Before the
DEPARTMENT OF ENERGY
Washington, D.C. 20585

In the Matter of	)	
	)	
Implementing the National Broadband Plan By Empowering Customers and the Smart Grid: Data Access, Third Party Use, and Privacy	)	NBP RFI: Data Access

COMMENTS OF NEUSTAR, INC.

Neustar, Inc. ("Neustar") hereby submits comments in response to the captioned Request for Information ("RFI") of the Department of Energy ("DOE").[1] The RFI seeks information on smart grid privacy and data collection policies, as well as third-party access to smart grid data and the role of the consumer in balancing the benefits of access and privacy.[2]

I. INTRODUCTION

Neustar provides innovative services that enable trusted communication across networks, applications, and enterprises around the world. One of those services, provided by Neustar Legal Compliance, enables hundreds of telecommunications carriers and Internet service providers nationwide to meet their law enforcement assistance obligations and respond to other legal demands, such as requests by civil litigants for communications calling records.

A. Current Law Enforcement Access to Utility Data

Law enforcement agencies ("LEAs") occasionally approach electric utilities with requests for access to customer usage data to help solve criminal investigations. For example, LEAs may need to determine whether the energy usage patterns at the residence of a suspected drug dealer reflect the presence of "grow lights," which are used for the indoor cultivation of marijuana. The LEA communicates its request by serving the utility with legal process, such as a subpoena. The utility must then review the legal instrument for validity, and if the instrument is found valid, the utility must disclose the requested data.

[1] 75 Fed. Reg. 26203 (May 11, 2010).
[2] *Id*. at 26203.

B. Potential Future Law Enforcement Access to Utility Data

Smart grids are expected to produce new kinds of customer energy records that are more detailed than ever before. Therefore smart grid deployments may generate more requests from LEAs. The requests could be made to investigate cyber attacks on the smart grid; cyber crimes (such as identity theft) perpetrated on the smart grid; or regular crimes, such as the use of a building for a criminal operation, where the smart grid may contain evidence of the crime.

Smart grid data also may be requested by parties engaged in civil litigation. Examples of these civil suits might include divorce cases and property disputes. As in the criminal context, a civil party would serve legal process on the utility. The utility would be required to review the legal process for validity, and if the legal process was found valid, the utility would be required to make the disclosure.

To the extent that existing laws governing privacy and disclosure among utilities are inadequate to address the rising demand for smart grid data, lawmakers could seek guidance from a related source of law. In the communications industry,[3] customer data can be disclosed in accordance with proper legal process. Accordingly, a detailed set of laws has been developed to manage the data in a manner that balances the privacy needs of customers with the disclosure needs of law enforcement and civil litigants. Smart grids are controlled by communications networks. Moreover, smart grids and communications networks perform similar types of data processing[4] for similar purposes.[5] Therefore, the privacy and disclosure principles of communications law are readily adaptable to smart grids.

The above issues are more fully explored in Neustar's white paper, entitled "When Smart Grids Grow Smart Enough to Solve Crimes." A copy of this white paper is attached at Exhibit A.

[3] The communications industry includes local and long-distance telephone companies, cellular radio providers, cable television operators, satellite carriers, Voice over Internet Protocol (VoIP) providers, broadband Internet access service providers, and other providers of voice and broadband data services.

[4] Both types of networks take continuous detailed measurements (in IP form) of service usage patterns among large segments of the population.

[5] Some of the common purposes are to maintain the security and efficiency of critical infrastructure, perform billing services, and determine the geographic location of certain customers or devices.

II. QUESTION 7: WHICH, IF ANY, INTERNATIONAL, FEDERAL, OR STATE DATA-PRIVACY STANDARDS ARE MOST RELEVANT TO SMART-GRID DEVELOPMENT, DEPLOYMENT, AND IMPLEMENTATION?

Some state public utility commissions already have begun to regulate smart grid data privacy. However, they do not appear to have addressed significantly the potential smart grid data needs of law enforcement. A possible model to use for this purpose may be the federal statutes governing the privacy of communications data.

For example, the Stored Communications Act contains a detailed framework for the disclosure of stored communications records to law enforcement.[6] Similar laws could be applied to stored smart grid records. These laws may help strike a balance between the right to privacy and the need to support criminal investigations.

Federal and state laws also govern the disclosure of evidence in civil proceedings.[7] These laws also probably apply to data produced by smart grids.

III. QUESTION 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?

The DOE should fulfill its smart grid mission in a manner that complements the mission of law enforcement. LEAs at the federal, state, and local levels may request smart grid data to conduct their investigations. There should be standards to determine what constitutes a valid request so that customer privacy is protected and investigations are not frustrated. Without a legal framework for the handling of such personally identifiable information, utilities will run the risk of making over-disclosures or under-disclosures to law enforcement.

IV. QUESTION 12: WHEN, AND THROUGH WHAT MECHANISMS, SHOULD AUTHORIZED AGENTS OF FEDERAL, STATE, OR LOCAL GOVERNMENTS GAIN ACCESS TO ENERGY CONSUMPTION DATA?

As explained above, existing laws already require utilities to disclose energy consumption data to LEAs and civil parties in response to valid legal process. As also noted, smart grids are designed to produce data in more variety and detail. The growing complexity of this data environment may invite data requests not contemplated by existing law. This is where the utility industry may need supplementary guidance. Such guidance could be modeled on the experience of the communications industry.

---

[6] 18 U.S.C. § 2701 *et. seq*.

[7] *See, e.g*. Rule 45 of the Federal Rules of Civil Procedure.

In the communications industry, the required legal process depends on the nature of the requesting party and the type of data requested. The appropriate process could be a subpoena, court order, search warrant, or a similar legal instrument used in national security investigations.[8] State laws generally track federal laws but sometimes vary significantly.

Beyond the issue of legal process, communications law imposes certain disclosure obligations on industry. For example, telecommunications carriers must install hardware/software solutions in their network so they can deliver certain technical capabilities to law enforcement when ordered to do so by a court.[9] The carriers must also be prepared, in response to valid process, to disclose usage records stored in the normal course of business. Certain data retention obligations also apply.[10] Similar mandates may be imposed on utilities. If so, lawmakers should carefully consider how to protect customer privacy, meet the needs of law enforcement, and minimize burdens on industry.

Law enforcement disclosure laws could also specify the conditions under which a utility may notify the customer of the LEA request. In certain cases such notice may be appropriate so the customer has the opportunity to challenge the validity of the legal process. In other cases the notice cannot be given without frustrating the investigation. Specifically, once a suspect is aware of the investigation he or she may take action to evade it, such as by destroying evidence or fleeing the jurisdiction.

These are the kinds of mechanisms that may be adopted for agents of federal, state and local law enforcement to gain lawful access to energy consumption data. If so, the goal of these mechanisms should be to strike a fair balance between the need to protect the privacy of energy data, the need to disclose the data in criminal investigations, and the need to minimize industry burdens.

V. QUESTION 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?

Just as smart grids may create the need for procedures to disclose data to agents of federal, state, and local governments, so may the new energy architectures trigger the need for disclosure mechanisms in civil suits. If civil requests are made for smart grid data, any standards of customer control may need to be harmonized with the civil process to avoid frustrating the civil proceedings while giving sensitive customer data the proper protections. Likewise, utilities

[8] *See* n. 2, *supra*.
[9] *Communications Assistance for Law Enforcement Act*, 47 U.S.C. § 1001 *et. seq*.
[10] 47 C.F.R. § 42.6 (requiring 18 months of retention for telephone toll records).

will need to know what kinds of smart grid data they must disclose to civil litigants and under what terms.

For example, in civil proceedings subpoenas are commonly issued by the attorneys who represent the parties. Alternatively, a subpoena may be issued by a clerk of court. The exact procedure varies from state to state. This legal process may need to be accommodated by rules governing smart grid privacy.

Authorities might also consider whether utilities should provide notice to the customers whose data is sought in the civil suits. In communication law, when a service provider is served with a civil subpoena for regular telephone calling records, the provider is generally permitted but not required to notify the affected user. However, a different notice policy may be appropriate for the unique sensitivities of smart grid records.

Undoubtedly, marketing firms and other commercial interests will also seek access to energy consumption data. No formal legal process will be needed in these situations. However, standards must be developed to ensure that the access occurs only with the appropriate control of customers and utilities. Utilities will also need liability protection from harm caused by any third-party misuse of the information.

VI. QUESTION 14: WHAT FORMS OF ENERGY INFORMATION SHOULD CONSUMERS OR THIRD PARTIES HAVE ACCESS TO?

In the communications industry there are no data elements considered off-limits to law enforcement. The only question is whether the given LEA serves the carrier with valid process. As a result, an LEA may collect a suspect's subscriber information (e.g. name, address and method of payment), communications billing records, IP login records, email content, wireless handset location, or any other communications-related information.[11] An LEA may even listen in on a suspect's voice communications in real time, if such monitoring is approved by a court.[12]

The fact that communications privacy law regulates the full gamut of communications data, including highly sensitive data, makes it a valuable resource to help the DOE manage the sensitivities of smart grid data.

VII. CONCLUSION

Utility customers already enjoy a degree of privacy protection when their energy usage data is requested by LEAs and civil litigants. The challenge of maintaining that protection may increase as users generate new types of energy data and reveal more detail about their consumption patterns.

---

[11] *See* n. 2, *supra*.
[12] *Federal Wiretap Act*, 18 U.S.C. § 2510 *et. seq*.

Communications law deals with the full range of communications data, from usage records to real time voice conversations. At the same time, the law carves out limited exceptions to meet the needs of law enforcement and civil litigants. The resulting disclosures of information protect user privacy while meeting the needs of legal process and avoiding undue burdens on industry.

Neustar submits that a similar balance of interests should be struck as the demands of legal process migrate from traditional utility networks to smart grids.

Respectfully submitted,

/s/_____
Joel M. Margolis
Senior Director, Neustar Legal Compliance
NeuStar, Inc.
46000 Center Oak Plaza
Sterling, VA 20166

July 12, 2010

Exhibit

EXHIBIT A

NEUSTAR WHITE PAPER