

**UNITED STATES OF AMERICA  
BEFORE THE  
DEPARTMENT OF ENERGY**

Implementing the National	)	NBP RFI: Data Access;
Broadband Plan by Empowering	)	Docket ID: DOE-HQ-2009-0003-0835
Consumer and the Smart Grid: Data	)	
Access, Third Party Use, and Privacy	)	

**COMMENTS OF  
SOUTHERN COMPANY SERVICES, INC.**

Southern Company Services, Inc., for itself and on behalf of Alabama Power Company, Georgia Power Company, Gulf Power Company, Mississippi Power Company, and its other affiliates (collectively, “Southern”), is pleased to have this opportunity to provide responses to questions contained in the Department of Energy (“DOE”) Request for Information referenced above regarding smart grid customer data issues.<sup>1</sup> Although more detailed responses to these questions are included, Southern would like to first raise some threshold considerations with respect to these customer data issues.

Southern sees great promise in smart grid technologies and has been deploying them for some time. Indeed, Southern has been collaborating with DOE on its Integrated Distribution Management System (“IDMS”) since 2005. This collaboration began with IDMS as a demonstration project on how to construct and integrate a self-healing distribution system along with improved management of the distribution system. It has now transformed into a project to make IDMS fully operational. While smart grid technologies will facilitate the ability to accumulate additional customer data, the legal and proprietary issues being discussed regarding customer data are fundamentally ones that electric utilities have managed for years with state regulatory oversight. Thus, while the technologies may be new, the legal issues are familiar, and there is generally an existing framework within which they can be properly managed. Indeed, Advanced Metering Infrastructure (“AMI”) -- which is a primary focus of many smart grid customer data discussions -- is itself not even a new technology. Rather, this technology has been used to serve commercial and industrial retail customers for some time with beneficial results. In other words, the extension of AMI to residential customers is simply a new application of a familiar technology. In this regard, Southern has deployed a substantial number of AMI meters across its system for its residential customers as well as for its industrial and commercial customers.

---

<sup>1</sup> 75 Fed. Reg. 26203 (May 11, 2010).

Utilities have been collecting customer energy usage data for decades as part of their business. Accordingly, its collection, use, and disclosure have traditionally been subject to the jurisdiction of state law and regulation. This is appropriate, given the primary role that states have in regulating retail electric service. Notably, it has historically been commercial and industrial retail customers -- not residential customers -- that have been most sensitive to the proprietary nature of their energy usage and costs. It is reasonable to expect that residential concerns could develop over time as these technologies evolve (and certain DOE questions anticipate ways in which this may occur). In that event, state regulators would continue to exercise responsibility for these issues.

As reflected in DOE's questions, Southern recognizes that there may be varying expectations regarding retail customers' access to their own usage data. Southern makes energy usage information available to retail customers through its online, secure EnergyDirect and Online Customer Care programs (in addition to information provided through billing statements). These programs include usage data at no additional charge and in a convenient format. In addition, for commercial and industrial customers who see value in obtaining more granular data about their usage (such as hourly load data tools), EnergyDirect provides more detailed information. The varying levels of EnergyDirect's premium services are structured to meet the different types of needs that customers have. Accordingly, EnergyDirect premium services include a subscription price that takes into account the added costs associated with rendering that more granular data and helps to avoid the subsidization of costs associated with premium services by customers who do not choose to use them.

Southern takes issues of data and network security seriously. Southern has its own security architecture in place and has implemented a due diligence program that performs security posture assessments to evaluate vendors who come into contact with customer data. Southern has been very deliberate in its deployment of AMI technology to promptly address any cybersecurity questions that arise and to refrain from deploying components of these technologies before it is satisfied that cybersecurity issues are being addressed.

As reflected by its deployment of the EnergyDirect and related programs and the fact that numerous customers utilize them to differing degrees, Southern supports the view that customers should have a range of reasonable choices in managing their usage and associated data. At the same time, such choices must accurately reflect the costs and benefits associated with them. Given that there can be substantial costs associated with different choices for managing customer data, careful attention should be paid to the costs and benefits associated with any mandate that particular data categories must be handled in a particular way. Moreover, policymakers should recognize the need to ensure that the beneficiaries of any such mandates need to bear their costs so that there is no socialization of costs to those who do not benefit.

With these general principles and understandings in mind, Southern's responses to the questions in DOE's Request for Information are included below.

## **DETAILED RESPONSES TO DOE QUESTIONS**

### **1. Who owns energy consumption data?**

The concept of ownership is broad, and raises complex issues regarding a wide range of rights and obligations, including ones related to control, access and confidentiality. With respect to energy consumption data, both the utility and the customer have interests in this data and will need to access it. A utility will, for example, need to use this information to render bills, maintain routine customer records, and use this information for planning and operating its system.

While these issues may be complex, it is important to note that they are ones that state regulators and utilities have had to manage for years as part of their traditional regulation of retail electric service. While there may now be a national focus on these issues, access and control of a customer's energy consumption data are topics that utilities managed long before the smart grid became a subject of discussion. In other words, while smart grid technologies may be new, these legal issues are not. States, as the authorities over retail electric service, have existing laws, regulatory requirements and accepted policies and practices that establish the current framework for these issues. The fact that the smart grid presents new technologies (or, rather, new applications of existing technologies) does not necessarily imply that the existing legal and policy structures in place for customer-specific energy consumption data are insufficient to address issues raised by these technologies or their application.

While it may not be convenient in these discussions that there is no "one-size-fits-all" response to questions of this nature, this fact reflects the central role that states play in regulating retail electric service and in overseeing the relationship between electric utilities and their customers. Indeed, as a further reflection of these dynamics, it can be expected that states which have adopted retail competition market structures will view ownership of customer energy information differently from other states.

### **2. Who should be entitled to privacy protections relating to energy information?**

The types of privacy protections that a customer would expect likely depend on the type of customer-specific "energy information" in question. In any event, it seems that, other than the utility providing the energy, the customer is the only party that reasonably would have expectations about the privacy of individual customer data. Consistent with the response to the above question, given the role that states have in regulating retail electric service, there likely may be different privacy protections or expectations in different jurisdictions. This is not surprising given the different retail market designs and regulatory frameworks that exist across different states. To the extent that the deployment of smart grid technologies raises new privacy issues, Southern expects that states will consider this within their existing regulatory framework and in conjunction with other retail service requirements. When a utility has aggregated or enhanced individual customer data in such a way that it has been disassociated from customer-specific

information, Southern does not believe that customers have privacy expectations associated with that aggregated or enhanced data.

**3. What, if any, privacy practices should be implemented in protecting energy information?**

Reference is made to the response to the questions above. As the authorities over retail electric service, states have existing legal and regulatory requirements that establish the current framework for these practices. The fact that the smart grid presents new technologies (or new applications of existing technologies) does not necessarily mean that the existing legal and policy structures for privacy practices and customer energy consumption data are insufficient to address issues raised by these technologies. Given the role that states have in regulating retail electric service, to the extent that the deployment of smart grid technologies raise new privacy issues, Southern expects that states will consider them within their existing regulatory framework and in conjunction with other retail service requirements. Should revisions to existing privacy practices be deemed necessary, Southern believes that they could be established through existing state regulatory processes.

**4. Should consumers be able to opt in/opt out of smart meter deployment or have control over what information is shared with utilities or third parties?**

Customer participation in a utility's AMI deployment should not be "opt-in." The decision to deploy AMI metering technology is a routine business decision not unlike many operational decisions made by utilities in deciding the most effective and efficient way to serve the customer. There are numerous system-wide benefits associated with deploying AMI technology that are not related to a particular customer such as reducing a utility's costs associated with meter reading. For these and other reasons, customer participation in smart meter deployment should not be on an opt-in basis because it could prevent a utility from obtaining the system-wide benefits that underlie a decision to deploy AMI technology.

Given the operational needs of a utility for customer information, a customer should not be able to "opt out" of sharing information with a utility. However, Southern does not have concerns with a state requiring that customers "opt in" to the sharing of their energy usage information with unaffiliated third parties that are not supporting the utility in providing services to the customer or providing services requested by the customer.

**5. What mechanisms should be made available to consumers to report concerns or problems with the smart meters?**

Existing mechanisms for reporting concerns or problems to state regulators should be sufficient and familiar to customers in terms of raising questions about the customer's retail electric service. Reporting a concern with a smart meter or AMI technology is not and should not be any different than reporting a concern with a traditional meter.

Customers and state regulators are very familiar with managing those issues. Southern sees absolutely no need to develop a new mechanism for reporting a concern or problem.

**6. How do policies and practices address the needs of different communities, especially low-income rate payers or consumers with low literacy or limited access to broadband technologies?**

Addressing the needs of low-income and other various customer communities is a constant concern, and state regulators have had years of experience in balancing various customers' needs. With respect to smart grid issues, state regulators will achieve this balance in part by focusing attention on the overall benefits associated with new technologies and by ensuring that the cost burden is being shared appropriately. This important evaluation that various states across the country have been (and will continue to be) undertaking is one that does not lend itself to a "one-size-fits-all" policy. Different jurisdictions will have differing perspectives on the relative benefits of these technologies and how they should be deployed. It is important to note that some smart grid technology benefits (*e.g.*, meter reading cost savings) will be enjoyed by the customer regardless of customer income, literacy, or access to broadband.

**7. Which, if any, international, Federal, or State data-privacy standards are most relevant to Smart-Grid development, deployment, and implementation?**

Although numerous data privacy standards exist from a variety of sources, Southern believes that, with respect to energy consumption data associated with retail electric service, state regulators are in the best position to assess these issues and already have authority over other aspects of the electric service out of which the data arises. They understand and are sensitive to the issues surrounding customer expectations and data privacy. To the extent that smart grid technologies prompt a need for additional review of these issues, state regulators are in the best position to weigh and balance the issues that may arise.

Any smart grid data privacy standard should avoid rendering current smart grid technologies obsolete or undermining their value. Moreover, any such standard should avoid creating technological risk by increasing uncertainty as to the prudence of a specific technology or by supporting one group of vendors over another. In other words, any standard should take care to avoid inadvertently discouraging investment in these technologies.

**8. Which of the potentially relevant data privacy standards are best suited to provide a framework that will provide opportunities to experiment, rewards for successful innovators, and flexible protections that can accommodate widely varying reasonable consumer expectations?**

Reference is made to the response to the question above. As noted, state regulators are in the best position to assess these issues and already have authority over the retail

electric service that produces the data. As stated earlier, these are not generally new issues for state regulators to address. However, to the extent that new issues arise with smart grid technologies, allowing state regulators to take the lead in this area creates opportunities for states to work as “laboratories of experimentation”<sup>2</sup> in these and other smart grid issues where they assess customer privacy concerns, cost issues, and opportunities for innovation. As state regulators continue to review and assess their privacy requirements, they may look to other states for information that will guide their review.

**9. Because access and privacy are complementary goods, consumers are likely to have widely varying preferences about how closely they want to control and monitor third-party access to their energy information: what mechanisms exist that would empower consumers to make a range of reasonable choices when balancing the potential benefits and detriments of both privacy and access?**

Customers who wish to provide third party service providers with access to their energy information have a variety of options in the marketplace and those options are likely to grow over time. Home Area Networks (HANs) and in-home displays are third-party in-home devices that provide customers with access to their energy information. The increasing variety of products available in the marketplace reflects the variety of preferences that consumers have with respect to the security level of such data. Customers who adopt these products and services should have a range of reasonable choices in this respect and these choices should grow over time.

**10. What security architecture provisions should be built into Smart Grid technologies to protect consumer privacy?**

Utilities will address security architecture issues associated with the deployment of smart grid technologies just as they have addressed security issues throughout the development of their systems. Given the variety of system designs that exist, it is not likely that a single security architecture will be appropriate for all utilities. Indeed, the security architecture will necessarily be tailored to the services a utility is providing, and a “one-size-fits-all” architecture would therefore end up being both over-inclusive and under-inclusive depending on the utility. Thus, for some utilities it would be inefficient whereas for others it may be ineffective. Simply put, there is no reason for a utility and its ratepayers to incur additional incremental costs installing security architecture to protect data that the utility does not gather and does not plan to gather.

One element that Southern believes is appropriate for its system involves the temporary segmentation and separation of personally identifiable information (PII) from energy usage information as the data flows from the meter back to the utility. Once the segmented and separated information arrives at back-end points within the utility’s secure

---

<sup>2</sup> See *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) (“It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.”)

corporate network, the PII can then be re-coupled with the energy usage information. This process helps to protect customers from third party intrusion by reducing the ability of such intruders to correlate the two sets of information outside of the secure network.

**11. 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?**

As noted above, states generally have the primary jurisdictional role in regulating electric utilities in their provision of retail electric service. This includes metering and customer information issues. DOE should recognize states' traditional jurisdiction and focus DOE efforts on the many activities within its statutory mission. The DOE Smart Grid Task Force was created by the Energy Independence and Security Act of 2007 to coordinate and report on, among other things, what various agencies and private entities are doing in terms of smart grid development and what standards and policies are being developed. DOE has also encouraged smart grid development through American Recovery and Reinvestment Act ("Stimulus Act") grants and other incentives. DOE can best fulfill its duties by continuing these current and valuable activities, without adding unnecessary jurisdictional complications regarding the regulation of retail electric service and associated customer energy information, which has traditionally been in the arena of state regulators.

**12. When, and through what mechanisms, should authorized agents of Federal, State, or local governments gain access to energy consumption data?**

As noted above, energy consumption data generated by smart grid devices does not necessarily present new issues. In fact, federal, state, and local law enforcement agencies already seek access to energy information, including consumption data, through existing legal processes such as subpoenas. In some cases, government agencies are statutorily authorized to periodically collect certain data from utilities. Southern is not aware of any reason or suggestion that these existing traditional mechanisms have proven insufficient.

**13. What third parties, if any, should have access to energy information? How should interested third parties be able to gain access to energy consumption data, and what standards, guidelines, or practices might best assist third parties in handling and protecting this data?**

As a general matter, an electric utility customer should be able to obtain the customer's own energy consumption data. In addition, the customer's expressly authorized, third-party service provider should also be able to obtain the customer's energy consumption data. In the ordinary course of their business, utilities will need to work with their own third-party service providers and vendors who may come into contact with or need energy consumption data as part of the services they are providing to the utility. In doing this, however, utilities should not allow third parties to have access to customer information unless the third party has a contract with the utility and is obligated to

appropriately maintain the confidentiality of such data. To the extent that these service providers / vendors receive customer data from the utility, utilities may require particular audits (such as Verification and Statement on Auditing Standards No. 70 (“SAS 70”) audits) of the security practices of contracted third parties. The utility may also subject the service providers / vendors to compliance with their confidentiality policies and agreements.

Reference is also made to the response to question 9. An array of third-party products provide customers with expanded access to home energy usage information. It is not clear that there is a standard for maintaining the security and confidentiality of customer data generated or collected by these third-party devices. It is worth noting that this issue has been identified by others and is being discussed as part of the National Institute of Standards and Technology’s (NIST) Smart Grid Interoperability Standards Project (SGIP). In the event that standards are developed by NIST or others, third parties should be held to the same standard as utilities. If the utility and vendors are held to different standards, then there could potentially be questions with respect to unauthorized disclosures of customer data that are not verifiable as to the source.

**14. What forms of energy information should consumers or third parties have access to?**

Reference is made to the response to the question above. As noted, customers should be able to obtain their own energy consumption data. In addition, the customer’s expressly authorized, third-party service provider should also be able to obtain the customer’s energy consumption data. Customers (and their third-party service providers) should have access to the data that is appropriate for the rate under which they are served. However, customers should not have expectations of access to information that is not even being collected by the utility or to data that is collected for reasons not related to their rates and which does not comprise a component in the calculation of their rates.

**15. What types of personal energy information should consumers have access to in real-time, or near real-time?**

Reference is made to the response to question 9. Residential customers can have real-time and near real-time access to their energy information through third-party devices and services that can be placed in their homes. In addition, Southern’s EnergyDirect and Online Customer Care programs are examples of additional services that provide access to this type of information. These services make basic usage information available to all customers. As discussed above, EnergyDirect also provides more detailed, near real-time information available to customers who have paid for those additional benefits. By following this approach, Southern helps to ensure that customers who are benefiting from these services are the ones bearing their costs.



**16. What steps have the states taken to implement Smart Grid privacy, data collection, and third party use of information policies?**

As discussed above, state regulators have traditionally exercised jurisdiction over retail electric service which includes customer information issues. The issues presented by smart grid technologies and AMI deployment are similar to issues managed in the past by state regulators and utilities. For this reason, states and utilities may not immediately seek to develop new policies. Nevertheless, some states have begun a review of these issues. This seems to confirm that the existing regulatory framework is appropriate for smart grid and AMI deployment customer data issues.

**17. What steps have investor owned utilities, municipalities, public power entities, and electric cooperatives taken to implement Smart Grid privacy, data collection, and third party use of information policies?**

Southern has implemented comprehensive policies to manage customer information and requirements regarding its collection, access and use. These policies cover the lifecycle of this information from how it is collected, through how it may be accessed and used, to how it must be secured, retained, and ultimately destroyed. These policies have also governed the collection of customer data in an AMI context for several years while Southern has been deploying this technology across parts of its system. While Southern is continually reviewing and refining these policies as circumstances warrant, it does not appear at this time that customer data developed in an AMI context raises unanticipated issues. Of course, if upon review or over time there are issues that need to be addressed, these policies will be updated appropriately.

**18. Should DOE consider consumer data accessibility policies when evaluating future Smart Grid grant applications?**

To the extent that DOE considers it appropriate to consider data accessibility policies as one of many criteria in evaluating future smart grid grant applications, DOE should recognize the authority of state regulatory requirements over customer data and cost recovery. Reference is also made to the response to question 7. In this regard, when DOE is evaluating grant applications, it should take care to avoid actions that could disrupt existing investments in smart grid technologies.

## CONCLUSION

Southern appreciates this opportunity to provide comments on these important questions, and it looks forward to participating further in the ongoing discussion of these and related smart grid issues.

Respectfully submitted,



---

Gordon G. Martin  
Senior Vice-President & General Counsel  
Alabama Power Company

OF COUNSEL:

BALCH & BINGHAM LLP  
Gregory P. Butrus  
Brandon N. Robinson  
1710 Sixth Avenue North  
Birmingham, AL 35203  
(205) 251-8100

Dated: July 12, 2010