Edison Electric Institute

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Re: Preliminary FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers

The Edison Electric Institute ("EEI"), on behalf of its member companies, hereby submits the following comments in response to the request by the Federal Trade Commission ("FTC" or "Commission") for input on the consumer privacy framework proposed by the FTC Staff in the above-referenced report.[1] EEI is an association of the United States investor-owned electric utilities ("IOUs") and industry associates worldwide. Its U.S. members serve almost 95 percent of all customers served by the shareholder-owned segment of the U.S. industry, about 70 percent of all electricity customers, and generate about 70 percent of the electricity delivered in the U.S. EEI frequently represents its U.S. members before federal agencies, courts, and Congress in matters of common concern.

Overview

EEI and its member companies are supportive of the Commission's goal "to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits of the ever-changing marketplace."[2] EEI and its members are also generally supportive of the direction of the FTC framework.

[1] Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (released December 1, 2010) ("*Staff Report*").
[2] *Staff Report* at iii.

The nation's IOUs recognize that protecting customer privacy is particularly important with regard to the type of consumer-specific energy–usage data ("CEUD")[3] collected and used by electric utilities to provide reliable service to their customers, as well as to secure the nation's electric grid.[4] However, an important distinction is that this CEUD which utilities collect and maintain is very different in nature and scope from the data which is of general concern to the FTC in the *Staff Report* (*e.g.* web site searches, social networking information, GPS information, grocery store purchase information, etc.).[5] Further, unlike many companies, electric utilities have a long-standing interest in and extensive experience with handling and protecting sensitive customer data in a highly regulated environment. As a result of state regulatory requirements and oversight, IOUs typically have policies and procedures in place to maintain the privacy of CEUD and other customer data. Many of these policies and procedures parallel those proposed in the *Staff Report* in that they control how and to whom customer data may be disclosed, require customer consent for the disclosure of data to third parties,[6] and establish organizational privacy policies. In fact, the "commonly accepted practices" put forth by the FTC for the purpose of delineating when customer consent is required and how data should be treated reflect well-established practices in the electric utility industry. The Department of Energy ("DOE") recognized both that issues of access to and privacy of energy data are not new and the historic role of electric utilities and the states in protecting and managing data access and privacy when in its *DOE Privacy Report* the agency "commend[ed] the utilities' strong track record of

[3] Customer energy usage data includes all data specific to an individual customer's energy use (e.g., total and time-differentiated energy and capacity use).

[4] As noted in a recent GAO Report the issues of data security and grid cyber security are linked because "increasing the amount of customer information being collected on systems (and transmitting it via networks) provides monetary incentive for adversaries to attack these systems, and could lead to the unauthorized disclosure and use of private information." GAO, *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key challenges Remain to be Addressed,* 9 (January 2011) (*GAO Report*).

[5] *Staff Report* at i-ii.

[6] Third parties are those parties who are not under contractual obligations with a utility that include maintaining confidentiality of customer energy usage data.

protecting the privacy of customer data and acknowledge[ed] the traditional responsibility of state utility commissions in regulating issues associated with data privacy."[7]

As was indicated in EEI's comments filed with DOE[8] as well as in the *DOE Privacy Report*, recent National Institute of Standards ("NIST") Guidelines[9] and the GAO Report, the growing deployment of Smart Grid technology introduces a number of new issues related to privacy and security of not only customer data, but of the operational security of the grid as well. Specifically, "[t]he Smart Grid brings with it many new data collection, communication, and information sharing capabilities related to energy usage, and these technologies in turn introduce concerns about privacy."[10] Moreover, "[t]he smart grid vision and its increased reliance on IT systems and networks expose the electric grid to potential and known cybersecurity vulnerabilities associated with using such systems, which in turn increase the risk to the smooth and reliable operation of the electricity grid."[11]

Recognizing that EEI's members have secured customer data for decades, pursuant to state oversight, the introduction of "smart" technologies does raise new issues which need to be addressed. With these concerns in mind EEI and its members have been working with states, DOE, the National Science and Technology Council's Smart Grid Subcommittee, the Federal Energy Regulatory Commission ("FERC"), the Federal Communications Commission ("FCC"), NIST, the White House Office of Science and Technology Policy, and consumers to address a variety of issues related to CEUD privacy, access and security.

---

[7] Department of Energy, *Data Access and Privacy Issues Related to Smart Grid Technologies* at 3 (released October 5, 2010) ("*DOE Privacy Report*").
[8] EEI Comments, DOE Request for Information-Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use and Privacy at 3 (filed July 12, 2010).
[9] The Smart Grid Interoperability Panel – Cyber Security Working Group, National Institute of Standards, *NISTIR 7628 Guidelines for Smart Grid Cyber Security* (August 2010*)* (*NISTIR 7628*).
[10] *NISTIR 7628 Vol. 2 at 1.*
[11] *GAO Report* at 9.

Consequently, EEI and its members urge the FTC to avoid taking any actions which would disrupt what has been described as a "well advised" state-federal partnership model in light of the fact that "Smart Grid technologies are only beginning to be widely deployed, and allowing for experimentation is a sound policy strategy."[12] Instead, the FTC should permit the process to evolve.

I. Scope

In its "Questions for Comment on Proposed Framework" the FTC Staff asks a number of questions related to Scope.[13] For example, it asks whether there are practical reasons that support excluding certain types of companies or businesses from the proposed framework. From both a practical standpoint and to avoid jurisdictional overlaps or conflicts, there is no need to impose the FTC Framework on electric utilities. This is appropriate given that privacy issues related to electric service are unique in view of the key role that states play in the regulation of electric utilities and consumer privacy, and given that utilities, the states, and other federal bodies are already seeking to address any outstanding questions.

Virtually every aspect of utility operation is regulated by state utility commissions, including rates, finances (capital structure, the ability to sell new debt and equity), corporate structure, and services offered.[14] States also control grid modernization because they have authority to disallow associated costs from recovery in rates. As a result, states have jurisdiction over the overall relationship between the utility and the retail customer out of which this data arises. Reflecting this comprehensive jurisdiction, privacy regulation of customer energy data has appropriately been the responsibility of the states, which have developed various privacy protection laws for customer data. States also have consumer protection laws safeguarding

[12] *DOE Privacy Report* at 6.
[13] *Staff Report* at A-1.
[14] *See e.g. NISTIR 7628* Appendix C

interests of energy consumers. Under these and similar laws, information is furnished directly from consumers to utilities in confidence, and it is well established that the public interest requires that utilities maintain the privacy of that information.

Recently, the ongoing role of both the states and the utilities in protecting the privacy of customer energy data has been subject to great scrutiny at the federal level. In its October 2010 *Data Privacy Report* DOE extensively reviewed the privacy efforts of electric utilities as well as the role of state jurisdiction and made a series of broad findings and recommendations on these issues to the states—findings and recommendations which parallel the FTC framework in many aspects. DOE found, *inter alia*, that:

- Utilities should continue to have access to CEUD and to be able to use that data for utility-related business purposes like managing their networks, coordinating with transmission and distribution-system operators, billing for services, and compiling it into anonymized and aggregated energy-usage data for purposes like reporting jurisdictional load profiles.[15]
- Consumers should be able to access CEUD and decide whether third-parties are entitled to access CEUD for purposes other than providing electrical power.
- All classes of electric utility customers should be entitled to protect the privacy of CEUD.
- Utilities should not disclose CEUD to third parties unless a given consumer has consented to such disclosure.
- Jurisdictions designing opt-in authorization processes should require a valid authorization that specifies the purposes for which the third-party is authorized to use CEUD, defines

[15] Utility use of CEUD, which in a rate making context is known as load data, benefits customers in two important ways: (1) it increases the accuracy and fairness of cost allocations, and (2) it increases the cost-effectiveness / efficiency of investments in new capacity.

the term during which the authorization will remain valid and identifies the means through which consumers can withdraw such authorizations.

- Third parties authorized to receive CEUD should be required to protect the privacy and the security (including integrity and confidentiality) of CEUD that they receive and to use it only for the purposes specified in the authorization.[16]

All of these findings and recommendations were broadly supported by the IOUs.

The August 2010 *NISTIR 7628* Privacy Chapter also addressed many of the issues of concern to the FTC; however, unlike in the *Staff Report*, this was done in the specific context of customer energy data. In this chapter NIST discussed the need for privacy impact assessments ("PIAs"), formal privacy policies, clear customer notice, choice and consent, and limitations on data collection, use, retention and access.[17]

The reality is that electric utilities already have their own data privacy policies and practices in place in accordance with state statutes and/or regulations promulgated by state regulatory authorities, and in some cases, state regulatory mandates. These utility privacy policies are not new and pre-date Smart Grid development. These policies and practices are already being studied and commented on at the state and federal levels. Through these processes utilities are following the practices advocated by the FTC and other Federal bodies.[18]

Even so, EEI members are undertaking a variety of approaches to mange confidential information with proper oversight from appropriate personnel. Among the best practices include the creation by some EEI members of a program for the management of confidential information with senior management oversight of corporate privacy policy issues, as well as monitoring for necessary policy changes, and responding to privacy-related concerns and inquiries. This is

[16] *DOE Privacy Report* at 10-15.
[17] *NISTIR 7628* at 40-43.
[18] See NARUC Resolution on Smart Grid (July 21, 2010).

consistent with *NISTIR 7628*, which recommends that an organization should formally appoint positions and/or personnel to ensure that information security and privacy policies and practices exist and are followed.[19] Likewise, consistent with the NISTIR's recommendation, some EEI members are tasking existing compliance officers and risk management with similar responsibilities. The need for confidential information management with oversight by senior management, as recognized by some utilities, arises from privacy issues greater than those posed exclusively by Smart Grid development.

Some EEI members are forming internal organizations to review customer privacy issues and policies. This is also consistent with the *NISTIR 7628's* recommendation that there should be audit functions present to monitor all data access and modifications.[20] Utilities are also gathering input and expertise from their legal departments in review of state privacy requirements as applied to customer privacy as Smart Grid technologies are continuing to be evaluated and/or in some cases deployed. Other utilities have developed data access policies to be implemented prospectively, based on the privacy and data access consensus guidelines developed by EEI's members. One particular program initiated by Consolidated Edison Company of New York, Inc. ("Con Edison") includes a home area network ("HAN") demonstration project involving approximately 300 customers who will have one of three different types of HAN technologies and approximately 1200 customers who will have a web service application to display meter usage. The HAN technologies are represented by three different vendors and variations of hardware combinations. As part of this pilot program, Con Edison is reviewing the security measures of each HAN provider to protect the privacy of the customer energy usage information. One key security requirement for these programs is SAS70 certification. Con Edison also has

[19] *NISTIR* 7628 at 18.
[20] *Id.*

administrative controls in place with vendors including non-disclosure agreements and contractual language that requires them to keep customer usage information private. Con Edison is sharing meter usage information through secure file transfer protocol ("FTP") from its corporate network to vendors' secure databases.

The current private/public process should be permitted to proceed. Smart Grid services and technologies are evolving, and it remains uncertain exactly what types of services will be available to consumers. Different types of Smart Grid technologies will demand different mechanisms to empower customers to make reasonable privacy choices.

Consequently, EEI urges the FTC to proceed carefully in developing guidance as to privacy practices to protect energy information. Smart Grid technology is new and evolving, and it is premature to decide what privacy practices should be implemented to protect consumer information. Any privacy practices must be sufficiently transparent for customers, utilities and third parties, and must facilitate, rather than impede, Smart Grid development. Further, utilities have a strong track record of safeguarding the privacies and energy usage information of their customers based on existing practices and regulatory structures. Absent clear evidence of neglect or abuse by utilities in protecting customer electronic data, there is no rational reason for the FTC to establish specific standards to protect energy information.

II. Consumer Choice

Notwithstanding EEI's view that the scope of the FTC's proposed framework should not be interpreted to apply to CEUD because it could further complicate—and even conflict with—the existing regulatory framework governing such data, many utility uses of CEUD would not be subject to choice even within the draft FTC framework. FTC Staff has indicated that under its proposed framework companies would not need "to provide choice before collecting and using

customer data for commonly accepted practices" once the customer has elected to use the service.[21] This is absolutely critical in the utility area. As noted by DOE, it is important that utilities be able to access and use CEUD for billing and operational purposes[22] and the list of commonly accepted practices reflects this fact. Utilities must continue to have full access to and control over all CEUD, including operational data and granular data, as part of their legally-mandated obligation to provide safe, reliable and cost-effective service. This information is required for reliability purposes, to ensure utilities can adequately meet daily and seasonal peak loads, and to make certain that utilities are continually aware of new system loads as well as existing and future penetration.

Moreover, since utility access to individual CEUD is required for proper utility billing, as well as for reliability, safety and compliance purposes, a customer should not be permitted to preclude utilities from using CEUD or other consumption data in connection with the provision of service. Similarly, utilities should not be required to obtain customer approval for use of this data in their provision of energy services.

The FTC also asks a series of other questions with regard to customer access to data.[23] With regard to customer access, customers should have access to CEUD reflecting the electric service they take, with that data being provided by utilities through accepted and secure methods of data transportation, using reasonable methods that are technically feasible for the utility. Consumers should have access to usage information that their utility or metering authority uses for billing purposes.

Consistent with applicable state regulations, customers should be able to choose to share CEUD (on an "opt-in" basis) with third parties, or request that their utility share this information

[21] *Staff Report* at 53.
[22] *DOE Privacy Report* at 10.
[23] *Staff Report* at A-3 – A-6.

to participate in utility or third party programs. The frequency and manner of providing access to CEUD should be developed between utilities and their applicable state regulatory agencies, since these elements of CEUD access must account for the rate design and other factors within a particular market area.

The FTC should recognize that different consumers will likely desire different degrees of CEUD access, and disclosure and mechanisms must account for these preferences. Some may permit access by multiple parties to broad portions of energy usage data, including HAN data, while other customers may prefer to be more restrictive in granting data access. Similarly, subject to resolution of cyber security concerns, third parties may be allowed to transmit data from the utility meter to other devices, while other states and their consumers will not prefer this activity.

As reflected in the *DOE Privacy Report*, electric utilities should not be required to share data with third parties unless specifically authorized by customers.[24] It is important that third party energy service providers be subject to the same restrictions as are electric utilities. In particular they should be required to obtain explicit customer approval prior to reselling or distributing data.

III. Transparency of Data Practices

The FTC asks for input on various questions related to the nature of the notice that should be given to customers, how consent should be obtained, and costs. With regard to the question of standardized notice formats, it is important that utilities not be required to provide notices or data in a uniform format because they are subject to varying state requirements.

Utilities should be able to charge third party energy service providers a reasonable cost for access to data. To the extent third parties desire access to more detailed energy usage data,

[24] *DOE Privacy Report* at 15.

access to data on a more frequent basis, or at a more granular level, the associated costs of providing such information should be appropriately allocated between third parties and utility customers as determined by state regulators. As DOE has recognized "to the extent that utilities are *required* to disclose data that is either reasonably available from consumers, in excess of that required to provide optimal electric-utility services, or utility-'enhanced' data not used in billing, a cross-subsidy may occur—at least if utilities cannot charge fees for third-party access to such data."[25] EEI agrees with DOE that "[s]ound economics and public policy suggest that an entity causing particular costs should pay for those costs so that these entities do not demand the good without appreciating its true cost."[26]

IV. Consumer Education

The Staff Report asks a very important question: "How can individual businesses, industry associations, consumer groups, and government do a better job of informing consumers about privacy?" In answer, EEI and its member companies recognize that customer engagement at all levels is critical, particularly with regard to new energy services. Generally, customers have not been exposed to the various benefits that the Smart Grid will produce, nor may they be generally aware of the privacy protections already in place under utility policies and practices adopted under state regulatory insight. Used properly, Smart Grid data can enhance customer quality of life and is not a threat.

Proactive utility communication and education efforts are vital to avoiding a consumer backlash against the Smart Grid. These efforts require outreach through different types of media channels, multiple languages and other innovative techniques. For example, Oncor Electric Delivery ("Oncor"), as part of its advanced metering deployment initiative, reached out to its

[25] *DOE Privacy Report* at 21.
[26] *Id.* at 22.

customers through mailings, leaflets, newspaper articles, and door hangers. The utility dispatched a mobile "experience center" demonstration truck that went directly to the communities, and hosted a series of events across its service territory to enhance communications with the public.

In addition to these types of proactive communication and outreach efforts, utilities should engage customers as necessary through innovative media channels, including social media outlets, Internet-based energy consumption tools, and email/text notification programs to reach customers. Given that customers differ in their needs and preferences for Smart Grid applications, and that these differences vary uniquely between service territories, utilities are best positioned to identify various individual customer segments, and to target messages to these groups.

As part of these efforts, there is also a need for broad public education about the electric system generally and about the benefits of Smart Grid technologies and applications. The federal government (with industry stakeholder support/involvement, etc.) can provide national leadership through broad public education messages to residential and commercial customers.

Given the complexity of these challenges, EEI believes that the most efficient path to addressing these challenges is to initiate a collaborative process that would encompass all major stakeholder groups including regulators (state and Federal) and the Administration. A few venues where collaboration is occurring include the ongoing work by EEI to engage industry stakeholders in dialogue to address Smart Grid implementation issues, the FERC/NARUC Smart Grid Collaborative, the current regional transmission planning process, and the DOE's Smart Grid Information Clearinghouse.

V. Conclusion

EEI respectfully requests that the Federal Trade Commission consider these comments and ensure that any action is consistent with them.

Respectfully submitted,

EDISON ELECTRIC INSTITUTE

David K. Owens
Executive Vice President

Aryeh B. Fishman
Director, Regulatory Legal Affairs
Office of the General Counsel
afishman@eei.org

Eric T. Ackerman
Director, Alternative Regulation
eackerman@eei.org

Edison Electric Institute
701 Pennsylvania Avenue, NW
Washington, DC 20004-2696
(202) 508-5000

H. Russell Frisby, Jr.
Jonathan P. Trotta
Counsel
STINSON MORRISON HECKER LLP
1150 18th Street, NW, Suite 800
Washington, D.C. 20036-3816
(202) 785-9100
(202) 785-9163 (Fax)
rfrisby@stinson.com
jtrotta@stinson.com

Dated: February 18, 2011