AUTOMATIC CONSUMER PRIVACY RIGHTS EMBEDDED IN SMART GRID TECHNOLOGY STANDARDS BY THE FEDERAL GOVERNMENT

INTRODUCTION

Our nation is suffering from a variety of energy challenges—whether it is dependence on foreign oil or aging domestic infrastructure—that will shape our future economy. Nationwide investment in "Smart Grid" technology can help resolve some of these energy challenges. Smart Grid technology would modernize the energy sector by allowing increased communication through the energy system, including sending consumer energy-use information to the utilities. Utilities can use consumer information to more effectively control demand and provide consumers with efficient energy-use tips. While Smart Grid technology presents many benefits, it also presents risks in terms of consumer privacy.

For an efficient Smart Grid, utilities and third parties will need access to greater levels of consumer information, thus presenting a new problem in the privacy world. Unlike telephone services and the internet, where consumers can choose to opt out of using such technologies in order to protect their privacy, Smart Grid technologies may be mandatory to consumers. Thus, it would force those on the grid to disclose personal information in a way that the electric industry has never required. In response to growing privacy concerns, in May 2010 the Department of Energy (DOE) requested comments from utilities, consumer groups, and other interested parties on the issue of energy consumer privacy on the Smart Grid.[1] Subsequently, the DOE issued two reports addressing privacy concerns in the Smart Grid.[2] The central focus of this Note will encourage utilities and the government to focus on consumer privacy at the outset when implementing Smart Grid technologies. I propose that a federal agency, likely the Federal Energy Regulatory Commission (FERC or Commission) or the DOE, regulate consumer information that utilities collect to ensure that consumer privacy is the default option. With privacy as the main concern, the utilities will foster consumer confidence in the

---

1. Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy, 75 Fed. Reg. 26,203, 26,206 (May 11, 2010) (inviting comment on eighteen broad questions concerning consumer privacy and implementing the Smart Grid, including potential practices to protect energy information privacy).

2. DEP'T OF ENERGY, DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES (2010) [hereinafter DATA ACCESS], *available at* http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf; DEP'T OF ENERGY, COMMUNICATIONS REQUIREMENTS OF SMART GRID TECHNOLOGIES (2010), *available at* htttp://energy.gov/sites/prod/files/gcprod/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf.

system and prevent problems from arising in the future when Smart Grid technologies are inevitably deployed nationwide.

Part I of this Note will focus on Smart Grid technology. With aging infrastructure in the energy industry, the current system can be improved to respond to increased energy consumption and environmental concerns. Technology can make the energy system more efficient by allowing utilities and system operators on the grid to communicate with one another and respond to consumer demand more effectively. In addition, new technologies can help consumers become more energy efficient by providing them with detailed information on their energy consumption. While Smart Grid technologies present many benefits to improve the energy sector, the potential collection of more detailed consumption data creates privacy concerns for energy consumers.

Next, Part II will analyze the constitutional right to privacy. While the foundational Supreme Court cases regarding privacy protect reproductive autonomy, the right has been extended to include an informational right to privacy. These cases demonstrate that an energy consumer can invoke a broad right to individual privacy against government actions that misuse Smart Grid information. Therefore, for this new technology to be successful, privacy should be a major concern in its implementation.

Finally, Part III will propose recommendations to the energy sector. For utilities to successfully implement Smart Grid technologies, they must consider consumer privacy in every action they take. Customers need to be informed of how utilities and third parties use their information. The Commission should establish basic privacy standards for utilities to ensure uniformity throughout the system. Any government action regarding the Smart Grid should make consumer privacy a default option, where consumers would have to opt-in to share certain information.

I. WHAT IS SMART GRID TECHNOLOGY?

Smart Grid technology is "the modernization of the existing electrical system that enhances customers' and utilities' ability to monitor, control, and predict energy use."[3] It refers to changes made to the electric power grid that allow it to better respond to supply and demand shifts.[4] Utilities need to be able to communicate with energy consumers to modernize the

3. Patrick McDaniel & Stephen McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE SECURITY& PRIVACY, May/June 2009, at 72, 72.

4. Himanshu Khurana et al., *Smart-Grid Security Issues*, IEEE SECURITY& PRIVACY, Jan./Feb. 2010 at 81, 81

energy sector. The Smart Grid involves "two-way communication" between the consumer and utility regarding the consumers' energy consumption.[5]

Implementing Smart Grid technology would have two major dimensions. First, every consumer would have a sophisticated meter attached to the home or building to record more information about energy use. Utilities would then collect information wirelessly from smart meters, which is a modernized computer version of the electric meters currently outside most homes.[6] Each meter "contains a processor, nonvolatile storage, and communication facilities" that allow it to collect energy-use data from inside the home, store it, and send it to the utilities through wireless internet or another connection.[7] Smart meters collect energy consumption data in short intervals, like every minute or every hour.[8] In contrast, utilities read most current meters on a monthly basis.

Second, implementing Smart Grid technology involves improved communication and automated technologies among energy generators and other devices on the transmission and distribution system. The Smart Grid is not limited to just smart meters.[9] Improved communications among these other components of the electric system, however, does not involve consumer data and privacy concerns and thus this Note does not further consider this aspect of the Smart Grid.

A. Benefits of Smart Grid Technology

Smart Grid technologies present benefits to revolutionize our nation's aging energy sector, including electricity reliability, energy efficiency, environmental conservation, and financial savings.[10] There are two main parties that benefit from these new technologies: utilities and consumers. First, the smart meter sends information to the utility to record individual energy demand.[11] This information allows utilities to offer new energy programs like real-time or dynamic pricing.[12]

---

5. *Id.*

6. McDaniel & McLaughlin, *supra* note 3, at 72.

7. *Id.*

8. Khurana et al., *supra* note 4, at 81.

9. *See* PETER FOX-PENNER, SMART POWER: CLIMATE CHANGE, THE SMART GRID, AND THE FUTURE OF ELECTRIC UTILITIES 34 (2010) (stating that definitions of the Smart Grid cannot be limited to only smart meters "since smart meters are only one small, albeit critical, part of the new world").

10. ELECTRIC POWER RESEARCH INST., REPORT TO NIST ON THE SMART GRID INTEROPERABILITY STANDARDS ROADMAP 6–7 (Post-Comment Period Version 2009), *available at* http://www.nist.gov/smartgrid/upload/Report_to_NIST_August10_2.pdf.

11. DEP'T OF ENERGY, PUBLIC ROUNDTABLE: DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES 37–38 (2010) [hereinafter DOE ROUNDTABLE], *available at* http://energy.gov/sites/prod/files/gcprod/documents/PublicMeetingTranscript_June29.pdf; *see also* SHERRY LICHTENBERG, SMART GRID DATA: MUST THERE BE CONFLICT BETWEEN ENERGY

Additionally, utilities will be able to communicate with the home "in a real time way" to allow customers to manage their energy load and keep them informed of their energy practices.[13] With instant energy-use information, utilities would, for example, be able to use more sophisticated rate designs and price signals to tell the customer to delay turning on the dishwasher until later when prices are lower. This has the potential to reduce overall costs for both the utility and consumer.[14] Smart Grid technology enables real-time communication with the home, allowing for communication with smart appliances like a dishwasher.[15] This technology can reduce carbon emissions by "making it easier to incorporate renewable energy sources" and informing consumers of high price times, which often corresponds with the most pollution.[16] Furthermore, utilities can price electricity according to the specific time and day when it is used based on information about consumer use.[17] Thus, Smart Grid technology presents many possibilities for utilities to use consumer information to improve the efficiency of the energy sector.

Second, the smart meter sends information to the consumer to inform the individual about his or her energy usage.[18] Then, consumers can adapt behaviors based on dynamic pricing models, where Smart Grid energy information "provide[s] the customer[s] with pricing information for current or future time periods."[19] While it is important for utilities to be connected and share supplies, Smart Grid technology has a more significant

---

MANAGEMENT AND CONSUMER PRIVACY?, at iii (2010), *available at* http://www.nrri.org/pubs/telecommunications/NRRI_smart_grid_privacy_dec10-17.pdf ("[B]y providing highly granular consumption data, the [S]mart [G]rid will benefit utilities, customers, and society by enabling more efficient 'real time' energy management . . . .").

12. *See* DOE ROUNDTABLE, *supra* note 11, at 46 (noting that if utilities receive increased energy consumer information, they will be able to better manage "demand response and load leveling," thus leading to more dynamic pricing models).

13. *Id.*

14. *Id.* at 46–47.

15. *See* ANN CAVOUKIAN ET AL., PRIVACY BY DESIGN, SMARTPRIVACY FOR THE SMART GRID: EMBEDDING PRIVACY INTO THE DESIGN OF ELECTRICITY CONSERVATION 8–9 (2009), *available at* http://www.privacybydesign.ca/content/uploads/2009/11/pbd-smartpriv-smartgrid.pdf (noting that smart appliances pose a great opportunity for the energy sector because they can be calibrated by the customer to communicate directly with the utility, which makes for "efficient and more productive use of electricity").

16. Khurana et al., *supra* note 4, at 81.

17. McDaniel & McLaughlin, *supra* note 3, at 72.

18. DOE ROUNDTABLE, *supra* note 11, at 22.

19. CAVOUKIAN ET AL., *supra* note 15, at 9; *see also* AHMAD FARUQUI & LISA WOOD, EDISON ELECTRIC INST., QUANTIFYING THE BENEFITS OF DYNAMIC PRICING IN THE MASS MARKET 1 (2008), *available at* http://www.eei.org/ourissues/electricitydistribution/Documents/quantifying_benefits_final.pdf (discussing the benefits of dynamic pricing, or "retail prices that reflect the varying cost of electricity in the wholesale market," on the grid, including consumer financial savings, increased consumer-demand response, and energy-sector savings in transmission and distribution costs).

impact on consumers.[20] New technology allows customers to have more control over energy use in their home, thus becoming more efficient energy consumers.[21] For example, people could theoretically turn off the hot-water heater while on vacation through a smartphone application that communicates with a smart meter. Smart meters can inform the utility if the customer is having problems with electricity.[22] Furthermore, smart meters can work with smart appliances and turn off a dishwasher during peak hours.[23] Studies show these technological tools do have an impact on consumer behavior and result in more energy efficient practices and staggering economic savings.[24]

B. Problems Presented by Smart Grid Technology

While Smart Grid technology creates benefits that would revolutionize the energy industry, it also presents significant drawbacks that may prevent its implementation on a nationwide scale if left unaddressed. With new electronics that communicate with the electric system, consumer information is increasingly recorded and reviewed.[25] Increasing amounts of information may be shared throughout the energy sector to make Smart Grid technologies effective.[26] Therefore, the energy sector must ensure consumer information is safe and used only for purposes known to the consumer.

Smart Grid technology presents a wide array of problems in two broad areas: cyber security and individual privacy. While cyber security is an important issue, this Note focuses solely on protecting individual privacy. Smart meters can track not only electricity use but also activities within a person's home. For example, detailed energy-use data can show when a person is at home or not.[27] Additionally, smart meters can track where

---

20. *See* FOX-PENNER, *supra* note 9, at 35 (noting that the impacts of Smart Grid technologies on end users "are potentially profound").

21. McDaniel & McLaughlin, *supra* note 3, at 72.

22. *Id.*

23. *Id.*; *see also* FOX-PENNER, *supra* note 9, at 36 (noting that new software can enable consumers to program their appliances "to react to prices").

24. *See* Steve Lohr, *Digital Tools Help Users Save Energy, Study Finds*, N.Y. TIMES, Jan. 10, 2008, at C1 (stating that since efficient consumer behavior lowers individual power bills and "reduce[s] the need to build new power plants," this could save up to $70 billion spent on power plants over twenty years).

25. *See* Khurana et al., *supra* note 4, at 82 ("The massive use of low-cost communication and electronics provides an explosion of information that bears different data formats and time stamps . . . .").

26. *See id.* (explaining that increased communication along the system "allows [for] finer-grained" control that is necessary to improve demand control).

27. *Id.* at 83; *see also* NAT'L INST. OF STANDARDS & TECH., GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 29 (2010) [hereinafter SMART GRID CYBER

electricity is specifically used inside the home, thus presenting the possibility of tracking when a person is watching television or cooking food.[28] Therefore, Smart Grid technologies can pose great threats to consumers' informational privacy rights.

Additionally, third parties will inevitably get involved with Smart Grid technologies, especially considering how much information would be shared.[29] Third parties include those with presumably authorized use of consumer energy information, like appliance manufacturers and marketers, and those with unauthorized use, like criminals.[30] Even though only small locations have tested Smart Grid technologies, Google is already involved.[31] It created an application, called Google PowerMeter, for consumers to track energy usage in the home.[32] This software communicates with smart meters to provide consumers with detailed energy information.[33] While consumers benefit by knowing how much energy they use at any given time, PowerMeter allows Google to gain access to consumer information to which it generally would not have access. Therefore, parties other than a customer's utility may have access to the consumer's entire energy report.

Finally, Smart Grid technology presents an even greater problem to consumer privacy when an individual's information is aggregated.[34]

SECURITY], *available at* http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf (noting that energy consumption information collected over a long period of time can show lifestyle patterns, including "the number of individuals at a premise, when the location is unoccupied, sleep schedules, work schedules, and other personal routines").

28. SMART GRID CYBER SECURITY, *supra* note 27, at 29; *see also* McDaniel & McLaughlin, *supra* note 3, at 72, 74 (stating that certain activities, like watching television, "have detectable power consumption signatures," thus making it easy to track television use); INFO. & PRIVACY COMM'R, PRIVACY BY DESIGN: ACHIEVING THE GOLD STANDARD IN DATA PROTECTION FOR THE SMART GRID 13 (2010), *available at* http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf ("Digital smart meter data . . . is vulnerable to copying and sending, and therefore lends itself to the possibility for a much larger dissemination of 'comings and goings.'").

29. DOE ROUNDTABLE, *supra* note 11, at 38.

30. SMART GRID CYBER SECURITY , *supra* note 27, at 35.

31. *Google PowerMeter: A Google.org Project*, GOOGLE POWERMETER, http://www.google.com/power meter/about/index.html (last visited Dec. 1, 2011).

32. *Id.*

33. *Become a Google PowerMeter Partner*, GOOGLE POWERMETER, http://www.google.com/powermeter/about/partnerships.html (last visited Dec. 1, 2011).

34. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1185 (2002).

> The aggregation problem arises from the fact that the digital revolution has enabled information to be easily amassed and combined. Even information in public records that is superficial or incomplete can be quite useful in obtaining more data about individuals. . . . For example, although one's Social Security number does not in and of itself reveal much about an individual, it provides access to one's financial information, educational records, medical records, and a whole host of other information.

Id.

Information collected about a consumer's energy use may be harmless by itself, but in the aggregate with all information collected by the Smart Grid, "it begins to paint a portrait about our personalities."[35] Not only can all Smart Grid information be compounded together, but it can also be compiled with other information collected by technology such as sites most frequented on the Internet. Bits of information that are meaningless by themselves can easily be gathered to create a "digital biography."[36] Such compilations become troublesome when the federal government and private sector use large databases to investigate individuals for various reasons.[37]

II. THE CONSTITUTIONAL RIGHT TO PRIVACY

Smart Grid technologies, by gaining access to and sharing energy-consumer information on an unprecedented level, inevitably implicate individual privacy. At the beginning of the twentieth century, the Supreme Court first began to recognize an individual's constitutional right to privacy and the importance of protecting this right against government intrusion.[38] The Constitution acknowledges and protects the worth of every individual, whose rights should be protected from government infringement.[39] Courts have since interpreted the Bill of Rights to include "the right to be let alone."[40] Even in earlier cases, the Supreme Court referenced the right to individual privacy. For example, in *Union Pacific Railway Co. v. Botsford*, the Court held that a plaintiff cannot be forced to submit to a medical examination to recover for injuries in a civil suit.[41] The Court reasoned that "the right of every individual to the possession and control of his own person, free from all restraint or interference of others" was the most protected right.[42]

---

35. *Id.*

36. *Id.* at 1186.

37. *Id.* at 1189.

38. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (expanding upon the liberty right and recognizing that the Framers sought to protect citizens from the government and provide for every citizen "the right to be let alone–the most comprehensive of rights and the right most valued by civilized men"); *see also* Meyer v. Nebraska, 262 U.S. 390, 399 (1923) (noting a person's specific liberty rights, including "freedom from bodily restraint . . . and generally to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness," but also noting that the Court did not "define with exactness the liberty thus guaranteed").

39. Erwin N. Griswold, *The Right to Be Let Alone*, 55 NW. U. L. REV. 216, 216 (1960).

40. *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

41. Union Pac. Ry. Co. v. Botsford, 141 U.S. 250, 251 (1891).

42. *Id.*

A. Constitutional Foundations of the Right to Privacy Through Reproductive Autonomy Cases

The Supreme Court formed the right to privacy under the Constitution through reproductive cases, evolving the doctrine of personal autonomy.[43] The foundation for the right was formed in *Griswold v. Connecticut*, where the Court held unconstitutional a Connecticut law banning the use or distribution of contraceptives.[44] Because the Court had already liberally expanded the First Amendment to include certain rights not specifically stated in the Constitution, the Court could also read the right to privacy into many constitutional amendments.[45] While the right to privacy is not specifically stated in the Constitution, the Court has found it in the penumbras of many provisions of the Constitution, including the First, Third, Fourth, Fifth, and Ninth Amendments.[46] Penumbral rights are those "necessary in making the express guarantees [of the First Amendment] fully meaningful."[47] Privacy is similar to the right of association, where associating with others to express an opinion is not directly stated in the First Amendment, but it is necessary to preserve free speech.[48]

To support its assertion, the Court cited sources taking an expansive view of what constitutes privacy.[49] The right to privacy protected not only the privacy of a married couple's bedroom but also the right to "control information about contraceptive use."[50] While the facts of the case were limited to a married couple, the Court's analysis of the right to privacy was more extensive.[51] The Court's expansive view paved the way for future cases to take a broad view on privacy rights under the Constitution since

---

43. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1106 (2002) ("The constitutional right to information privacy is an offshoot of the Supreme Court's substantive due process 'right to privacy' cases such as *Griswold v. Connecticut* and *Roe v. Wade*.").

44. Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965).

45. *See* Pierce v. Soc'y of Sisters, 268 U.S. 510, 510 (1925) (holding that a parent had the right to choose how to educate one's child); Meyer v. Nebraska, 262 U.S. 390, 399–400 (1923) (holding that a parent had the right to control one's child's education by allowing a schoolteacher to instruct in German).

46. *Griswold*, 381 U.S. at 484–85.

47. *Id.* at 483.

48. *See* NAACP v. Alabama, 357 U.S. 449, 460 (1958) ("[F]reedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment . . . .").

49. *Griswold*, 381 U.S. at 484; *see also* Boyd v. United States, 116 U.S. 616, 630 (1886) (noting that the right to privacy aims to prevent "the invasion of his indefeasible right of personal security").

50. Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643, 648 (2007).

51. *Griswold*, 381 U.S. at 484–85.

this foundation case relied on theories that took a liberal view.[52] Therefore, the right to privacy is expansive, granting broad privacy rights to individuals in all aspects of life, and not limited to intimate relations.

Later reproductive-freedom cases cite the *Griswold* right to privacy and do not limit the broad scope of the right. In *Eisenstadt v. Baird*, the Court held unconstitutional a Massachusetts law that prohibited the distribution of any contraception.[53] While this case focused on reproductive rights like *Griswold*, it noted that the right to privacy extends to all individuals "to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person."[54] Additionally, in *Roe v. Wade*, the Court held that the government cannot prohibit women from seeking abortions prior to fetus viability, and any government restriction on abortion must pass strict scrutiny.[55] Instead of finding that the right to privacy is a penumbral right within the Bill of Rights, the Court held that it is a fundamental right drawn from a person's liberty interest in the Fourteenth Amendment.[56] The Court explained the right to privacy established in *Griswold*, holding that the right includes those deemed so "fundamental or implicit in the concept of ordered liberty."[57] The right to privacy is thus not limited to reproductive rights but includes other arenas that are inherent to individual liberty.

Since its decision, *Roe v. Wade* has been sharply criticized as improper judicial legislation and for creating a complicated framework for abortion laws.[58] Despite its criticism of the ultimate decision in *Roe*, the Court still accepts its legal analysis and holds that there is a fundamental right to privacy drawn from the language of the Constitution.[59] Additionally, other cases have affirmed the Court's legal analysis. In *Carey v. Population*

---

52. *See id.* at 484–86.

> [S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. . . .
>
> . . . .
>
> We deal with a right of privacy older than the Bill of Rights—older than our political parties, older than our school system.

Id. (citing Poe v. Ullman, 367 U.S. 497, 516–22 (1961)).

53. Eisenstadt v. Baird, 405 U.S. 438, 440 (1972).

54. *Id.* at 453 (citing Stanley v. Georgia, 394 U.S. 557 (1969); Skinner v. Oklahoma, 316 U.S. 535 (1942); Jacobson v. Massachusetts, 197 U.S. 11, 29 (1905)).

55. Roe v. Wade, 410 U.S. 113, 166 (1973).

56. *Id.* at 153.

57. *Id.* at 152 (quoting Palko v. Connecticut, 302 U.S. 319, 325 (1937)) (internal quotation marks omitted).

58. *See* Webster v. Reprod. Health Servs., 492 U.S. 490, 520 (1989) (stating that *Roe* improperly created an entire constitutional framework of analysis throughout a pregnancy, which is traditionally left to state regulation as an issue of medical health).

59. *Id.* at 548.

Services International, the Court held that a New York law banning the distribution of contraceptives to minors was unconstitutional.[60] The Court affirmed *Roe* and held that the right to privacy is a fundamental right drawn from the liberty interest in the Due Process Clause of the Fourteenth Amendment.[61] Despite much criticism of the ultimate holding in *Roe*, the Court has never challenged its legal analysis of a broad right to privacy.

B. Constitutional Protections Afforded the Right to Informational Privacy

While the foundational cases for the right to privacy primarily dealt with personal autonomy, the Court also recognizes a right to informational privacy.[62] Earlier cases like *Griswold* did not discuss informational privacy because technology was not as advanced as it is today, thus not presenting threats to an individual's information. Even though the early Court did not specifically address the right to informational privacy, this right is not an entirely modern concept. Early Supreme Court cases that established the right to privacy, like *Griswold* and *Eisenstadt*, were factually limited to marriage and reproductive rights but did not take such a narrow view on the substance of the right.[63] Therefore, privacy rights should be seen as a broad protection of an individual's right to control things so fundamentally affecting oneself.[64] The right to privacy is not limited to reproductive autonomy but has been extended to include many different privacy interests.

The Court has extended the right to privacy beyond personal autonomy to include personal information, especially with the advent of increasing technology and information-sharing.[65] However, since information-sharing technologies like the computer and the internet are relatively new, the right to informational privacy is much less developed in the courts than the right

---

60. Carey v. Population Servs. Int'l, 431 U.S. 678, 681 (1977).

61. *Id.* at 685.

62. *See* JON L. MILLS, PRIVACY: THE LOST RIGHT 14 (2008) (stating that the right to privacy includes both "decisional" and "information" privacy (quoting Dorothy J. Glancy, *Privacy on the Open Road*, 30 OHIO N.U. L. REV. 295, 321 (2004))).

63. *See* Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (holding people have the right "to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person"); Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (holding that the Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects" (quoting U.S. CONST. amend. IV)).

64. *See* JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 62 (1997) (explaining that this broad privacy right includes "our ability to control information about ourselves, our ability to govern access to ourselves, and our ability to make self-expressive autonomous decisions free from intrusion or control by others").

65. Since *Griswold*, the Court has expanded the right to privacy to include a right to information privacy. DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 21 (2003).

to personal autonomy.[66] In *Whalen v. Roe*, the Court held that a state filing system with the names of all patients taking certain controlled substances, as prescribed by a doctor, did not violate privacy rights.[67] Despite its holding, the Court specifically outlined a person's right to informational privacy. Along with the right to make important decisions, such as to bear or beget a child, as seen in *Roe* and the reproductive-autonomy cases, individuals have the right to resist "disclosure of personal matters" under *Whalen*. [68] The Court held that the filing system infringed upon a person's "interest in the nondisclosure of private information."[69] The state could still create the database, however, because health-care law requires certain public disclosure of private patient information, as in providing information to insurance companies.[70] After concluding that individuals have the right to keep personal information private, the Court upheld the provision only because health-care law has always required certain patient disclosures to the state.[71]

While the Supreme Court has recognized that the Constitution protects informational privacy, this right is not as highly protected as personal autonomy. Any government restriction on a fundamental right, like the right to reproductive autonomy, must past the highest standard of strict scrutiny.[72] The Court has not held that the right to personal informational privacy is a fundamental right, thus any state restriction on this right will not be subject to the strictest standard of review. The right to informational privacy, however, is still a privacy interest that deserves protection. Therefore, governmental restrictions on this right are subject to rational basis review, a lesser standard that gives great deference to a legislative decision.[73]

In most cases where the government has restricted an individual's right to informational privacy, the courts have upheld the government action because the lower scrutiny standard is relatively easy for the government to

---

66. *See* MILLS, *supra* note 62, at 16 ("Control of personal information is the least developed sphere of privacy and the sphere with the least legal protection.").

67. Whalen v. Roe, 429 U.S. 589, 591 (1977).

68. *Id*. at 599.

69. *Id*. at 600.

70. *Id*. at 602.

71. *Id.* at 601–04.

72. *See* Roe v. Wade, 410 U.S. 113, 155–56 (1973) (holding that the government must show a compelling state interest that is "narrowly drawn to express only the legitimate state interests at stake" when it restricts a fundamental right).

73. MILLS, *supra* note 62, at 17 (noting that rational-basis review "requires a legitimate governmental interest"); *see also* Heller v. Doe, 509 U.S. 312, 319 (1993). *Heller* held that rational-basis review is appropriate for restrictions "neither involving fundamental rights nor proceeding along suspect lines," as with race-based regulations. Restrictions subject to rational-basis review are "accorded a strong presumption of validity." *Id.*

meet.[74] However, some cases have found that the government unconstitutionally intruded upon an individual's informational privacy interest. In *Kallstrom v. City of Columbus*, the Sixth Circuit applied strict scrutiny and held that the city could not release the names and addresses of police-officer witnesses who testified against gang members because it placed the officers' families in "special danger."[75] *Kallstrom* is significant because it shows that a court has only rejected governmental disclosure of personal information when such disclosure has also impacted an individual's autonomy in making decisions about the family.

Additionally, courts will protect individuals from governmental intrusion into intimate matters. In *Sheets v. Salt Lake County*, the Tenth Circuit affirmed the district court's ruling that the county violated a husband's right to privacy when it allowed an author to obtain a copy of his murdered wife's diary because it contained information about their marriage.[76] In *Anderson v. Blake*, the court held that the state could not release a video depicting the victim's alleged rape because it showed private matters.[77] Therefore, based on current case law, utilities' use of consumer information will likely be held unconstitutional only if it presents a specific threat towards consumers or infringes upon information regarding an individual's family or intimate relationships.

C. The Constitutional Right to Informational Privacy Related to Smart Grid Technology

A court will likely extend an individual's informational privacy right in light of the new and unique situation Smart Grid technology presents. The Court has recognized that there is an "interest in protecting the well-being, tranquility, and privacy of the home."[78] An individual's home is unique because it is "the last citadel of the tired, the weary, and the sick."[79] In cases

---

74. MILLS, *supra* note 62 at 128; *see also Whalen*, 429 U.S. at 602 (upholding the New York State Controlled Substances Act, which granted the New York Department of Health the ability to electronically store prescriptions for certain controlled substances because certain "private information must be disclosed" to the Department); United States v. Richter, 610 F. Supp. 480, 485–86 (N.D. Ill. 1985) (holding that the Bank Secrecy Act could require individuals to disclose currency transactions); Soc'y of Jesus of New England v. Commonwealth, 808 N.E.2d 272, 283–84 (Mass. 2004) (holding that the state could compel disclosure of a church's members because the governmental action did not create any "adverse consequences" for the members).

75. Kallstrom v. City of Columbus, 136 F.3d 1055, 1067 (6th Cir. 1998).

76. Sheets v. Salt Lake Cnty., 45 F.3d 1383 (10th Cir. 1995).

77. Anderson v. Blake, 469 F.3d 910 (10th Cir. 2006).

78. Frisby v. Schultz, 487 U.S. 474, 484 (1988) (quoting Carey v. Brown, 447 U.S. 455, 471 (1980)) ("The State's interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society." (quoting *Carey*, 447 U.S. at 471)).

79. Gregory v. Chicago, 394 U.S. 111, 125 (1969) (Black, J., concurring).

like *Whalen* and *Richter*, the challenged governmental restrictions involved medical-history and financial-transaction information, which are types of information that the public has consistently tried to protect, unlike energy-consumption information.[80] The Court found no privacy invasion in *Whalen* because patients routinely disclose medical information to insurance companies and government entities.[81]

In contrast, Smart Grid technology would grant utility companies access to information about what goes on inside a person's home, which has never been shared on a mass scale to utilities and government entities. The Court has consistently upheld the right to individual privacy inside one's own home.[82] In *Kallstrom*, the Sixth Circuit preserved the sanctity of the home by denying opposing counsel the ability to know the home addresses of officers because it invaded their right to privacy.[83] Although current Supreme Court jurisprudence indicates that the Court is reluctant to overturn government actions restricting individual informational privacy,[84] this trend will likely change when the energy sector introduces Smart Grid technology. Based on the unique evolutionary jurisprudence around protecting the privacy and seclusion of one's own home, the Court will likely protect informational privacy from excessive intrusion by Smart Grid technology.

Regardless of how the Court may rule on informational privacy relating to the Smart Grid, the reasoning in *Whalen* is important because it shows that individuals have the right to keep certain information private. Even though the government may be allowed to use consumer information, it still must ensure it does not do so excessively and carelessly. An individual's right to privacy includes an "interest in independence in

---

80. The public has not been as concerned with protecting "[e]nergy consumption patterns" as it has been with health and financial records because meters historically only show energy use over a long period of time and the energy sector does not share this information on a mass scale. However, with the rise of the Smart Grid, public concern for individual privacy will likely increase because "energy consumption data can reveal personal activities and the use of specific energy using or generating appliances, and . . . the data may be used or shared in ways that will impact privacy." SMART GRID CYBER SECURITY, *supra* note 27, at 9.

81. Whalen v. Roe, 429 U.S. 589, 602 (1977) ("[D]isclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice . . . .").

82. *See Frisby*, 487 U.S. at 488 (upholding a statute that prohibits picketing near any individual's residence); Rowan v. U.S. Post Office Dep't., 397 U.S. 728, 738 (1970) (holding that businesses could not send unwanted merchandise to a person's home because he is essentially held captive by the material inside his home); Stanley v. Georgia, 394 U.S. 557, 568 (1969) (holding that the state cannot criminalize an individual's "mere possession" of obscene material "in the privacy of his own home").

83. Kallstrom v. City of Columbus, 136 F.3d 1055, 1067 (6th Cir. 1998).

84. *See Whalen*, 429 U.S. at 591 (holding that the medical filing system did not violate the constitutional right to privacy).

making certain kinds of important decisions."[85] In *Whalen*, the State of New York could compile a database of personal drug prescription information because it provided adequate protective safeguards.[86] The state held many hearings and performed studies on the issue of drug abuse and even established a special commission solely to deal with compiling this information for the purpose of combating the state's drug problem.[87] While New York could create the database, the Court still recognized that such a database posed a serious "threat to privacy."[88] If the government must compile such a comprehensive database, then it also has the duty "to avoid unwarranted disclosures."[89] Therefore, any governmental compilation of consumer information from the Smart Grid should take adequate precautions to protect individuals' privacy rights.

Privacy should not be viewed as either completely private or completely public.[90] In this technological age, it is almost impossible to remain completely isolated from any public record.[91] Additionally, the government should not allow full public access to all of its records. It is therefore improper to think of privacy as either wholly public or wholly private. Personal-information privacy should "entail[] control over and limitations on certain uses of information . . . [including] altering levels of accessibility."[92]

Some courts have begun to recognize the idea that privacy interests depend upon the context and that an individual may even have a privacy interest in personal information housed in public records. For example, in *U.S. Justice Department v. Reporters Committee for Freedom of the Press*, the Court held that the reporters' publishing of FBI "rap sheets" constituted an invasion of personal privacy under the Freedom of Information Act exemptions.[93] Although the government once reported the information to the public, the individuals still had a privacy interest based on the

---

85. *Whalen*, 429 U.S. at 599–600 (citing, e.g., Roe v. Wade, 410 U.S. 113 (1973); Doe v. Bolton, 410 U.S. 179 (1973); Loving v. Virginia, 388 U.S. 1 (1967)).

86. *Id*. at 601–02.

87. JOHN D. WOODWARD ET AL., BIOMETRICS: IDENTITY ASSURANCE IN THE INFORMATION AGE 227 (2003).

88. *Whalen*, 429 U.S. at 605 ("We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."); *see also* WOODWARD, *supra* note 87, at 228 ("The Court's opinion concluded with a cautionary note that still echoes loudly today . . . .").

89. *Whalen*, 429 U.S. at 605.

90. Solove, *supra* note 34, at 1177.

91. *Id.*

92. *Id*. at 1178.

93. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 767 (1989) ("[O]ur cases have . . . recognized the privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public.").

circumstances.[94] Thus, the reporters could not dig up and publish the rap sheets.[95] Therefore, even though the energy sector uses information collected by the Smart Grid, it does not mean that the information is purely public. Rather, the information can only be used for the limited purposes for which it was collected.

III. SOLUTIONS TO THE PRIVACY PROBLEM IN SMART GRID TECHNOLOGIES

While Smart Grid technology presents many benefits to modernize the energy sector for a sustainable future, it also threatens individuals' informational privacy by collecting and maintaining increased consumer data. For the Smart Grid to be effective, the energy sector must gain consumer confidence and recognize the dangers this new technology presents to privacy rights.[96] Therefore, in regulating how utilities use consumer information obtained by the Smart Grid, the federal government should build privacy into the Smart Grid model to establish a consistent privacy standard throughout the grid.[97] This way, the energy sector will avoid time-consuming criticism and scrutiny of consumer privacy rights.[98]

The energy industry is unique in our nation because it is monopolized by a few large utilities.[99] Generally, in an open market for goods, consumers can force companies to change unfavorable practices simply by not

---

94. *Id.* at 770–71.

95. *Id.* at 780.

96. *See* DOE ROUNDTABLE, *supra* note 11, at 38 (explaining that the key to effectively implementing Smart Grid technology is gaining consumer confidence).

97. *See* SMART GRID CYBER SECURITY, *supra* note 27, at 40 (stating that for Smart Grid innovation to be successfully implemented on a mass scale, there needs to be "effective and transparent privacy practices [that] are consistently implemented, followed, and enforced within the Smart Grid"). According to the Electric Power Research Institute, one procedural challenge to the Smart Grid is gaining a consensus on the standards. Therefore, EPRI recommends a consensus on the standards applicable to the Smart Grid because "[c]onsensus-based standards deliver better results over." ELECTRIC POWER RESEARCH INST., *supra* note 10, at 9–10.

98. *See* CAVOUKIAN ET AL., *supra* note 15, at 13.

> Since the future Smart Grid relies on consumers to use and invest in smart technologies, the Smart Grid itself is dependent on ensuring that consumers see the value of such time and investment. If the Smart Grid and smart appliances become synonymous with privacy invasion, visions of the Smart Grid may slow or stall altogether.

Id. (footnotes omitted).

99. Lincoln L. Davies, *Power Forward: The Argument for a National RPS*, 42 CONN. L. REV. 1339, 1346 (2010) (stating that the energy sector is based on several "regulatory compact[s]" where the government gives a public utility a "legally protected monopoly to serve a specified geographic area and, in exchange, assumes the obligation to reliably deliver that service under 'intensive regulation, including price regulation'" (quoting Jersey Cent. Power & Light Co. v. Fed. Energy Regulatory Comm'n, 810 F.2d 1168, 1189 (D.C. Cir. 1987) (Starr, J., concurring))).

supporting them.[100] In contrast, energy consumers have little to no choice in where to get electricity. Thus, they cannot use market pressures to force utilities to protect information collected by smart technologies. Therefore, if the energy industry is to maintain the trust of its consumers, it must consider privacy. Utilities can easily use their monopoly power to control consumer information. This, however, would lead to a complete lack of trust by consumers and potential harmful backlash. The federal government may place strict regulations on the Smart Grid in response, for example. If utilities want to avoid problems in the future, then they should take consumer privacy into account at the outset of Smart Grid implementation. First-generation deployment of Smart Grid technologies should protect customer privacy to avoid costly legal battles that will dampen the success of this needed overhaul for the energy sector.[101]

A. Existing State Laws Regulating Smart Grid Information

Currently, no single federal agency has authority to regulate and enforce privacy protections afforded to energy consumer information.[102] Absent federal regulations, many states have already enacted Smart Grid policies.[103] As the grid expands and becomes interconnected, however, the federal government will have more authority to regulate matters like consumer privacy. Thus, this Note assumes that the federal government will have jurisdiction to protect consumer privacy on the Smart Grid.

Many states have instructive laws on the Smart Grid. These state laws should serve as guidance to the federal government in regulating Smart Grid technology because they show local concern for consumer information. In 2009, California implemented a basic Smart Grid policy to modernize the energy sector "to improve reliability, security, and efficiency of the electric grid."[104] While the policy mentions increased communications between consumer homes and utilities,[105] it glaringly omits consumer privacy. This is a brief policy, only expressing a desire to modernize the grid, which might account for the privacy rights omission.

---

100. PAUL H. RUBIN & THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 3 (2002) ("[M]arket pressures force businesses to compete for the favor of customers, and subject them to consequences—lost business—if they do things that make customers unhappy.").

101. McDaniel & McLaughlin, *supra* note 3, at 74.

102. LICHTENBERG, *supra* note 11, at 31.

103. CAL. PUB. UTIL. CODE § 8360 (2009); ME. REV. STAT. ANN. tit § 3143 (2010); COLO. REV. STAT. § 40-4-118 (2010); S.D. CODIFIED LAWS § 49-34A-93 (2009); D.C. CODE § 34-1562 (2011).

104. CAL PUB. UTIL. CODE § 8360(a) (West 2009).

105. *Id*. § 8360(e).

Even if a Smart Grid policy is brief, however, it must still explicitly protect consumer privacy to ensure consumer confidence in the system.

Recently, Maine enacted a more comprehensive Smart Grid policy, including legislative findings that it is in the state's economic and environmental interests to modernize its energy sector.[106] The state agreed to pursue Smart Grid technologies "that [are] consistent with applicable standards for reliability, safety, security and privacy," and declared that its own state commission may implement rules to protect consumer privacy.[107] Maine properly recognizes that the federal government has the authority to regulate certain aspects of the Smart Grid, and it will follow any future privacy law restrictions the DOE places on the Smart Grid.[108] Additionally, while the DOE does not have consumer privacy protections, Maine's policy specifically states that the local Smart Grid will protect consumer privacy.[109] Maine's policy is a good example of how states can properly address consumer privacy when implementing the Smart Grid.

Some parties argue that states are best suited to protect consumer privacy rights because they can require utilities to follow specific privacy standards.[110] State regulations alone, however, are insufficient to protect customer privacy rights because this approach could result in regulation inconsistencies for a new technology that moves energy information across state boundaries.

B. Federal Government Authority to Regulate Consumer Privacy on the Smart Grid

While some states currently have enacted their own Smart Grid policies, the federal government should regulate to protect consumer privacy to ensure utilities protect this fundamental right in a uniform manner. The most logical way for the federal government to play a role would be to establish standards for how utilities collect and use Smart Grid consumer information. The Federal Power Act delegated basic powers to the federal and state governments in the sale of electricity.[111] The federal

106. ME. REV. STAT. ANN. tit. 35-A § 3143(2) (2010).

107. *Id.* § 3143(3).

108. *Id.* § 3143(1).

109. *Id.* § 3143(3).

110. *See* Cheryl Dancey Balough, *Symposium of Enegy Law: Privacy Implications of Smart Meters*, 86 CHI. KENT L. REV. 161, 187–88 (2011). Balough notes that state regulation of utilities will protect consumer privacy rights because "public utility commissions have regulatory authority over utilities" and "most commissions also have customer privacy policies in place—albeit ones that pre-date smart meters—and utilities take commission policies very seriously." *Id.* (citing NAT'L INST. OF STANDARDS AND TECH., SMART GRID CYBER SECURITY STRATEGY AND REQUIREMENTS, DRAFT 2 at 103 n. 28 (2010)).

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

government regulates electricity transmission lines and wholesale power, while state governments regulate electricity distribution and retail power.[112] Upon first glance, one might assume the states are better suited to regulate Smart Grid information because they regulate small distribution lines to consumers and retail electricity prices to consumers. The federal government, however, is better suited to regulate Smart Grid information to protect consumer privacy rights for three reasons.

First, the federal government has provided substantial Smart Grid funding and thus has a substantial interest in this new technology. The federal government could condition this federal money upon utilities following basic requirements to protect individual privacy. In 2009, the federal government granted $3.4 billion in stimulus funding to promote Smart Grid technology, with much of it going to fund projects in individual states.[113] The federal government often conditions funding to the states and requires the states accepting such funds to take certain actions.[114] The government may condition federal funding pursuant to the Taxing and Spending Clause, so long as the condition is unambiguous, promotes "the general welfare," and is related "to the federal interest in particular national projects or programs."[115] Since Smart Grid technology and consumer privacy rights promote the general welfare and are in the interest of the DOE's programs, the federal government should not have a problem conditioning federal funding for utilities who receive money, so long as the condition is unambiguous. While not all utilities receive federal grants, the federal government may still place privacy conditions for the states that do in order to set a standard for other utilities or local regulators to follow. Thus, the federal government may regulate certain utilities' use of consumer information by conditioning federal funding.

Second, the Commerce Clause grants the federal government the authority to regulate the manner in which utilities collect Smart Grid information. The Commerce Clause grants the federal government the power to regulate "[c]ommerce with foreign Nations, and among the several States, and with the Indian Tribes."[116] Since its creation, the Court has allowed the federal government to regulate activities ranging from purely

---

112. *Id.*

113. Peter Behr, *DOE Grants Jump-Start the Smart Grid Toward a Still Undefined Future*, N.Y. TIMES (Oct. 28, 2009), http://www.nytimes.com/cwire/2009/10/28/28climatewire-doe-grants-jump-start-the-smart-grid-toward-44552.html?scp=2&sq=obama%20funding%20smart%20grid&st=cse.

114. *See, e.g.*, National Minimum Drinking Age Act, 23 U.S.C. § 158 (2006) (stating that States that do not have the drinking age at 21 will receive less federal highway funding).

115. South Dakota v. Dole, 483 U.S. 203, 207 (1987) (quoting Massachusetts v. United States, 435 U.S. 444, 461 (1978) (plurality opinion)) (internal quotation marks omitted).

116. U.S. CONST. art. I, § 8, cl. 3.

local wheat production to local medicinal marijuana.[117] The Commerce Clause grants the federal government the power to regulate channels of interstate commerce, instrumentalities of interstate commerce, and activities substantially related to interstate commerce.[118] In *Gonzales v. Raich*, the Court upheld the Commerce Clause regulation of a woman's local medicinal marijuana use because Congress had a rational basis to believe her activities, "taken in the aggregate, substantially affect interstate commerce."[119] Similarly, utilities often use energy information to make important decisions that affect many states, such as setting rate prices. Since the Smart Grid makes the energy system more interconnected and crosses state lines, a single utility's local use of consumer information may substantially affect interstate commerce, when viewed in the aggregate. Thus, the federal government may regulate local utilities' use of consumer information based on its Commerce Clause powers.

Finally, it is wise for the federal government to create uniform privacy standards for the Smart Grid. Society has recently had much enthusiasm for Smart Grid technologies because of the benefits they present; however, the pressure to implement these technologies has lead to "fragmented efforts with little or no stakeholder coordination or agreed-upon standards."[120] The Electric Power Research Institute (EPRI) recognizes how important it is to provide uniform standards for Smart Grid technologies to ensure "a fully-connected smart grid" that "offer[s] lasting and extensible value."[121]

C. Existing Federal Privacy Laws That May Serve As a Limitation on Different Actors' Use of Smart Grid Information

Since the Court first outlined the right to privacy, the computer and internet have drastically changed the debate surrounding technology and privacy.[122] There are two different actors that could use information collected by the Smart Grid: the government or the private sector, such as third parties hired to collect information. Regulations are already in place that limit the manner in which a specific party may use consumer information.

---

117. Gonzales v. Raich, 545 U.S. 1, 22 (2005); Wickard v. Filburn, 317 U.S. 111, 128–29 (1942).

118. United States v. Lopez, 514 U.S. 549, 558–59 (1995).

119. *Gonzales*, 545 U.S. at 22.

120. ELECTRIC POWER RESEARCH INST., *supra* note 10, at 18.

121. *Id.*

122. SOLOVE & ROTENBERG, *supra* note 65, at 459 (noting that the computer permanently revolutionized record-keeping and databases).

1. Existing Laws That Limit the Government's Use of Smart Grid Information

The government would be limited by existing regulations in instances where it uses Smart Grid information.[123] Congress embedded an informational privacy right in many statutes for the federal government to follow. For example, the Freedom of Information Act (FOIA) provides that every federal agency shall make their records available to the public.[124] Since its enactment in 1974, amendments to FOIA have made it even easier to access information.[125] However, FOIA still prevents the public from gaining access to personal files, "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[126] Even though the purpose of FOIA is to increase transparency in federal agencies, it still provides specific safeguards for an individuals' right to informational privacy. There is, however, no absolute right to informational privacy under FOIA. If personal information is disclosed because it does not create an "unwarranted intrusion" on individual privacy, the agency does not need to notify the individual, nor does the person have the right to prevent the dissemination.[127]

Smart Grid technology presents a unique problem for regulating agencies and FOIA because the energy sector has never implemented this technology on a mass scale. Cases dealing with informational privacy, like *United States Department of Justice v. Reporters Committee*, can be instructive. The right to privacy includes the right to control information about and involving oneself.[128] Private information is that which is not available to the public, and instead only "intended for . . . the use of a particular person or group or class of persons."[129] Public dissemination of information specifically linked to private individuals does not further the goals of the FOIA because an individual's personal information does not reveal anything about the agency's conduct.[130]

With Smart Grid technology, however, any agency using information would base its energy decisions upon energy consumer information. For

---

123. While the DOE may not be the best federal agency to ultimately regulate consumer privacy, it is currently the best option. A new federal agency may be created just for this purpose. *See* Implementing the National Broadband Plan, *supra* note 1. Recognizing that DOE alone cannot regulate the Smart Grid, the agency asks: "How can DOE best implement its mission and duties in the Smart Grid while respecting the jurisdiction and expertise of other Federal entities, states and localities?" *Id.*

124. Freedom of Information Act, 5 U.S.C. §§ 552(a)(2)(A)–(E) (2006).

125. SOLOVE & ROTENBERG, *supra* note 65, at 462.

126. 5 U.S.C. § 552(b)(6).

127. Solove, *supra* note 34, at 1162.

128. U.S. DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

129. *Id.* at 763–64.

130. *Id.* at 773.

example, the agency may wish to promote the installation of more solar panels in an area because its consumers use more energy during the day. A party wishing to know why the agency made a specific determination would, presumably, be granted access to the agency's findings of consumer behavior. This disclosure runs the risk of exposing individuals' personal information to an "unwarranted invasion."[131] Yet, if the agency does not disclose the information, it may run afoul of FOIA requirements. Therefore, the agency must remove specific consumer names and identifying marks in its findings that may be made public. It may present data to the public of specific energy figures in an area, but it may not leave any identifying marks to any particular consumer.

Additionally, the Privacy Act represents great concern over individual privacy rights in centralized federal government databases.[132] Congress enacted the Privacy Act eight years after FOIA in response to concerns raised by the scope of FOIA. While FOIA grants access to federal agency information, the Privacy Act grants individuals more control over information about themselves in agency records.[133] Even though FOIA contains a specific provision protecting personal information from unwarranted intrusion, Congress enacted further protections to safeguard personal information through the Privacy Act. Therefore, if the federal government uses consumer information collected through Smart Grid technologies, it must consider privacy issues based upon these existing federal regulations.

2. Existing Laws That Limit the Private Sector's Use of Smart Grid Information

Another actor who would be likely to use Smart Grid consumer information is the private sector. The Constitution only prevents government actors, not private ones, from intruding upon personal privacy rights.[134] Thus, the constitutional protections for consumer privacy in *Whalen* may not apply to private entities. These protections will apply to private entities, however, if there is a "sufficiently close nexus" between the government and private entity.[135] It is more likely that utilities will have a

131. 5 U.S.C. § 552(b)(6).

132. *U.S. DOJ*, 489 U.S. at 767.

133. *See* Greentree v. United States Customs Serv., 674 F.2d 74, 76 (D.C. Cir. 1982) ("The Privacy Act limits access to any 'record' contained in a 'system of records' without the consent of the individual to whom the record pertains . . . ." (footnotes omitted) (quoting 5 U.S.C. §§ 552a(a)(4)–(5) (1982))).

134. MILLS, *supra* note 62, at 124 (citing United States v. Morrison, 529 U.S. 598 (2000)).

135. Jackson v. Metro. Edison Co., 419 U.S. 345, 350–51 (1974) (holding that the state-regulated utility did not have a "sufficiently close nexus" with the government to constitute a state actor).

"sufficiently close nexus" to the government than a private corporation. Utilities are generally more connected to the government than private corporations are, and the federal government has provided substantial funding for states to implement Smart Grid technologies.[136] While utilities may have enough of a connection with the government to be considered a state actor—and thus subject to constitutional protections—third-party corporations are likely to be considered private entities and, as such, outside the realm of constitutional protection.

Many federal statutes limit private entities' use of personal information, mostly imposing criminal liability for wrongful conduct. For example, the Computer Fraud and Abuse Act imposes criminal penalties if a person "intentionally accesses a computer without authorization or exceeds authorized access."[137] The Electronic Communications Privacy Act makes it unlawful for a person to "intentionally access[] without authorization" a stored database of information.[138] Finally, the Wiretap Act criminally punishes a person who "intentionally intercepts . . . any wire, oral, or electronic communication."[139] Most of these criminal penalties apply only to those purposefully and wrongfully gaining access to personal information. If private parties collect personal information from the Smart Grid, then it is likely because a governing body granted them access. There are, however, criminal sanctions for private parties who gain access to and use consumer information without the consent of the utility or the consumer. These criminal penalties would not apply to a private entity that was allowed to collect consumer information unless it intentionally infringed on consumer privacy rights.

D. Federal Agency Involvement in Protecting Consumer Privacy in Smart Grid Technology

1. Federal Agencies with the Authority to Establish Smart Grid Privacy Standards

The federal government, through a division in the Commission, should regulate how utilities can use consumer information collected by the Smart

136. Kate Galbraith, *States Get Federal Smart Grid Funds*, N.Y. TIMES GREEN BLOG (Oct. 27, 2009, 8:02 AM), http://green.blogs.nytimes.com/2009/10/27/administration-announces-smart-grid-funds/.

137. 18 U.S.C. § 1030 (2006).

138. 18 U.S.C. § 2701 (2006).

139. 18 U.S.C. § 2511 (2006).

Grid.[140] The Commission is currently the most appropriate federal agency to create a standard for utilities to protect consumer privacy rights.[141] Other agencies that could create such a standard include the DOE, the Department of Homeland Security, or even the Department of Interior. The Commission, however, is better suited than these agencies to protect consumer privacy rights because of the recently enacted Energy Independence and Security Act of 2007 (EISA), which charges two federal agencies with responsibilities relating to this Smart Grid issue.[142] The National Institute of Standards and Technology (NIST) shall "coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of [S]mart [G]rid devices and systems."[143] Once NIST has established a "sufficient consensus" on this framework, the Commission shall "institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to insure smart-grid functionality and interoperability."[144]

Based on the plain language of EISA, NIST creates the framework for Smart Grid interoperability standards, and the Commission ultimately creates the standard through rulemaking. This final Commission rule may include a standard for utilities' use of consumer information that protects individual privacy rights. On July 16, 2009, the Commission adopted a Policy Statement to provide guidance on the important standards to achieve the goals under Section 1305 of EISA, which focused more on cyber security[145] and refused to address the use of consumer energy information.[146] While the Commission initially declined to address the issue of consumer privacy rights, it may choose to address it in its final rulemaking based on NIST's subsequent publications. Throughout its

---

140. *See* 91 Stat. 565, 567 (1977) (establishing the Department of Energy and granting it the authority to "promote the general welfare by assuring coordinated and effective administration of Federal energy policy and programs").

141. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, REPORT TO CONGRESSIONAL REQUESTERS: ELECTRICITY GRID MODERNIZATION – DROGRESS BEING MADE ON CYBERSECURITY, GUIDELINES, BUT KEY CHALLENGES REMAIN TO BE ADDRESSED 1 (2011), *available at* http://www.gao.gov/new.items/d11117.pdf (noting that the Commission is "the primary federal regulator of the electricity system").

142. Energy Independence and Security Act of 2007, Pub. L. No. 110-140, § 1305, 121 Stat. 1492, 1787–88 (2007).

143. *Id.* § 1305(a).

144. *Id.* § 1305(d). Additionally, it is important to note that the Commission recently issued an order that denied instituting rulemaking at that time, pursuant to the Energy Independence and Security Act, because the Commission found there was "insufficient consensus" on the NIST framework. Order on Smart Grid Interoperability Standards, 136 FERC ¶ 61,039 para. 1 (2011).

145. Smart Grid Policy, 128 FERC ¶ 61,060 para. 40 (2009).

146. *See id.* at para. 94 ("Limitations on access to, and use of, individual customer power usage information may be addressed by retail regulators and, in any event, are beyond the scope of this Policy Statement.").

framework publications in 2010, NIST focused on protecting consumer information[147] and even dedicated an entire volume of its first installment of its Smart Grid framework to consumer privacy.[148] Furthermore, the Commission specifically stated that the NIST framework is "the best vehicle for developing smart grid interoperability standards."[149] Thus, while the Commission may have focused solely on cyber security in its initial policy statement, it may still create a final rule that incorporates privacy protections because NIST focused heavily on individual privacy rights and such standards are necessary for information management to "insure smart-grid functionality and interoperability."[150]

Additionally, it is wise for the Commission to adopt privacy standards because it is working with state energy regulators who are concerned with Smart Grid implementation standards. While EISA grants the Commission the power to adopt Smart Grid interoperability standards, it does not provide the Commission independent authority to enforce these standards. Thus, the Commission may only enforce privacy standards created pursuant to EISA if it has independent statutory authority to do so. One source of this independent authority is the Federal Power Act, where the Commission must find those privacy standards are "necessary for smart grid functionality and interoperability in interstate transmission of electric power, and in regional and wholesale electricity markets."[151] While the Commission may be able to justify standards that protect consumer privacy rights under this rationale, it also may not be able to do so, meaning state energy regulators would need to enforce the standards. The Commission is in a good position to establish uniform privacy standards and recommend

---

147. *See* NAT'L INST. STANDARDS & TECH., NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS, RELEASE 1.0, at 37 (2010), *available at* http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf (noting that security in the Smart Grid system is necessary to "ensure that the confidentiality, integrity, and availability of Smart Grid information, control systems, and related information systems are properly protected").

148. SMART GRID CYBER SECURITY, *supra* note 27; *see also* NAT'L INST. STANDARDS & TECHNOLOGY, THE SMART GRID INTEROPERABILITY PANEL, INTRODUCTION TO NISTIR 7628 GUIDELINES FOR SMART GRID CYBER SECURITY 18 (2010), *available at* http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf (noting that the volume dedicated to privacy was developed by representatives from a variety of interested areas, including electric energy, telecommunications, and government, to provide recommendations for relevant privacy concerns).

149. Smart Grid Interoperability Standards, *supra* note 144, at para. 10.

150. Energy Independence and Security Act of 2007, Pub. L. No. 110-140, § 1305(d), 121 Stat. 1492, 1788 (2007).

151. Smart Grid Policy, 128 FERC ¶ 61,060 para. 22 (2009); *see also Smart Grid Architecture and Standards: Assessing Coordination and Progress: Hearing Before the S. Comm. on Tech. & Innovation*, 111th Cong. 5 (2010) (statement of Mason W. Emnett, Associate Director, Office of Energy Policy and Innovation, Federal Energy Regulatory Commission), *available at* http://www.ferc.gov/EventCalendar/Files/20100701105022-Emnett-Testimony-07-01-10.pdf; U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 141, at 13.

that state energy regulators enforce because of their interactions. For example, the Commission and the National Association of Regulatory Utility Commissioners (NARUC) formed the Smart Grid Collaborative to allow federal and state energy regulators to discuss issues and barriers surrounding nationwide deployment of the Smart Grid.[152] Therefore, even if the Commission does not have the jurisdiction to enforce any Smart Grid privacy standards it may still create these standards pursuant to its rulemaking power under EISA and encourage state regulators to enforce them.

In addition to the Commission, the DOE is another well-suited federal agency to create Smart Grid privacy standards. After finding that the nation had a shortage of nonrenewable energy and that energy policy responsibilities needed to be centralized, Congress created the DOE to "promote maximum possible energy conservation measures" and "deal with the short-, mid- and long-term energy problems."[153] The DOE has comprehensive energy power and investigative authority to handle this nation-wide concern.[154] In fact, the DOE has already taken steps to address this issue by asking for comments.[155] Additionally, the DOE's Smart Grid Implementation Strategy Team aims to educate stakeholders about modernizing the energy grid.[156] If consumer privacy is to be considered at the beginning of implementation, then this Smart Grid innovative agency should be the one to enforce regulations that protect consumer privacy. Thus, if the Commission is not sufficiently suited to create consumer privacy standards, then the DOE is another prime candidate for the task.

Both of these agencies recently recognized that consumer privacy should be protected in Smart Grid implementation. Under EISA, the Commission is charged with the responsibility of creating a National Action Plan for Demand Response to reach the nation's maximum demand response potential.[157] The Commission and the DOE filed a joint report

---

152. Letter from Jon Wellinghoff, Chairman of the Fed. Energy Regulatory Comm'n, to the Honorable Joseph I. Lieberman, Chairman of the Senate Comm. on Homeland Sec. & Governmental Affairs, and the Honorable Susan M. Collins, Ranking Member of the Senate Comm. on Homeland Sec. & Governmental Affairs 2 (March 10, 2011), *available at* http://www.ferc.gov/industries/electric/indus-act/smart-grid/lieberman-collins.pdf.

153. Department of Energy Organization Act, 42 U.S.C. §§ 7111–12 (2006).

154. *Id.* § 7111.

155. Implementing the National Broadband Plan, *supra* note 1, at 26,206.

156. *Energy Bar Association Panel Discussing the Smart Grid*, 31 ENERGY L.J. 81, 83–84 (2009).

157. *See* Energy Independence and Security Act of 2007, Pub. L. No. 110-140, § 529(b), 121 Stat. 1492, § 529 (2007). The Act charges the Commission with the following tasks in the National Action Plan:

> (1) Identification of requirements for technical assistance to States to allow them to maximize the amount of demand response resources that can be developed and deployed.

with Congress. In this report, both agencies referenced consumer privacy protections, assuming Smart Grid technologies would protect privacy rights.[158] For example, part of the National Action Plan requires the DOE to provide "detailed quantitative and qualitative information about demand response programs," but these reports will hide individual consumer information to protect privacy rights.[159] The Commission and the DOE properly considered consumer privacy in this early stage of Smart Grid implementation, even though the proposal was solely concerned with studying demand response.

Furthermore, utilities have a "sufficiently close nexus" with the federal government to submit to federal regulation that protects consumer privacy rights based on its federal funding and Commerce Clause powers. It is dangerous to allow private parties to collect information independently and free from restriction because there would not be enough uniformity in the system to ensure the national grid can communicate effectively. Additionally, utilities may bring in their own third-party companies to maintain consumer information databases, thus granting more parties access to consumer information. These companies could target consumers using energy-use information. Marketing agents could use consumer energy information to target an advertising audience.[160] While this is appealing to advertising companies, consumers likely do not want to be bombarded with more advertisements based on how they use energy. Therefore, the Commission or the DOE must regulate how utilities use consumer information.

2. Privacy Principles That the Commission Should Consider

Because Smart Grid technology presents a new challenge to the energy sector, the Commission must establish guidelines for utilities to follow in using information collected by the Smart Grid. A good start is to look at

---

> (2) Design and identification of requirements for implementation of a national communications program that includes broad-based customer education and support.
>
> (3) Development or identification of analytical tools, information, model regulatory provisions, model contracts, and other support materials for use by customers, States, utilities and demand response providers.

Id.

158. *See* FED. ENERGY REGULATORY COMM'N AND THE DEP'T OF ENERGY, IMPLEMENTATION PROPOSAL FOR THE NATIONAL ACTION PLAN ON DEMAND RESPONSE 7 (2011), *available at* http://ferc.gov/legal/staff-reports/07-11-dr-action-plan.pdf (noting that the DOE is working closely with recipients of federal smart grid grants to study consumer behavior for a few years while ensuring "an appropriate privacy level" in using consumer energy information).

159. *Id.* at 14.

160. SOLOVE & ROTENBERG, *supra* note 65, at 492.

guidelines already in place to protect information communicated in the existing digital marketplace. For example, the Fair Information Practices created by the Department of Housing, Education, and Welfare, is a good guidepost.[161] This standard aims to protect individuals' privacy on the internet and it outlines four major principles: (1) companies must notify consumers of any information collected from them; (2) consumers must have the ability to find out how their information is used; (3) consumers must be able to deny a company the ability to use their data in such a manner; and (4) companies collecting consumer data must take reasonable steps to protect the information.[162] The Privacy Act amended FOIA in 1974 and essentially codified the Fair Information Practices. The language used in the purpose of the Privacy Act is to protect personal information from federal intrusion by permitting the individual to require his consent before an agency uses his information.[163] The Privacy Act "permit[s] an individual" to take such steps, thus the federal agency is not mandated to follow the Fair Information Practices.[164]

While Smart Grid technology will likely have to follow these guidelines under the Privacy Act, the Commission should still specifically mention these principles in its regulations placed on utilities' use of the Smart Grid. If the Commission specifically adopted and informed its customers of these principles, then consumers would be aware that the energy sector is conscious of and taking steps to protect privacy rights. Adopting these principles means the federal agency and utilities must follow them. First, the Commission and utilities must inform its customers of any database of consumer information.[165] Simply adding a smart meter to a person's home is not enough to inform them of a change in the energy sector. Consumers must be specifically informed of what Smart Grid technology does and how information utilities collect about their energy usage would be used. Second, individuals must be able to contact the utilities to find out how their energy information is being used.

---

161. *Id.* at 472; Advisory Comm. on Automated Pers. Data Systems, Dep't of Hous., Educ., & Welfare, *Records, Computers and the Rights of Citizens*, U.S. DEP'T OF HEALTH & HUMAN SERVICES: ASSISTANT SEC'Y FOR PLANNING & EVALUATION (Jul. 1973), http://aspe.hhs.gov/dataacncl/1973 privacy/toprefacemembers.htm.

162. SOLOVE & ROTENBERG, *supra* note 65, at 470.

163. 5 U.S.C. § 552a (2006).

164. *Id.*

165. *See* CAVOUKIAN ET AL., *supra* note 15, at 17 (stating that utilities using Smart Grid information must inform consumers about how personal information is used).

3. Who Controls the Information Dictates the Manner in Which the Commission Should Protect Consumer Information

One major concern of parties involved in Smart Grid technology is who owns the information collected by the Smart Grid. There is no absolute owner of Smart Grid information; instead, control of the information is key and control depends upon the situation.[166] If consumer information is used for the public good, then the private utility or government agency controls the information.[167] If the information is used for a commercial purpose, however, then the consumer controls the information.[168] These two basic principles are important to outline how parties in the energy sector may use consumer information. Thus, because various actors have different rights to access information based on the situation, consumer-privacy-protection standards should not be "an all or nothing at all choice."[169]

First, the utility, or government regulatory entity, controls consumer information collected by the Smart Grid for the public good, for example, when deciding whether to build a new generator.[170] For the Smart Grid to be effective, utilities must be able to collect basic information regarding when and how much energy consumers use.[171] This allows utilities to make informed decisions for the public good. Thus, all consumers connected to the Smart Grid must submit to utilities' use of the most basic information. Allowing consumers to opt out of this information sharing would significantly weaken the effectiveness of the Smart Grid. Utilities must receive basic information on each consumer's energy use to determine the exact demand for a given time, thus allowing for better demand load management and more informed decision-making. To ensure the Smart Grid is effective, no customer should be allowed to opt out of its most basic functions.

---

166. There is a difference between ownership of and access to (or control of) Smart Grid information. For the purposes of this Note, it does not matter who owns the information, and the key to protect consumer privacy is determining who has control, or access, to the information. *See* DATA ACCESS, *supra* note 2, at 26 ("[A]ll of the commenters noted the importance of access to energy consumption data . . . .").

167. LICHTENBERG, *supra* note 11, at 24.

168. *Id.*

169. ELECTRIC POWER RESEARCH INST., *supra* note 10, at 11.

170. LICHTENBERG, *supra* note 11, at 24.

171. *See* Mid-Atlantic Power Supply Ass'n v. Pa. Pub. Util. Comm'n, 746 A.2d 1196, 1199 (Pa. Commw. Ct. 2000). Here, the court upheld a Public Utility Commission order allowing consumer choice for electricity generators while also allowing consumers to protect personal information. The court noted that this program required a delicate balance between granting generators broad access to consumer information and protecting customer privacy. Nonetheless, generators needed access to basic information like "a customer's name, address, account number, rate class, and load data" for the program to be effective. *Id.*

Second, the consumer controls information collected by the Smart Grid used for commercial purposes, for example, targeted advertising and consumer energy management.[172] Consumers should be able to require consent before their information is used for commercial purposes because the central goal of the Smart Grid is to promote the public good in the energy sector, and not commercial gains. The third principle under the Fair Information Practices—allowing consumers to opt out of a program—is complicated for Smart Grid technology because utilities must be able to use basic consumer information.[173] Yet, this does not mean that utilities can use consumer information in any manner without consent.

4. Automatic Privacy Protection for Energy Consumers

Along with requiring utilities to follow the Fair Information Practices, the Commission should create a privacy standard that automatically accounts for customer privacy.[174] The privacy policy should allow consumers to opt-in to any programs using personal information beyond the utilities' basic needs.[175] Thus, consumer privacy would be protected automatically unless and until the consumer takes affirmative steps to participate in any program using personal information. This "opt-in" option ensures consumers know how their information is being used. With an increasingly technological society, it is essential for privacy to be the default option with Smart Grid technologies to ensure utilities protect individual rights.[176]

Google's PowerMeter is an illustrative example of consumer information used for commercial purposes. This service monitors "real-time [energy] usage statistics" from a consumer's smart meter and delivers the information to the individual's Smartphone.[177] Many consumers may find

---

172. *Id.*

173. *See* CAVOUKIAN ET AL., *supra* note 15, at 17 ("If an individual does nothing, their [sic] privacy remains intact. No action is required on the part of the individual to project their [sic] privacy—it is built into the system, *by default*.").

174. *See* Implementing the National Broadband Plan, *supra* note 1, at 26,206 (asking "[w]hat security architecture provisions should be built into Smart Grid technologies to protect consumer privacy" after first assuming that privacy would be taken into account when regulating the Smart Grid).

175. *See* DATA ACCESS, *supra* note 2, at 11 (finding that despite the debate about privacy rights and Smart Grid technology, almost all parties involved agree that "[c]onsumers should decide whether and for what purposes any third-party should be authorized to access or receive [personal information]").

176. *See* Privacy by Design, *supra* note 28, at 28 ("*Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.").

177. McDaniel & McLaughlin, *supra* note 3, at 74.

this information helpful, but it also grants a third-party corporation access to an individual's energy use information. Of course, customers must choose to use this Google service on their own, thus making it an "opt-in" program.[178] Any service that allows third parties to use Smart Grid information should be an opt-in service.

The Commission should not use the alternative—an "opt-out" program that automatically uses consumer information unless the individual takes affirmative steps not to participate. Such opt-out programs are time consuming and costly for both consumers and third-party companies.[179] Additionally, companies may not effectively communicate to consumers how their information is used and how they may opt out of the program. People will likely not know how their personal information is used, let alone how to protect it. Therefore, any use of personal information, beyond the basic needs of a utility to manage demand load, should require customer consent.

Even though consumers should opt-in to third parties' use of their personal information, the energy sector could greatly benefit from third-party involvement in the Smart Grid. For example, algorithms can help consumers save money by knowing what they do in their home to save money.[180] Third-party companies can analyze consumer energy use and inform individuals on what behaviors they can change to save money, like changing thermostat temperature.[181] Since these programs should be opt-in, consumers may not know what benefits the Smart Grid presents. Therefore, utilities and the Commission must frame Smart Grid technology as not only a benefit for utilities, but also as a benefit for consumers. While consumers opting-in is the best option for the energy sector to gain consumer trust, it does not mean consumers will necessarily choose to participate in these programs. Many people do not want anyone knowing what goes on inside their homes, so it will be difficult for utilities to get people to opt-in to programs that delve into and analyze energy usage inside their home.[182] Therefore, utilities bear the burden of showing consumers that participating in Smart Grid programs will benefit their overall quality of life.[183]

---

178. *Id.*

179. Jeff Sovern, *Opting In, Opting Out, or No Options at All: The First for Control of Personal Information*, 74 WASH. L. REV. 1033, 1075 (1999).

180. DOE ROUNDTABLE, *supra* note 11, at 45.

181. *Id.*

182. *Id.* at 44.

183. *Id.* at 48.

CONCLUSION

Our nation is suffering from energy problems that require immediate action. One of the most important investments that we must make is in Smart Grid technology, which can increase the overall efficiency of the energy sector. Increased information about real-time energy consumption allows utilities to more efficiently manage demand loads and also allows consumers to manage energy consumption more efficiently. Even though Smart Grid technology presents many benefits to the energy sector, it also presents a major threat to individual privacy rights.

The right to privacy was formed in personal autonomy cases. While the facts of these cases mostly dealt with reproductive rights, the Court took an expansive view on the right to privacy drawn from the Constitution. These foundational decisions paved the way for the Court to hold that the right to informational privacy exists. These cases are instructive to the energy community because privacy must be taken into account when developing Smart Grid technology.

Preventative efforts to protect consumer privacy should be taken at the outset of Smart Grid implementation to avoid bigger problems in the future. Therefore, the Commission must establish standards to protect consumer privacy rights and require utilities to make privacy a default option in any program using consumer information. These steps will ensure that the Smart Grid is consistent with constitutional principles and maintains consumer confidence in the energy sector by protecting personal customer information.

–Lauren Reilly[*†]

* J.D. and Master of Environmental Law and Policy Candidate 2012, Vermont Law School; B.A. 2009, College of the Holy Cross.

† The author would like to thank the staff of the *Vermont Law Review* who worked tirelessly to prepare this article for production. Many thanks to Kevin Jones for his guidance through this subject matter and Professor Michael Dworkin for sparking an interest in the topic. Finally, thanks to all the colleagues, friends and family for the feedback and support, especially Steve Savidge, John & Lil Reilly, and John Reilly.