEEE European (2015) [hereinafter Security Perspective].

5. Christopher Bosch, Note, *Securing the Smart Grid: Protecting National Security and Privacy Through Mandatory, Enforceable Interoperability Standards*, 41 FORDHAM URB. L.J. 1349, 1354 (2015). The infrastructure and regulatory environment of the power grid, as it existed prior to recent Smart Grid modernization efforts, serves as the foundation for its continued development. *Id.*

6. Frisby & Trotta, *supra* note 3, at 299.

7. Smart Grid benefits include: (1) helping integrate renewable resources; (2) allowing for communication of "near-real-time consumption information" between utilities and consumers; (3) allowing the grid to "sense problems quickly and respond effectively;" (4) adjusting to "variations in output by drawing energy from other sources when needed;" and (5) allowing for advanced energy storage practices which means "energy can be stored for later consumption when it is least expensive to generate, allowing for reduced peak loads." Bosch, *supra* note 5, at 1358–61.

8. Security Perspective, *supra* note 4.

9. *Id.*

10. *Id.* (stating that the home, like the grid, is also categorized by a shift "towards the integration of intelligent control systems").

11. For a detailed discussion of the advanced metering infrastructure, *see infra* Part I.C.

Industry leaders and Smart Grid regulators are pushing for greater interoperability[12] within the Smart Grid. Although greater interoperability would be beneficial, if unchecked, this policy will lead to a kinetic cyber attack. Kinetic attacks "us[e] weapons that rely on energy—blast, heat, and fragmentation, for example—to cause their damage."[13] A kinetic cyber attack uses cyber means[14] to effect a kinetic attack.[15] A kinetic attack can be so severe that it leads to "an industry-defined Severe Event, namely one so damaging that afterwards the electricity services remain degraded for months or years."[16] The risk of a kinetic cyber attack on the grid is already real,[17] but unchecked development of the smart home will only increase the danger of this national security threat. Comprehending the risk of a kinetic cyber attack requires an understanding of the technology behind the smart home and the Smart Grid, primarily the concepts of CPS and IoT. Analysis of the threat of kinetic cyber attack also requires an examination of how the new business that is developing around the home coupled with the current state of Smart Grid regulation contributes to this risk.

### *A. The Current Regulatory Environment*

Compared to the rapid technological growth of the power grid, regulatory change has been rather sluggish. Regulation of the grid involves

12. Interoperability is defined *infra* Part I.A.2.

13. Roland L. Trope et al., *Article: Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid,* 40 WM. MITCHELL L. REV. 647, 652 n.12 (2014). CPS and IoT are important to the evolution of the power grid and the home because they impact society, the economy, and the environment. *See* Security Perspective, *supra* note 4. Society is more aware of the planet's limited resources, and CPS and IoT help make important physical processes more efficient. Kyoung-Dae Kim & P.R. Kumar, *Cyber-Physical Systems: A Perspective at the Centennial,* 100 PROC. OF THE IEEE, 1287 (2012), ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6176187 [https://perma.cc/H8YL-H5VW]; Ahmad-Reza Sadeghi et al., *Security and Privacy Challenges in Industrial Internet of Things*, 52 Proceedings of the 52nd Annual Design Automation Conference 1 (2015). For example, CPS and IoT influence energy consumption in the home and, more generally, energy generation and distribution for the grid.

14. Use of communication pathways serve as an example of "cyber means." *See* SCOTT D. APPLEGATE, THE DAWN OF KINETIC CYBER 1, 6 (2013), ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf [https://perma.cc/89TC-KYYX].

15. *See* Trope et al., *supra* note 13, at 652–54.

16. *Id.* at 652–53.

17. *See* APPLEGATE, *supra* note 14, at 2 ("Generally, the main targets for kinetic cyber attacks are cyber physical systems").

multiple jurisdictions,[18] but it is still primarily governed by two primary actors: the Federal Energy Regulatory Commission (FERC) and individual state Public Utility Commissions (PUCs). With this federal and state division, and the complexity of energy regulation, the current regulatory regime is unequipped to handle the evolution of the power grid, specifically the creation of communication networks that transcend state lines.

*1. The Important Actors: FERC and State PUCs*

The most important actors in the current regulatory landscape are PUCs and FERC. PUCs regulate retail sales of electricity and distribution services.[19] FERC has regulatory authority over the interstate wholesale of electricity and interstate transmission of electricity.[20] FERC also has the authority to enforce reliability standards for the bulk power system.[21] The PUCs' ability to regulate is seen as a natural exercise of state power, whereas the federal government's limited ability to regulate is an exercise of Congress' Commerce Power.[22] The Federal Power Act (FPA),[23] the Energy Policy Act of 2005 (EPAct),[24] and the Energy Independence and Security Act (EISA)[25] together establish FERC's jurisdictional authority.

*2. Current Federal Legislation*

Because they establish FERC's jurisdiction over the Smart Grid, the FPA, the EPAct, and EISA represent the most relevant federal legislation for this Comment. The FPA establishes FERC's authority to regulate "matters relating to generation," the interstate transmission, and the

18. Federal, state, and local actors are all involved at some stage of Smart Grid regulation. Joel B. Eisen, *Smart Regulation and Federalism for the Smart Grid,* 37 HARV. ENVTL. L. REV. 1, 20–21 (2013) ("Both the states and the federal government have jurisdiction over parts of the Smart Grid. Depending on which part of the system is involved, either FERC, a state PUC, or the governing council or board of a municipal or cooperative utility has jurisdiction.").

19. *Id.* at 17.

20. 16 U.S.C. § 824 (2012).

21. 16 U.S.C. § 824o. The bulk power system includes "facilities and control systems necessary for operating an interconnected electric energy transmission network" and "electric energy from generation facilities needed to maintain transmission system reliability." 16 U.S.C. § 824o(a)(1)(A)-(B).

22. Elec. Bond & Share Co. v. Sec. & Exch. Comm'n, 92 F.2d 580, 588 (2d Cir. 1937) ("Congress has paramount authority to regulate the transmission or sale for transmission of gas and electric energy across state borders."), *aff'd*, 303 U.S. 419 (1938).

23. 16 U.S.C. §§ 791–823(d) (2012).

24. The relevant portion of this Act can be found at 16 U.S.C. § 824 (2012).

25. Energy Independence and Security Act, 42 U.S.C. §§ 17001–17386 (2007).

interstate sale of energy at wholesale.[26] FERC's authority to create mandatory reliability standards is established under the EPAct.[27] Facilities used in the local distribution of electricity are specifically excluded from FERC's authority and remain under the exclusive jurisdiction of the states.[28]

Reliability standards provide for, among other things, cyber security protection.[29] FERC works with the North American Electric Reliability Corporation (NERC) to create these reliability standards.[30] Although, NERC develops the standards, FERC must approve the standards in full for the standard to be given regulatory effect.[31] Furthermore, FERC can only approve a proposed standard if it determines that the standard is "just, reasonable, not unduly discriminatory or preferential, and in the public interest."[32]

EISA represents the federal government's policy to support the adoption of Smart Grid technologies throughout the nation.[33] In achieving this goal, EISA encourages the development of interoperability standards that are "technologically neutral and sufficiently flexible."[34] Interoperability deals with the communication paths between devices and other actors in the Smart Grid infrastructure. Therefore, the goal of developing interoperability standards is to create a "language" that all devices speak regardless of the manufacturer, so that the entire grid infrastructure works properly.[35] Interoperability is an important goal for Smart Grid success, but it does not encompass all of the issues surrounding communication.[36]

---

26. 16 U.S.C. § 824.
27. "Reliability standards" are standards for "existing bulk-power systems and facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities." 16 U.S.C. § 824o(a)(3).
28. *See* 16 U.S.C. § 824o(a)(1).
29. 16 U.S.C. § 824o(a)(3).
30. Bosch, *supra* note 5, at 1378. NERC is an international, not-for-profit institution of users and operators of the bulk-power system. *See, e.g.*, *id.*; *About NERC,* NERC, nerc.com/AboutNERC/Pages/default.aspx [https://perma.cc/X2UR-VVDF] (last visited Feb. 21, 2017). NERC is the Electric Reliability Organization that was certified by FERC in 2006 pursuant to 16 U.S.C. § 824o(a)(2)'s requirement. *See About NERC.* NERC, nerc.com/AboutNERC/Pages/default.aspx [https://perma.cc/X2UR-VVDF] (last visited Feb. 21, 2017); *see also* 16 U.S.C. § 824o(a)(2) and (c).
31. *See* 16 U.S.C. § 824o(d).
32. 16 U.S.C. § 824o(d)(2).
33. 42 U.S.C. § 17381 (2012).
34. Frisby & Trotta, *supra* note 3, at 308.
35. Bosch, *supra* note 5, at 1380.
36. *See* discussion *infra* Part II.A (detailing issues of two-way communication).

EISA gave the National Institute of Standards and Technology (NIST) the responsibility for creating interoperability standards.[37] In developing these standards, FERC named with six priorities, including cyber security.[38] NIST accepted FERC's priorities with the addition of two more priorities.[39] The process of developing interoperability standards gives the responsibility to NIST to work with federal and state agencies, along with private organizations to develop interoperability standards.[40] NIST then presents these standards to FERC for approval, and if FERC comes to a "sufficient consensus,"[41] it will adopt them.[42] However, the process for creating these standards has proven ineffective, as only voluntary standards have developed.[43]

*3. Other Federal Actors*

EISA also affects other entities in the development of the Smart Grid. EISA charges the Department of Energy (DOE) with the obligation of creating multiple entities dedicated to research, development, and organizing the efforts of other entities in one form or another.[44] The first of these obligations is to create the Smart Grid Advisory Committee,

37. Bosch, *supra* note 5, at 1379–80. In the interoperability standard development process, NIST has the primary responsibility of coming up with the standards. *See* 42 U.S.C. § 17385. NIST not only works with FERC to develop interoperability standards, but also works with the DOE's OEDER, SGTF, SGAC, and "other relevant Federal and state agencies." Frisby & Trotta, *supra* note 3, at 308.

38. The complete list of the six priorities are: (1) system security (*i.e.*, cybersecurity); (2) inter-system communication and coordination; (3) wide are situational awareness; (4) demand response; (5) electric storage; and (6) electric transportation. *See* Smart Grid Policy, 74 Fed. Reg. 37098–37101(Jul. 27, 2009) (to be codified at 18 C.F.R. chap. I).

39. These additional priorities are automation of advanced metering and automation of distribution systems. Frisby & Trotta, *supra* note 3, at 311.

40. Some of these private organizations include: GridWise Architecture Council, the International Electrical and Electronics Engineers, the North American Electric Reliability Corporation, and the National Electrical Manufacturer's Association. 42 U.S.C. § 17385(a)(2).

41. This term was not defined by Congress and is an issue in the entire adoption process of interoperability standards. Bosch, *supra* note 5, at 1380.

42. 42 U.S.C. § 17385(d). The enforceability of standards that have been adopted has been questioned. *See* Bosch, *supra* note 5, at 1380.

43. *See infra* Part III.B.

44. EISA also charges DOE with the primary responsibility of "funding Smart Grid research and development efforts, as well as regional demonstration projects to exhibit the potential benefits of Smart Grid investments." *See* Frisby & Trotta, *supra* note 3, at 306; 42 U.S.C. § 17384(b). DOE is also responsible for "developing and establishing procedures for Smart Grid Investment grants." Frisby & Trotta, *supra* note 3, at 306.

whose purpose is to advise DOE and other relevant federal entities about the ongoing evolution of interoperability standards within the Smart Grid.[45] EISA also charges DOE with creating the Smart Grid Task Force (SGTF).[46] The SGTF is tasked with overseeing the traditional power grid's transition into the Smart Grid.[47] The scope of SGTF's responsibility includes carefully studying key interactions on the grid.[48] Most notable is oversight of interactions between Smart Grid technology, utility regulation, and system security.

With regard to the states, "EISA creat[ed] two new standards for state regulatory commission consideration under Title I of the Public Utility Regulatory Policies Act,"[49] including: (1) demonstrating consideration of adopting Smart Grid technology, and (2) necessity of states to come up with cost recovery methods for Smart Grid development.

### *B. CPS and IoT: Gateway to the Future*

Grasping the deficiencies of the current regulatory environment requires an understanding of the technology behind the Smart Grid: CPS and IoT. CPS does not have a single, mutual definition,[50] but, in an abstract sense, it is a system that creates a bridge between the cyber-world and the physical world.[51] This bridge is created through a system of embedded

45. *See* Frisby & Trotta, *supra* note 3, at 306.

46. SGTF "consists of representatives from DOE's Office of Electric Delivery and Energy Reliability (OEDER)." *Id.*

47. *Id.*

48. *Id.*

49. *Id.* at 309 n. 62.

50. Although the term CPS is fairly new, CPS can be understood as a continuation of a series of technological advancements. Kim & Kumar, *supra* note 13. Thus, CPS has been referred to as the "*next generation* of engineered systems." *Id.* An engineered system is "a combination of components that work in synergy to collectively perform a useful function." *What's an Engineered System*, ENG'G RESEARCH CENTERS, erc-assoc.org/content/what%E2%80%99s-engineered-system [https://perma.cc/B5WV-FY75] (last visited Feb. 21, 2017). The Massachusetts Institute of Technology defines an engineering system in two ways, the relevant definition for this comment being: "a class of systems characterized by a high degree of technical complexity, social intricacy, and elaborate processes, aimed at fulfilling important functions in society. Such systems include electrical grids, transportation, manufacturing supply chains, and health care delivery." *Engineering Systems FAQs,* MIT ENG'G SYS. DIV., esd.mit.edu/about/faqs.html [https://perma.cc/RU2Q-42JA] (last visited Feb. 21, 2017).

51. Ragunathan Rajkumar et al., *Cyber-Physical Systems: The Next Computing Revolution*, 2010 47th ACM/IEEE Design Automation Conference (DAC) 731 (2010), ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5523280 [https://perma.cc/J937-6BF5].

devices that control and interact with the physical environment.[52] These devices represent an integration of computation, communication, and control.[53] Particularly important to the Smart Grid and the smart home is real-time computation[54] and communication networks.[55] Together with sensing technology, CPS devices are able to collect data about the physical environment, share that data with other interconnected devices on the same network, and eventually affect the physical environment.[56]

Likewise, the growing phenomenon of IoT can also impact the environment.[57] IoT shares many characteristics with CPS and can even be considered a form of CPS.[58] Similar to CPS, IoT is a network made up of physical objects embedded with communicating, sensing, measuring, and

52. An embedded device is an object that has been incorporated with technology, giving the object the ability to perform functions that would otherwise be provided by separate, independent software. *See* HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 470, 1149 (28th ed. 2014). An embedded device can either be fixed in design to perform one specific application, or it can be programmable to perform multiple or general functions. *Id.* at 470. An example of a device with a fixed design would be a controller on a fan that has fixed speeds. Conversely, a smart phone is an example of a general purpose device that is programmable.

53. Rajkumar et al., *supra* note 51. Communication is "the transmission of data from one computer to another, or from one device to another." *Communications.* WEBOPEDIA, webopedia.com/TERM/C/communications.html [https://perma.cc/D2T7-CNHD] (last visited Feb. 21, 2017).

54. *See infra* Part I.C. Real-time computation involves scheduling computational tasks so that they are completed before a deadline. *See* Kim & Kumar, *supra* note 13, at 1288.

55. *See* Kim & Kumar, *supra* note 13, at 1302. Communication and real-time computation technology contribute to more efficient use and more responsive and reliable energy production and distribution. For a more detailed discussion of how communication and real-time computation affect the Smart Grid and Smart home, *see infra* Part I.C.

56. Kim & Kumar, *supra* note 13, at 1288.

57. IoT is experiencing rapid growth because of its increased use in familiar consumer objects, such as our cellular phones. Scott R. Peppet, *Article: Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent,* 93 TEX. L. REV. 85, 90–91 (2014) (Quoting the now former FTC Commissioner Julie Brill, "On the Internet of Things, consumers are going to start having devices, whether it's their car, or some other tool that they have, that's connected and sending information to a number of different entities, and the consumer might not even realize that they have a connected device of that the thing that they're using is collecting information about them."). IoT consumer devices are now more feasible due to the decrease in cost to produce the necessary technology. *See id.* at 98 (stating that the cost of sensors used in IoT devices has decreased from twenty-five dollars per unit to less than one dollar per unit allowing the sensors to be "incorporated into consumer products available at scale.").

58. *See supra* note 1.

computing technology.[59] One of the more important aspects of IoT technology is Microelectromechanical systems (MEMS) sensors.[60] MEMS sensors are embedded in physical objects and allow the embedded device to "translate physical phenomenon, such as movement, heat, pressure, or location into digital information."[61] By connecting embedded devices to the Internet, the devices are able to communicate, or transfer, this digital information with data centers.[62] The data centers interpret the data it receives, and then sends back more data to the device, allowing the device to react to the environment.[63] Altogether, this makes a "giant network of connected 'things'"[64] that connects "people [to] people, people [to] things, and things [to] things,"[65] illustrating another aspect where communication is critical.

### *C. Change is Coming: How IoT and CPS are Reshaping the Energy Industry*

The Smart Grid's entire infrastructure represents a large scale CPS, while the smart home represents a medium scale CPS.[66] Effectively, the Smart Grid and smart home will share many benefits and disadvantages as a CPS.[67] Generally, the development of the power grid into a modern CPS can make the important physical processes[68] of the grid cleaner, more efficient, and cost-effective.[69] Better CPS technology is also important in preventing many other problems, such as blackouts.[70]

The benefits of CPS and IoT technology are implicated in many areas. CPS technology allows for Distributed Energy Resource technologies, like wind or solar power, to be more effectively used in the Power Grid.[71]

---

59. *See, e.g.*, Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (May 13, 2014, 12:05 AM), forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/ [https://perma.cc/F3GC-5SEK]; Kim & Kumar, *supra* note 13, at 1289; NEWTON, *supra* note 52, at 664.

60. The use of IoT technology in consumer devices has become more practical due to the reduced cost of producing these types of sensors. Peppet, *supra* note 57, at 98 & n. 52.

61. *Id.* at 98.

62. *See* NEWTON, *supra* note 52, at 690.

63. *Id.*

64. Morgan, *supra* at 59.

65. *Id.*

66. Security Perspective, *supra* note 4.

67. *See id.*

68. These processes are: power generation, transmission, distribution, and consumption (or end use). *Id.*

69. Kim & Kumar, *supra* note 13, at 1302.

70. Rajkumar et al., *supra* note 51.

71. Kim & Kumar, *supra* note 13, at 1302.

Illustrating the point, consumers with solar panels can produce energy for their homes or sell that same energy back to their utility company.[72] In addition, alternative energy sources can be stored when produced but not needed, or they can alternatively be redirected to other points in the grid.[73] For example, if a home has solar panels and those panels produce more energy than the home needs, that energy can be redirected to a neighbor's home.[74] This is all made possible, in part, because of the communication and information technology present in CPS that "allow[s] the grid to engage in bidirectional flow of information and electricity" from utility to customer and vice versa.[75]

The benefits of CPS and IoT technology can also be obtained through real-time computing and networking in the smart home. Real-time computation benefits the power grid because it can make distribution of energy more responsive by communicating to the grid how much power is actually needed in a certain home.[76] Real-time computation also affects the end-use of energy by making energy consumption cheaper and more efficient for consumers. The advanced metering infrastructure (AMI) represents how this computation, communication, and control technology work together.[77] The AMI works through the installation of smart meters[78] on consumers' homes.[79] These smart meters communicate with each other, the utility company, and those smart appliances located in the consumer's home.[80] Since electricity consumers are charged more for energy consumption during peak load times, the AMI assists consumers in avoiding consumption during peak times and provides them with real-time

---

72. *Id.*

73. *Id.*

74. *Id.* ("Thanks to the infrastructure and mechanisms for bidirectional exchange of information and electricity, Smart Grid also allows traditional electric energy consumers to become providers. Electric energy that is stored or generated at residential and industrial facilities from renewable energy sources such as wind and solar can be sold to other consumers in the neighborhood or electric power providers.").

75. *Id.*

76. *Id.*

77. The AMI describes how the smart meters communicate and transmit meter data to the utility at "regular intervals." U.S. DEP'T OF ENERGY, 2014 SMART GRID SYSTEM REPORT (2014) [hereinafter SMART GRID REPORT]; Peppet, *supra* note 57, at 109 ("The home is increasingly monitored via sensors in a second way as well: the smart electricity grid.").

78. Bosch, *supra* note 5, at 1357 (A smart meter is a device that uses "digital technology to record customer consumption information on a frequent basis.").

79. Yang Liu et al., *Vulnerability Assessment and Defense Technology for Smart Home Cybersecurity Considering Pricing Cyberattacks*, IEEE/ACM Int'l Conf. on Computer-Aided Design (ICCAD) (2014), ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7001350 [https://perma.cc/T4KZ-BW6A].

80. *Id.*

pricing information from the utility company.[81] The smart meters use the pricing data provided to "schedule" energy consumption of smart appliances within the home, and also to record energy consumption.[82] The reduced consumption during peak load times reduces the consumer's electricity bill, the amount of electricity needed in the grid, and, ultimately, stress on the entire system.[83] The AMI is just one example of how beneficial end-use controls are in the Smart Grid infrastructure.

*D. The New Kids in Town: Edge Services and Edge Service Providers*

Smart Grid development has led to new businesses and services[84] that are changing the structure of the energy industry. These new services, termed "edge services,"[85] have opened the door for entities not traditionally involved in the power grid to provide new services to customers.[86] Edge services are services, or products, that are provided to end-use consumers, specifically those in the smart home.[87] The benefits of these services range from greater control over appliances, resulting in greater control over energy bills, to consumer participation in programs that promote competition in the energy market.[88] However, this comment primarily focuses on the development of smart appliances.[89] An edge

81. Kim & Kumar, *supra* note 13, at 1302.

82. Smart meters also perform the traditional function of recording energy consumption. *See* Liu et al., *supra* note 79.

83. This reduction in stress and the benefits it can produce are illustrated in the 2014 Smart Grid System Report produced by the Department of Energy (DOE). In the report, it was noted that the AMI infrastructure reduced peak demand of electricity to an extent that the Oklahoma Gas and Electric Company may potentially be able to avoid building a new power plant due to the addition of customer-based technologies, like a communicating thermostat. SMART GRID REPORT, *supra* note 77, at 6.

84. "New third-party market entrants [that] will strategically position themselves between the customer and the utility, resulting in what has been termed 'customer disintermediation'—an occurrence in which vendors offer attractive energy products and services to customers that will allow customers to bypass their local utility." Frisby & Trotta, *supra* note 3, at 301.

85. ELIAS LEAKE QUINN, SMART METERING & PRIVACY: EXISTING LAW AND COMPETING POLICIES, A REPORT FOR THE COLORADO PUBLIC UTILITIES COMMISSION 4 (2009).

86. *See id.*

87. *Id.* (defining edge services as those that are "provided to the electric consumer or that are focused on the last mile of electricity distribution").

88. Frisby & Trotta, *supra* note 3, at 303.

89. A type of edge service that can "tap into price signals sent from the electric utility and allow consumers to automate their appliance use depending on electricity costs." QUINN, *supra* note 85, at B–3.

service provider (ESP) can be an electric and gas utility company, a third party,[90] or even a traditional customer.[91]

The world has seen a proliferation of companies take advantage of the IoT consumer market to provide edge services. For example, General Electric and Whirlpool provide a variety of smart appliances, including washers, dryers, and refrigerators.[92] Many entities are working on ways to improve communication and connectivity among these devices.[93] Nest, which developed the popular Nest Smart Thermostat, provides a model of a smart appliance that has the desired effective communication capabilities. Recently acquired by Google in January 2014,[94] some view the acquisition of Nest as establishing credibility in the IoT market.[95] While IoT's goals are not primarily about energy efficiency, many scholars believe energy efficiency will begin to have a bigger influence on the market.[96] Thus, the energy field will likely see more ESPs in the market very soon. This development, although beneficial, presents some dangers to smart home and Smart Grid cyber security.

---

90. Edge Services "will ultimately be provided by electric and gas utilities, as well as third party service providers in competition with one [an]other." Frisby & Trotta, *supra* note 3, at 303. Third party here refers to those entities who were not previously involved in the power grid prior to the development of edge services.

91. "Many customers, possibly through aggregators or other energy service providers, will participate in the retail energy market, thus vastly increasing the number of participants." Bosch, *supra* note 5, at 1358.

92. Frisby & Trotta, *supra* note 3, at 303.

93. *See* Peppet, *supra* note 57, at 109. "SmartThings," for example, connects a variety of sensors found in the home, "such as an open/shut sensor (to monitor doors and windows); a vibration sensor (to monitor knocking on the front door); a temperature sensor (to control a thermostat); a motion sensor; and a power-outlet monitor (to turn outlets on and off remotely)." *Id.*

94. Lance Whitney, *Google Closes $3.2 Billion Purchase of Nest*, CNET (Feb. 12, 2014, 5:00 AM), cnet.com/news/google-closes-3-2-billion-purchase-of-nest/ [https://perma.cc/ZRH8-3GL5].

95. *See* Owen Poindexter, *The Internet of Things Will Thrive on Energy Efficiency*, GOVTECH.COM (July 28, 2014), govtech.com/fs/news/The-Internet-of-Things-Will-Thrive-On-Energy-Efficiency-.html [https://perma.cc/B4KK-B5U9]. Many feel that Google's acquisition of Nest will lead to more investments in the IoT market, as more startups will appear in hopes of following Nest's path to success. *See id.*

96. *Id.*

## II. THE QUINTESSENTIAL EDGE SERVICE: NEST SMART THERMOSTAT, CATASTROPHE, AND YOU

Nest, due to its popular smart thermostat,[97] adequately highlights the dangers that edge services and ESPs present to the smart home and the Smart Grid. Nest is "a smart device designed to control a central air conditioning unit based on heuristics and learned behavior."[98] Nest can be remotely controlled through another device, like a smartphone, and it communicates with other Nest smart devices.[99] Lack of interoperability between smart devices made by different manufacturers is a noted issue within the smart home.[100] However, Nest prides itself on having the ability to connect and communicate with a multitude of other IoT devices through its "Works with Nest" program.[101] According to Nest, this service allows a Nest device to interact securely with other devices located inside and outside of the home.[102]

---

97. The term Nest will be used to refer to Nest and its Smart Thermostat interchangeably. Nest makes other products as well, such as a fire alarm and a home security camera. *Nest Protect,* NEST, nest.com/smoke-co-alarm/meet-nest-protect/ [https://perma.cc/VAD8-7QDX] (last visited Feb. 21, 2017); *Nest Cam,* NEST, nest.com/camera/meet-nest-cam/ [https://perma.cc/BM3H-ET3H] (last visited Feb. 21, 2017).

98. Grant Hernandez et. al, *Smart Nest Thermostat: A Smart Spy in Your Home* 2, BLACK HAT (2014), blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf [https://perma.cc/H94C-GPQ4]. "Heuristics are criteria, methods, or principles for deciding which among several alternative courses of action promises to be the most effective in order to achieve some goal." JUDEA PEARL, HEURISTICS: INTELLIGENT SEARCH STRATEGIES FOR COMPUTER PROBLEM SOLVING 3 (1984). A solid description of Nest and its functions: Nest "tracks your behavior at home to set temperature more efficiently. The thermostat accepts and records direct user input (e.g., to increase or decrease temperature) but also contains sensors to sense motion in a room, ambient light, room temperature, and humidity. All such information is stored on Nest's cloud servers and can be accessed and controlled via a user's smartphone or other Internet-connected computer." Peppet, *supra* note 57*,* at 108–09.

99. *See* Hernandez et. al, *supra* note 98, at 2.

100. Roberto Baldwin, *Nest Gets More Smart Home Devices Talking to Each Other*, ENGADGET (Oct. 1, 2015), engadget.com/2015/10/01/works-with-nest-update/ [https://perma.cc/UZ9N-DAAQ]. Interoperability is an issue that plagues IoT devices in general. *Id.* In light of their technical similarities, this is likely the reason why interoperability has become such a key issue in Smart Grid policy. *See supra* Part I.A.2 & Part I.A.3.

101. *Works with Nest: How It Works*, NEST, nest.com/works-with-nest/ [https://perma.cc/C7MQ-LU4T] (last visited Feb. 21, 2017). "Works with Nest" allows other smart appliances such as Phillips Hue lights and Whirlpool washers and dryers to connect with the Nest smart home network. *Id.* Nest also has the ability to work with many IoT devices, including cars, fans, locks, and smart watches. *Id.*

102. *Id.*

Nest has also partnered up with utility companies and other ESP service providers. Nest's affiliation with Ohmconnect in its "Rush Hour" rewards program provides an illustration.[103] The partnership is designed to help utility companies cut down on demand during peak load hours.[104] This program incentivizes customers by paying them a certain sum each year for efficient energy use,[105] which incidentally results in a reduced energy bill for the customer. The Rush Hour Rewards program also benefits utility companies because it allows for reduced stress on the grid.

The Rush Hour program works when the customer gives Ohmconnect authorization to access his or her smart meter and smart devices, like the Nest Smart Thermostat.[106] Once connected, Ohmconnect will automatically cut back consumption when appropriate to reduce peak load.[107] To accomplish this task, Ohmconnect communicates with the grid through the smart meter to determine peak load times and uses the Nest Smart Thermostat to automatically adjust the temperature. Nest offers customers a right to retain ultimate control. The customer is alerted during each "rush hour" or spike in the energy load before Nest automatically begins the process of cutting back energy consumption, giving the customer the final say in whether to participate in the program or not.[108]

### *A. Inherent Vulnerabilities of IoT and CPS: Breeding Ground for a Kinetic Cyberattack*

Even though ESPs, like Nest, are largely unregulated, many argue that this is beneficial for both smart home and Smart Grid development.[109] However, this position is gravely inaccurate. The products that ESPs provide to consumers suffer from inherent security flaws, which can ultimately subject homes and the entire grid to a kinetic cyber attack. Much of a CPS's functions involve "two-way communication," meaning that

---

103. *Rush Hour Rewards*, NEST, nest.com/energy-partners/#rush-hour [https://perma.cc/9X2D-ZMEA] (last visited Feb. 21, 2017).

104. *Id.*

105. Klint Finely, *The Internet of Anything: The System that Pays You to Use Less Electricity*, WIRED (Feb. 15, 2015, 8:00 PM), wired.com/2015/02/ohmconnect/ [https://perma.cc/N2HC-2LP6].

106. *Id.*

107. *Id.*

108. *Learn More about Rush Hour Rewards*, NEST, nest.com/support/article/What-is-Rush-Hour-Rewards [https://perma.cc/P35C-F3QE] (last visited Feb. 21, 2017).

109. *See* Eisen, *supra* note 18, at 7 (noting that technologies, such as those involved in the smart home and Smart Grid, can change an entire industry overnight; thus, it would be advisable to "avoid constraining the grid's Steve Jobs" who could make innovations that would make the Smart Grid decades from now, entirely different from anything contemplated today).

data and network processes flow in two directions.[110] This two-way communication provides a hacker with more opportunities to manipulate those communications.[111] Consequently, two-way communication becomes a double-edged sword for Smart Grid development. "[O]n the one hand, [it] offer[s] savings, convenience, and efficiency, but on the other hand, it creates dangerous vulnerabilities."[112] Further, cyber security is not being studied enough, especially in smart home development.[113] Thus, important security concerns are overshadowed by the benefits of this technology for policy makers and ESPs.[114]

*1. Inherent Risks of CPS Technology*

CPS security vulnerabilities are studied in two areas: in systems and devices, and in communication.[115] The first area concerns how the devices that make up a CPS can be attacked through malware, bugs, and other types of malicious software.[116] The second area of study involves methods that impact communication with the Smart Grid.[117] Study in this area is grounded in the principle that a CPS, by nature, involves a "tightly interconnected system." Therefore, as the number of connections between devices increases, those connections create new communication based pathways, or vulnerabilities, that could undermine the entire system.[118]

Two-way communication presents a difficult issue for regulators to address because of its dual nature. Many scholars note that this technology fulfills the desire of many participants in the grid who want to remotely control equipment and devices.[119] However, the same technology that makes remote control of equipment possible "allow[s] attackers a gateway

110. For example, a smart meter facilitates two-way communication between the utility company and the customer to facilitate smart home scheduling. *See* Liu et al., *supra* note 79.

111. Bosch, *supra* note 5, at 1364. FERC has stated that "the Smart Grid could create opportunities for malicious access to Smart Grid devices, which could be used to disrupt grid functionality." Frisby & Trotta, *supra* note 3, at 311.

112. Bosch, *supra* note 5, at 1365.

113. Security Perspective, *supra* note 4 (suggesting that that security focus has generally been more on protecting privacy, opposed to the integrity of a smart device). *See, e.g.*, *id.* Persons in the field have stated that IoT consumer devices where not designed with security in mind. The author used a fitbit as an example to show that "the device was not engineered with data security in mind." Peppet, *supra* note 57, at 134.

114. Studies in this context reveal that many devices are implemented with "inadequate level[s] of security measures." *See* discussion *infra* Part II.A.2.

115. Security Perspective, *supra* note 4.

116. *Id.*

117. *Id.*

118. *Id.*

119. Bosch, *supra* note 5, at 1364–65.

into the system."[120] Smart Grid developments can lead to an attack because of the expensive and uncertain nature of securing the grid.[121] Further, some of the vulnerabilities will not be apparent until they are attacked. A strong cyber security defense must be strong everywhere to be successful; whereas an attacker only needs to find a single vulnerability to prevail.[122] Thus, security in this context is reactionary to hacks, whether they are staged by employed internal hackers, or are real attempts by malicious entities. Additionally, society's reliance on the grid only increases the likelihood of an attack.

Cyber attacks are not a thing of fiction. Institutions once perceived to be impenetrable have experienced hacks that took advantage of this two-way communication. These institutions include: banks, nuclear programs, stock exchanges, and even electrical utilities.[123] However, the threat of a kinetic cyber attack becomes more likely when the object of the attack is the power grid, and when the vulnerability of two-way communication is proliferated by increased efforts to make devices interoperable.[124] Two-way communication between the home and the grid is rapidly increasing, as evidenced by programs like Nest's Rush Hour rewards.[125] Therefore, continuing this trend will only give more incentive to attack the home in order to get to the grid.

*2. Inherent Risks of IoT Technology*

Even though the number of IoT consumer devices in the home have proliferated over the years, Professor Peppet noted in a recent article that these devices could be inherently prone to security flaws.[126] Isolated research has been done on the vulnerability of IoT devices. For example, a worm was discovered by a security firm that "targeted small IoT devices, particularly home routers, smart televisions, and Internet-connected security cameras—in addition to traditional computers;"[127] all items currently found in the modern home. Professor Peppet listed several reasons why IoT devices may be inherently vulnerable to security risks: (1) they are not designed with security in mind; (2) their small size limits how much processing power they can have and also restricts implementing

120. *Id.*
121. *Id.* at 1364.
122. A "defense needs to be strong everywhere, while the offense only needs to succeed in one place." *Id.*
123. For a detailed discussion of the recent cyberattacks on different industries across the world, including electrical utilities, see *id.* at 1363–68.
124. *See* discussion *supra* Part I.A.2 and Part II.
125. *See supra* Part II.
126. Peppet, *supra* note 57, at 133.
127. *Id.*

a large enough battery to support more processing power;[128] (3) many do not have the capability to receive security patch updates once they are sold; (4) communication between devices can lead to a hack of both devices if either are compromised;[129] and (5) these devices are often manufactured by producers that are inexperienced with important security issues.[130]

Admittedly, not all of the risks that Professor Peppet raised may be of concern for devices in the smart home.[131] However, it is important to consider that these risks are present in general IoT consumer devices. The smart home is still developing; thus, there is no way to tell what sort of IoT consumer devices will be in the home in the future, so understanding the inherent risks of all IoT consumer devices is necessary.

### *B. Practical Implications of Security Flaws*

A study conducted on the Nest Smart Thermostat revealed what researchers termed "an attack vector" of the Nest's hardware.[132] The researchers attacked the "boot up," or power on, process of the Thermostat by attacking some crucial flaws in one of the Thermostat's processors.[133] Eventually, the researchers were able to turn the Nest Smart Thermostat into a spy with the capability of determining the inhabitant's routines, their cyber activities, and further, providing a backdoor into their local network.[134] Therefore, a hacker could potentially peer into a customer's home through the "Nest window" and watch the inhabitants' every move for months at a time, completely unnoticed.

---

128. Increased processing power would allow the devices to support more security functions. *Id.*

129. Or, in the very least, it can affect how a consumer uses other devices related to the infected one. *Id.* at 134. Using an insulin pump as the example here, the author noted that the pump and the small monitor that the pump communicates with wirelessly could be hacked. "Radcliffe has shown that these monitors are also easily accessed, leading to the possibility that a malicious hacker could cause a monitor to display inaccurate information, causing a diabetic patient to mis-administer insulin doses." *Id.*

130. *Id.* at 135; Peppet, *supra* note 57, at 134 n.305.

131. Arguably, most IoT devices in the home will at the least be larger than those considered by Peppet (think a smart fridge versus what Peppet may have been considering (*i.e.*, a smart watch)). These devices will also likely be connected to a power outlet, taking care of the problem of energy source for greater security functions. On the other hand, the increased need of energy for these appliances could make the device less energy efficient.

132. Hernandez, *supra* note 98, at 5. Here, an "attack vector," means a vulnerability in the device's cyber security.

133. The researchers used a technique known as "peripheral booting" to attack gaps the Nest Thermostat's AM3703 processor. *See id.*

134. *Id.*

Consequently, a hack of this nature would not only affect the Nest device, but also other devices on the same network[135] because networked smart devices can be attacked as well.[136] This means that hackers can get into one smart device and affect an entire CPS.[137] The implications of such a hack on a device—like the Nest Smart Thermostat—that connects and communicates with many other IoT consumer devices in the home is alarming. Many IoT consumer devices do not reach the level of interoperability with other devices that Nest does, but Nest shows the danger of that increased interoperability. Yet, Nest is simply doing what the market is driving it to do. Federal regulators believe the grid will truly become beneficial when there is increased interoperability.[138] However, the danger of such a policy becomes apparent if just one device is hacked.

*1. Stage One: Attacking the Smart Home*

If a Nest Smart Thermostat is used to its upmost potential of interoperability in a home with a smart meter and full of other non-Nest IoT devices, the Nest Smart Thermostat becomes the central piece that connects them all. Thus, the security vulnerabilities of the Nest Thermostat become that of the other smart devices, regardless of what security measures the other devices possess. Interestingly, the security vulnerability is not solely dependent on a flawed product design. Many times, the vulnerability results from the consumer who has given authorization to another device or other edge service.[139] At this point, it may not matter that the device connected to the Nest Thermostat is more secure than the thermostat itself. The consumer has essentially bypassed that security measure by providing consent to use the two devices in tandem. Thus, a hack of a Nest Smart Thermostat can easily put the entire smart home CPS at risk. It is this combination of a device's security vulnerability coupled with consumer consent to connect devices that poses more risk to smart home cyber security.

---

135. The researchers noted that "[t]he Nest Thermostat backdoor is exacerbated by the fact that local network credentials are stored on the device and become accessible to our client software. The extraction of these credentials from the device imply that we could deploy other rogue devices into the local network, further shaping local traffic and scanning for *exploitable vulnerabilities other devices in the network may have*." *Id.*

136. Security Perspective, *supra* note 4.

137. *Id.*

138. *See* SMART GRID REPORT, *supra* note 77.

139. For example, such authorization that is required for a consumer to participate in the "Rush Hour Rewards" program.

A recent bug found in a software update sent out in December 2015, shows how a malfunctioning Nest can affect a home's inhabitants.[140] The bug drained the Nest's battery, causing homeowners nationwide to wake up in very chilly homes.[141] The timing of the glitch could not have been worse, as the temperature was dropping throughout much of the country.[142] As many affected consumers noted, cold temperatures present a health hazard for buildings with infants and the elderly.[143] Since the Nest's battery was dead, the only way to fix the issue required a manual nine-step process, which likely required calling a technician to come out to each individual home.[144] There was no indication that the bug was the result of some cyber attack; however, it does illustrate how even a simple malfunction can cause real world problems.

*2. Stage Two: Attacking the Smart Grid*

The implications of a Nest-like device being hacked become more frightening when one considers what could happen when Nest connects with a smart meter. The smart meter is also subject to vulnerabilities of its own in the form of two recognized cyber attacks: (1) pricing cyber attacks and (2) energy theft.

*a. Pricing Cyberattack*

Smart meters use scheduling to help other smart devices and appliances make decisions about when to use electricity, this is based in part on when it would be cheapest for the appliance to consume electricity.[145] For scheduling to work, the smart meter receives guideline-pricing data and uses that data accordingly to "schedule" energy consumption in the home.[146] A hacker, such as a neighbor, can manipulate the guideline pricing data in order to reduce his or her own electricity bill, and raise the cost of his neighbors' bill.[147] However, this type of attack could potentially be more malicious if the goal of the hacker goes beyond simply reducing his or her own energy bill. If the attacker substantially manipulates the guideline pricing data of multiple homes, he or she can

140. Nick Bilton, *Nest Thermostat Glitch Leaves Users in the Cold,* N.Y. TIMES, Jan. 13, 2016, nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html?_r=0 [https://perma.cc/TQB5-TXZ7].
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.*
145. *See supra* note 55 and accompanying text.
146. Security Perspective, *supra* note 4.
147. *Id.*

create a peak energy load.[148] If this "created" peak load is extreme enough, it could potentially overload the system, leading to a blackout.[149]

*b. Energy Theft*

Another type of attack that can affect the grid and the home through manipulation of the smart meter is known as energy theft. Energy theft occurs when an attacker "manipulate[s] measurements of energy consumption" in a way that shows a lower use of energy than actually has been consumed.[150] An attack of this sort would result in a reduced bill for the attacker, but it would cause the grid to shut down the energy supply, if the energy theft is large enough. In this instance, the energy load on the grid would be much higher than what is being communicated via the AMI.[151] Although both a pricing cyber attack and an energy theft can have the same effects on the power grid, each is initiated differently. Pricing cyber attacks affect pricing-data communicated over the grid, and an energy theft attacks the measurement data of energy consumption. The smart meter illustrates how the goal of increasing interoperability in both smart home and Smart Grid devices greatly foregoes the inherent cyber security threat that increased two-way communication presents.

In light of the risks and flaws in both devices, a scenario where the compromise of an entire home, including the essential smart meter of that home, because of an attack on the Nest Smart Thermostat, and thus leading to an entire AMI crashing, is now more realistic. In this scenario, the Nest communicates with the smart meter, but the smart meter also communicates with other smart meters and the utility company. There is a shift at this stage of the Nest cyber attack from a damaging compromise of an individual's home to a potential national security threat, all through the vulnerability of one device. However, this scenario could occur without a cyber attack. Potentially, the damage could be done if any of the devices or networks in the Rush Hour program were to malfunction. For example, an attack of this nature could occur if a smart meter sends Ohmconnect and Nest the wrong pricing data, which would result in a collection of Nests in a community to turn on every device in each home during a peak load hour. Questions arise as to the effects that such malfunctions in one CPS can have on another CPS absent a cyber attack.

Even if Nest fixes this vulnerability, which is likely, it gives a practical illustration of how things can go from bad, to worse, to catastrophic, when

148. *Id.*
149. Rajkumar, *supra* note 51.
150. Security Perspective, *supra* note 4.
151. *Id.*

a single device that specializes in two-way communication is hacked due to a security flaw. This hypothetical Nest hack highlights the potential danger of the two-way communication that makes CPSs and IoT devices so popular. Without oversight, and if left up to market pressures, ESPs, especially startups, likely will not invest in costly security measures. Even if ESPs invest in proper security measures, the threat of those measures being bypassed by the mere act of a consumer that connects a less secure device always poses a risk.

## III. FALLING THROUGH THE CRACKS: GAPS IN THE CURRENT LAW

Considering the expected growth of the edge service market and the dangers that edge services present, the state of the current regulatory landscape is troubling. Smart Grid regulation has proven to be problematic due to its complex and novel legal issues.[152] Because of the technological similarities,[153] the regulatory issues surrounding the smart home expose a portion of the problems surrounding Smart Grid regulation as a whole. Current regulation suffers from two important deficiencies: (1) lack of clear jurisdiction over ESPs and (2) voluntary adoption of federal standards. Regulation that affects the home is primarily focused with ensuring fair pricing for consumers.[154] However, edge services and ESPs are significantly restructuring the home's role within the grid,[155] and these new services greatly impact Smart Grid security.[156] Further, current efforts for developing federal cyber security standards have only resulted in voluntary adoption.[157] Presently, the issue of cyber security has been left to the states, opening the potential to a patchwork of standards.[158]

---

152. "Smart Grid development presents a variety of novel and practical legal issues that involve a multitude of regulatory jurisdictions, federal departments and agencies, and state authorities." Frisby & Trotta, *supra* note 3, at 304–05.

153. *See supra* Part I.B.

154. *See* THE REGULATORY ASSISTANCE PROJECT, ENERGY REGULATION IN THE US: A GUIDE 5–6 (2011) (describing how utilities and the government have entered into a "regulatory compact" in order to ensure the "provision of safe, adequate, and reliable service at *prices* (or revenues) that are sufficient, but no more than sufficient to compensate the regulated firm for the costs…that it incurs to fulfill its obligation to serve."); *see also id.* at 25 (stating that the "first and best established functions of the state commission are to . . . establish the prices or rates for each class of consumers.").

155. *See supra* Part I.D.

156. *See supra* Part II.

157. *See* Bosch, *supra* note 5, at 1377.

158. "Without national standards, 51 different state public utility commissions ("PUCs") could adopt 51 different Smart Grid models, or *implement systems that fail to protect the grid from cyberattacks*." Eisen, *supra* note 18, at 4.

*A. Lack of Clear Jurisdiction over ESPs*

The current regulatory environment does not provide any entity with jurisdiction over ESPs, like Nest, or its activities as it relates to the energy field. FERC likely does not have authority over edge services and ESPs, since these services do not involve interstate wholesale of electricity or interstate transmission of electricity. Arguably, edge services could fall under FERC's authority to create reliability standards because the vulnerability of an edge service can affect the bulk power system. However, FERC's jurisdictional authority to enforce such standards is limited to the bulk power system;[159] unfortunately, the scope of the bulk power system is not clear.[160] Even if ESPs did fall within the scope of the reliability standards development, NERC's interpretation that reliability standards do not include telecommunication systems or communication paths[161] would make jurisdiction ineffective. FERC could also have authority over ESPs under EISA, but FERC has interpreted EISA in a way that does not give it the power to "mandate or enforce these standards."[162] Further, the extent that EISA extends FERC's jurisdiction is still a matter of debate, and the process for developing interoperability standards has only been invoked once since EISA has been enacted.[163]

However, the U.S. Supreme Court's recent decision in *FERC v. Electric Power Supply Ass'n,*[164] may greatly change this calculus. The Court dealt with FERC's Order No. 745, which attempted to ensure that demand response programs[165] (programs similar to that of Ohmconnect) are compensated at the same rate as traditional electricity generators.[166] Opponents of FERC's order argued that "FERC has no jurisdiction under

159. *See* 16 U.S.C. § 824o(e).

160. Andreas S. V. Wokutch, *The Role of Non-Utility Service Providers in Smart Grid Development: Should They Be Regulated, and if So, Who Can Regulate Them?,* 9 J. ON TELECOMM. & HIGH TECH. L. 531, 549 (2011) ("It is unclear what is considered a local distribution facility and what is considered part of the bulk power system.").

161. Bosch, *supra* note 5, at 1379.

162. Wokutch, *supra* note 160, at 551.

163. Bosch, *supra* note 5, at 1382.

164. 136 S. Ct. 760, 193 L. Ed. 2d 661 (2016), *as revised* (Jan. 28, 2016).

165. A demand response program is one in which "operators of wholesale markets pay electricity consumers for commitments *not* to use power at certain times." *Id.* at 767 (emphasis original).

166. Stephen J. Humes, *Supreme Court Walks Energy Policy Tightrope As It Addresses Federalism and States' Rights,* 4 ABA TRENDS 7, March/April 2016; Gavin Bade, *Updated: Supreme Court upholds FERC Order 745, affirming federal role in demand response,* UTILITY DIVE, Jan. 25, 2016, utilitydive.com/news/updated-supreme-court-upholds-ferc-order-745-affirming-federal-role-in-de/412668/ [https://perma.cc/96Q5-Z4WE].

the FPA over the electric consumption of end-use customers at their homes or places of business."[167] The rationale behind the argument was that the FPA gives FERC jurisdiction over wholesale electricity, but not over demand response programs.[168] Opponents believed that demand response programs are an issue of retail sales, which is within the jurisdiction of the states.[169] The Court disagreed, holding that "[w]hen FERC regulates what takes place on the wholesale market, as part of carrying out its charge to improve how that market runs, then *no matter the effect* on retail sales, [the FPA] imposes no bar."[170] The Court reasoned that "the wholesale and retail markets in electricity . . . are not hermetically sealed from each other . . . " and transactions that occur on either market can affect the other.[171]

As a result of the U.S. Supreme Court's decision, there is now precedent establishing FERC's ability to extend its jurisdiction into areas traditionally regulated by the state. However, it is too early to tell how far this holding can be extended. There are already some limitations present in this holding, namely, FERC's actions only *indirectly* affected the state's jurisdiction.[172] Further, this decision, for purposes of this comment, only dealt with pricing, *not cyber security measures*. Thus, although *Electric Power Supply Ass'n.,* presents a step in the right direction in extending FERC's jurisdiction, its limitations prohibit it from establishing clear and direct jurisdiction over all ESPs and edge services.

PUCs, similarly, do not have clear jurisdiction over ESPs.[173] PUCs only have the authority to regulate interactions between utilities and consumers, which do not contemplate third party interactions involving ESPs.[174] A PUC's authority revolves intimately around the regulation of "public utilities," and ESPs are likely not considered public utilities.[175] There is evidence to counter a PUC's lack of jurisdiction since some states, such as California, have enacted legislation that affects ESPs. Once the third party ESP receives data from a utility company, California law shifts liability to ESPs.[176] Even if states have authority to regulate, it would only

167. Humes, *supra* note 166, at 8; *FERC,* 136 S. Ct. at 767 (stating that one of the issues facing the Court was "does the FPA permit FERC to regulate these demand response transactions at all, or does any such rule impinge on the State's authority").
168. Humes, *supra* note 166, at 8.
169. *Id.*
170. *FERC,* 136 S. Ct. at 776.
171. *Id.*
172. Bade, *supra* note 166; Humes, *supra* note 166, at 8.
173. *See* Wokutch, *supra* note 160, at 552–55.
174. *See id.*
175. *See id.* at 553–54.
176. Frisby & Trotta, *supra* note 3, at 326 (citing California S.B. 1476 (2010) (Chapter 497, Statutes of 2010)).

mean that edge services would fall into the same patchwork of voluntary federal standards that utility cyber security standards fall under.

Likewise, DOE's limited authority in this area makes it unlikely that it has authority to regulate ESPs. DOE has the power to create entities that would help lead to Smart Grid development, not to regulate such development.[177] The FCC potentially has the authority to regulate ESPs, but is unlikely to do so.[178] FCC was granted some authority in the Smart Grid realm under the American Reinvestment and Recovery Act; however, it has interpreted its role as one of "guidance and assistance rather than active involvement."[179] Power grid regulation already involves an awkward relationship between PUCs and FERC, and adding another entity, such as the FCC or DOE, will only further complicate things.

*B. Lack of Nationwide Cybersecurity Standards*

Even if Congress were to establish jurisdiction over ESPs, the lack of mandatory federal cyber security standards would still present a problem. FERC's authority to enforce cyber security measures does not apply to all entities, nor does it apply at every stage of the power grid.[180] NERC's interpretation of its mandate to create reliability standards[181] is also troubling in light of the issues that two-way communication presents to the Smart Grid. The lack of mandatory standards makes the risk of a kinetic cyber attack more probable and only highlights the need for greater cyber security measures in the grid.

EISA potentially extends FERC's jurisdiction to enforce cyber security measures based on FERC's interpretation of its authority under the act. FERC has interpreted that the standards it adopts will be applicable to devices and markets at the local and intrastate level.[182] FERC's interpretation would extend its jurisdiction to an area of the power grid that has generally been the realm of PUCs.[183] Consequently, opponents of FERC's interpretation noted that any attempt to actually exercise this new

177. Wokutch, *supra* note 160, at 555–57.
178. *Id.* at 558.
179. *Id.* at 557.
180. *See supra* Part I.A.2. For example, local distribution systems are expressly left out of FERC's jurisdictional authority. 16 U.S.C. § 824o(a)(1)(B).
181. *See supra* Part III.A.
182. *See* Smart Grid Policy, 74 Fed. Reg. 37098, 37101, para. 22 (Jul. 27, 2009) (to be codified at 18 C.F.R. ch. I); Bosch, *supra* note 5, at 1381–82.
183. Bosch, *supra* note 5, at 1381–82.

power would be met with hostility.[184] As a result, the law is at a stalemate, and FERC has yet to mandate any interoperability standards.[185]

The failure of the interoperability adoption process under EISA presents another roadblock to the adoption of mandatory federal standards. NIST has failed to produce any standards that meet the "sufficient consensus" requirement of FERC.[186] In fact, since EISA's enactment, NIST attempted this process only once and failed.[187] Nevertheless, NIST has continued to work with SGIP to develop voluntary standards and put together reports relating to cyber security of communication interfaces in the Smart Grid.[188] However, the process of interoperability adoption has proven to be ineffective. Thus, even if accepted by FERC, the enforceability of these standards is likely to be questioned.[189]

A study by Congressmen Edward Markey and Henry Waxman shows how ineffective a voluntary regime is in this area.[190] The report done on NERC's voluntary and mandatory standards revealed that the majority of utilities only implemented the mandatory standards.[191] A voluntary adoption regime can be successful in some instances, but Smart Grid cyber security is an issue of national security and should not be left up to such a regime.[192] Also, with the development of cyber security standards lying in the hands of the states, there is the possibility of fifty-one[193] different

184. "If FERC attempted to change the existing distribution of authority between it and the states (for example, by setting national interoperability standards that the states would be required to force utilities to adopt in individual projects), it could exacerbate the well-documented tension between the federal and state governments in electric utility regulation." Eisen, *supra* note 18, at 21.

185. FERC did note that "adoption of any Smart Grid standard under EISA does not make the standard mandatory, nor does EISA give FERC authority to require the development of any Smart Grid standard. Any Commission authority to make Smart Grid standards mandatory, or to allow rate recovery of Smart Grid cost must derive from its existing authority under the FPA [which has been replaced by the EPAct]." Frisby & Trotta, *supra* note 3, at 310. "The commission added that adoption of national standards for Smart Grid technologies and standards should enhance policy choices available to states, and should not interfere with states' abilities to adopt certain advanced metering or demand response programs." *Id.*

186. Bosch, *supra* note 5, at 1382.

187. *Id.*

188. *Id.* Fifty-six voluntary standards have been approved by SGIP and are included in their catalog of standards. *Id.*

189. Wokutch, *supra* note 160, at 551.

190. *See* STAFF OF CONGRESSMEN EDWARD J. MARKEY & HENRY A. WAXMAN, ELECTRIC GRID VULNERABILITY: INDUSTRY RESPONSES REVEAL SECURITY GAPS 12 (2013), markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf [https://perma.cc/S37V-Z985].

191. *Id.*

192. *See* Bosch, *supra* note 5, at 1377.

193. A federal model and fifty state models.

models for cyber security, which could collectively fail to protect the grid.[194] Further, developing cyber security standards without establishing jurisdiction over ESPs will weaken the entire framework due to the inherent risks of edge services.[195] Both the voluntary adoption regime and lack of jurisdiction over ESPs must be addressed in order for the Smart Grid to be successful. Instead, the current regime focuses on policy aimed at furthering the adoption and development of new Smart Grid technology.[196] Continuing to ignore the voluntary nature and lack of jurisdiction of the current regime creates a breeding ground for a kinetic cyber attack.

The development of the smart home relies on the continued development of IoT devices. Despite the inherent risks of IoT devices, the fact that the home is the area where ESPs are the most active is what truly makes smart home development dangerous. If these concerns are not properly addressed, the growth of the smart home will be stunted, and in turn, so will the growth of the Smart Grid. If customers do not trust the technology that is necessary for the continued growth of the smart home and Smart Grid, both will inevitably fail. While some industry leaders claim to be cognizant of the need to address these security concerns, [197] important cyber security considerations are still overlooked.[198] This oversight can be traced to a number of factors[199] and has important consequences. If a Nest-like device compromises other devices it communicates with and leads to physical harm, there is no clear way to determine the extent of the ESPs' liability.[200] Accordingly, the thought of leaving ESPs free to follow market pressures in developing cyber security

194. Eisen, *supra* note 18, at 4.

195. *See* discussion *supra* Part II.

196. *See generally* Energy Independence and Security Act, 42 U.S.C. §§ 17001–17386 (2007).

197. Nest Founder, Tony Fadell, stated that "[the Nest Thermostat] will never take off if people don't trust it." Hernandez et al., *supra* note 98, at 1.

198. Security Perspective, *supra* note 4, at 1.

199. For one, many developers of IoT consumer devices are startups with limited capital and are unable to afford proper security measures. *See* Hernandez et al., *supra* note 98. A second factor relates to IoT device design flow. According to researchers, security measures likely do not extend beyond the application and network level, meaning that "designers often treat IoT and wearable devices as standard networked devices and try to apply the security protections developed for regular, everyday use computing devices." *Id.* at 1. This vulnerability in design flow can be used to upload malicious firmware into the software of an IoT device. *Id.*

200. With regard to liability, the service agreements of many companies like Nest limits a customer's remedy to arbitration. *See Terms of Service*, NEST, nest.com /legal/terms-of-service/ [https://perma.cc/8SEH-4VHF] (last visited Feb. 23, 2017). The customer must give up the right to seek a remedy in court or to join a class action. *Id.* Many have categorized the terms of such agreements as very unfriendly to consumers. *See* Bilton, *supra* note 140.

measures should be extremely alarming, but the current regulatory regime has not established clear jurisdiction over ESPs. Further, even if they did, ESPs would enter a regime where cyber security measures are not mandatory.

## IV. CRAFTING A SOLUTION

The issues surrounding the smart home by no means include all of the problems with current Smart Grid development. Given the inadequate cyber security standards and the multiple actors involved in regulation, the entire structure of the power grid regulatory regime needs to be addressed. However, restructuring the current regime will take a significant amount of time and effort. Further, at this early stage of development, mandatory and stringent regulation may not be possible or desirable. The smart home, and the Smart Grid are still developing, and making premature laws regarding cyber security would not be wise. With that said, as a matter of policy, the security of the smart home and oversight of ESPs and their services must be considered a priority in ongoing development. This new smart home policy should be geared toward several goals that will be discussed in part.

### *A. Defining the Smart Grid and Establishing FCC Authority*

First, the lack of definitions surrounding of the Smart Grid realm hurts regulatory efforts.[201] Accordingly, the first goal in progressing smart home cyber security is crafting clear definitions of the categories of services, devices, actors, and the relationships between these and traditional[202] entities in the growing smart home infrastructure. Developing and implementing standards or regulations will be ineffective and almost impossible to draft without first completely understanding the object of the standards. Therefore, the first step should be accomplished by forming a coalition of relevant federal agencies and ESP industry leaders that would study the smart home industry, create reports based on these studies, and ultimately suggest uniform standards. Among these industry leaders, it is vital that companies like Google, Microsoft and Whirlpool take part. However, actively engaging the FCC in the process will be more important. The FCC has expertise in telecommunications and broadband Internet, and their expertise would play an important role in the development of the smart home.

---

201. *See supra* Part I.
202. Such as traditional utility companies.

Thus, Congress should give the FCC the primary responsibility of overseeing ESPs and edge services and crafting clear definitions, at least until the power grid regulatory regime is restructured. This step should not be difficult to implement, since this model is essentially already in place with regard to the development of the rest of the Smart Grid infrastructure.[203]

*B. Enforceable Cyber Security Standards for ESPs*

The second goal of developing a smart home policy should be the crafting of enforceable federal standards for ESPs. Many of the roadblocks to mandatory standards for utility companies are not present in the realm of edge services. The edge service market is a new, developing market with no clear regulatory authority in place, so there is no jurisdictional battle impeding these standards or their enforcement. However, wholesale regulation may not be appropriate because it may do more to damage the development of the smart home than to protect it. It is important to keep in mind the policy of promoting development of the Smart Grid and the newly proposed policy of securing the smart home. These policies should complement, not detract from, one another. Oversight of ESPs should emphasize to smart appliance developers and legislators that the industry's success requires more than greater interoperability. People have to trust this technology in order for the industry and the Smart Grid to grow. Therefore, it is essential that the technology should not make people feel less secure in their homes.

Oversight in this realm may take the form of a system that is analogous to the Underwriters Laboratories' standards.[204] This model would involve the creation of mandatory security standards for appliances that have the potential to communicate with the grid directly or through second-hand communication.[205] An example of a mandatory security standard would be

203. The purpose of this step is just to put added emphasis on the smart home in light of the issues discussed.

204. Underwriters Lab is a private organization that is well established in multiple countries that comes up with standards for appliances that plug in to the grid that promote protection of grid and the appliance (*i.e.*, surge protectors). Underwriters Lab is one of the few companies that is approved by the U.S. Occupational Safety and Health Administration to perform safety testing. *See, e.g.*, *Standards,* UNDERWRITERS LABORATORIES, ulstandards.ul.com/ (last visited Feb. 23, 2017); *Underwriters Laboratories, Inc.*, inc.com/encyclopedia/underwriters-laboratories-ul.html (last visited Feb. 23, 2017).

205. Direct communication would involve direct communication with a device like a smart meter. Second-hand communication would involve a device that has intermediary between it and the smart meter, for example a device that communicates with the Nest Smart Thermostat, and the Nest Smart Thermostat communicates with the smart meter.

that a device must have the ability to receive software patch updates in a way similar that a smartphone receives updates. Understandably, these mandatory security standards will increase the costs for ESPs to enter and stay in the market. Therefore, costs and effects in the market will need to be considered in crafting these standards, but the greater interest is to protect the nation and individual consumers; thus, it should not give way to market pressures.

### *C. Liability Framework*

In light of the possibility of market effects by mandatory security standards and the likelihood that the threat of hacks will always be present,[206] the third goal should be the creation of a liability scheme in the event that a kinetic attack occurs. The liability scheme would have multiple stages of punishment for ESPs who do not comply with the mandatory standards and whose devices lead to the kinetic attack.

The liability scheme would be broken down into three levels based on compliance with the mandatory standards. The first level would afford ESPs the most protection from liability. This stage would be applicable to those ESPs who fully comply with the mandatory standards imposed on them. Since it will be a government-led coalition that creates these standards, if the security of devices fail, then the government should bear the majority of the burden. However, the burden of liability will not solely be on the government, since an ESP can always adopt higher standards as it is able and feels necessary.

The second level would apply to those ESPs who do not fully adopt the mandatory standards. This level would deal with the reality that not every ESP would be able to afford the security measures that are made mandatory. The second level would also serve to increase competition and development in this field. Thus, as long as the ESP engages in certain activities that meet a minimum threshold of appropriate cyber security,[207] the ESP can still participate in the development of smart home products. Further, the ESP's liability, in the event of an attack, would be mitigated based on the ESP's security practices. However, to encourage adoption of the mandatory standards, ESPs would suffer some sort of financial penalty.[208]

---

206. A "defense need to be strong everywhere, while the offense only needs to succeed in one place." Bosch, *supra* note 5, at 1364.

207. For example, having a team of internal hackers constantly checking for flaws in security, which could potentially be cheaper than meeting government mandatory standards.

208. Financial penalties could take the form of a tax every two to five years ESPs do not adopt the standards.

The third and final level applies to those ESPs who do not adopt the mandatory standards or adopt voluntary practices of the second level. In this level, the ESP cannot engage in the sale of IoT consumer devices, and in the event that they somehow get a device into the home and that device is used to conduct a kinetic cyber attack, the ESP will have no shield of liability.

## CONCLUSION

The emergence of the smart home is an important development in human history, but it is not without its dangers. The new industry is developing around the smart home, edge services, and the technology being used to make the smart home a reality, IoT and CPS, present both benefits and inherent risks to individuals in the home and the nation. The threat of a kinetic cyber attack on the grid via the smart home is technologically possible and probable. Thus, as a policy matter, smart home cyber security needs to become a priority and security standards need to be developed. Equally important is keeping in mind the practical limitations of such standards. Hacks and malfunctions in these devices are inevitable, and imposing these standards on ESPs may not always be economically feasible. Therefore, a liability framework should also be adopted to incentivize acceptance of standards but to also shield ESPs in the event of a kinetic cyber attack. No solution to such a complex problem is perfect, but this solution achieves the appropriate balance to begin solving the problems surrounding the Smart Grid. The smart home cannot be left alone any longer.

*Chanse J. Barnes*[*]

---

* J.D./D.C.L., 2017 Paul M. Hebert Law Center, Louisiana State University.
I would like to thank God for blessing me with the ability and opportunity to write for the Journal. I would also like to thank my parents, Roy and Cheree Barnes and all of my family and friends for their continued support throughout my life. Additional thanks to my advisors, Professor Richards and Professor Lockridge, and my fellow members of the Journal. Finally, this article is dedicated to the memory of Matthew Cameron who helped inspire the topic of this article.