BEFORE THE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
WASHINGTON, D.C. 20230

Developing the Administration's Approach to Consumer Privacy	))))	**Docket No. 180821780-8780-1**

COMMENTS OF THE EDISON ELECTRIC INSTITUTE

The Edison Electric Institute ("EEI") respectfully submits these Comments in support of the Request for Comments ("RFC") issued by the National Telecommunications and Information Administration ("NTIA"), on behalf of the U.S. Department of Commerce ("Department"), requesting comments on ways to advance consumer privacy while protecting prosperity and innovation.[1]

EEI supports an Administration approach to consumer-privacy establishes "user-centric privacy outcomes" and a set of "high-level goals" for consumer-privacy protections."[2] Reducing the current state of patchwork regulation and increasing harmonization and interoperability of the regulatory landscape, nationally and globally, without placing significant additional burdens on businesses should be a key goal for any Federal approach to consumer privacy policy. To this end, any Administration approach to consumer-privacy policy should adopt an outcome- and

[1] NTIA, *Developing the Administration's Approach to Consumer Privacy, Notice and Request for Public Comments*, Docket No. 18821780-8780-1, 83 Fed. Reg. 48600 (September 26, 2018); *See also* NTIA, *Developing the Administration's Approach to Consumer Privacy, Notice, extension of comment period*, 83 Fed Reg. 51449 (October 11, 2018).

[2] *See* RFC, 83 Fed Reg. at 48601. Note that the RFC does not clearly define the term "user-centric privacy outcome."

risk-based approach that provides electric companies with the ability to adopt reasonably flexible privacy protections capable of accommodating varying consumer expectations. A Federal approach to consumer privacy should identify a set of user-centric privacy outcomes, which then underpin the protections that should be produced by any Federal actions on consumer-privacy policy. Such an approach should be non-prescriptive and cost-effective, setting out high-level goals that describe the outlines of the ecosystem that should be created to provide those privacy protections.

EEI is the trade association that represents all U.S. investor-owned electric companies. Its members provide electricity for 220 million Americans and operate in all 50 states and the District of Columbia. The electric power industry supports over seven million jobs in communities across the United States. In addition to its U.S. members, EEI has more than 60 international electric companies, with operations in more than 90 countries, as International Members and hundreds of industry suppliers and related organizations as Associate Members. EEI's members are major users of telecommunications systems to support the goals of clean power, grid modernization and providing customer solutions.[3] For example, electric companies are investing over $100 billion annually in smart grid infrastructure not only to assure the safety, reliability and security of the grid, but also to enhance their ability to provide new individualized services to their customers. At the same time, the public's adoption of electric end-use technologies or "electrification" is increasing.[4]

EEI therefore has a strong interest in any NTIA proposal or recommendations for an

[3] The electric power industry is modernizing the nation's electric grid using advanced technologies to deliver more reliable power to customers across the country and allow two-way communication between customers and their electric companies.

[4] *See gen.*, U.S. National Electrification Assessment, Electric Power Research Institute (2018).

Administration approach protecting the privacy of American consumers, including electricity customers, while also allowing companies to use information about customers to innovate and deliver better products and services to consumers.

BACKGROUND

Protecting customer privacy is an important and well-established priority for EEI's members that have policies in place to protect access to personally identifiable information ("PII") and other customer information. Electric companies make the security and privacy of other customer data a key component of their grid modernization efforts. EEI's members are thus committed to protecting customer privacy and work diligently to ensure that policies and procedures address new and emerging privacy issues.

Electric companies have a long history of protecting the privacy of customer data and respecting the civil liberties of their customers in a highly regulated environment. Electric companies often store PII, such as Social Security numbers[5] and financial account numbers, in their payroll or billing systems and have been obligated to follow the associated legal requirements for safeguarding this type of data for many years. Traditionally, privacy regulation of customer data has been the responsibility of the states, which have developed various privacy protection laws for customer data. States also have consumer protection laws safeguarding interests of energy consumers. Under these and similar laws, information is furnished directly from consumers to electric companies in confidence, and it is well established that the public interest requires maintaining the privacy of that information. For example, some states have legislation that covers utility data privacy collection and third-party use policies. Many states

[5] EEI understands that many electric companies are moving away from using Social Security numbers to using different methods to identify customers that present less risk of identity theft and protect their customers' privacy.

also use more generally applicable laws to address data privacy issues associated with electric companies' protection of consumer-privacy. In addition to state laws, electric companies comply with the data privacy guidelines and regulations set by state public utility commissions ("PUCs").[6] Thus, electric companies typically operate in a context where different state authorities may be relevant when fulfilling consumer-privacy obligations.[7]

Given that the electric industry is complex and EEI's members face varying state regulatory requirements, electric companies have implemented consumer-privacy practices on a company-by-company basis as opposed to a uniform nationwide basis. Electric companies therefore have their own data privacy policies in accordance with regulations promulgated by state regulatory authorities. Because of technology developments, the electric industry in recent years has had to revisit industry privacy practices; as a result, the industry has developed even stronger privacy practices. The electric industry also has worked with Federal and state officials, (including the National Institute of Standards & Technology), as well as other stakeholders, to refine and improve its privacy practices. As a result, electric companies typically have policies to protect customer data and will have processes in place to update these policies as needed based on evolving customer needs, regulatory requirements, internal assessments, benchmarking, etc.

[6] For example, PUCs in states such as California, Pennsylvania and Texas have required consumer consent before electric companies can release customer information to a third-party even in absence of electric company-specific legislation.

[7] For example, the Michigan Public Service Commission rules govern electric and gas utilities generally in addition to Michigan's identity theft protection Act and Social Security Number Privacy Act.

COMMENTS

A. An Administration approach to consumer-privacy should be outcome- and risk-based

The Administration should adopt an approach to consumer-privacy that establishes how to best achieve user-centric privacy outcomes in a manner that is both flexible and clear, which will serve as a set of inputs for companies to build better privacy protections into products and services. Using an outcome- and risk-based approach would allow electric companies to tailor the collection, use, storage and sharing of PII[8] and other customer data in a way that is reasonable and appropriate in the context of an already heavily regulated sector. Companies that collect and use small amounts of non-sensitive consumer data should not have to devote the same level of resources to implementing privacy programs as companies that collect vast amounts of consumer data, collect data of a sensitive nature or engage in the business of selling consumer data.

B. Privacy outcomes should not be prescriptive

The Administration should avoid overly prescriptive approaches to protecting privacy that can result in compliance checklists that impede innovative privacy solutions. Principle-based approaches to privacy that dictate both the "how" and the "what" tend to result in complicated, legal style, regulator-focused privacy policies. The better alternative is to limit the focus to the outcomes of organizational practices (the "what") instead of prescribing specific practices (the "how") that reduce a company's flexibility to achieve these outcomes. Any

[8] NTIA should consider proposing one nationwide definition for PII that harmonizes definitions in sectoral laws such as the Health Insurance Portability and Accountability Act.

approach to consumer-privacy policy should intentionally define concepts and principles in a non-prescriptive manner. This is important because electric companies vary tremendously in terms of size, market or service territory, demographics, ownership structure, regulatory environment, etc. Any approach to consumer-privacy policy should give electric companies discretion in how to best implement privacy policies within the context of their circumstances.

C. Any approach to consumer-privacy should promote cost-efficiency

In the context of a heavily regulated industry, cost-efficiency is an important concern for electric companies, customers and state regulators. Privacy, customer data access, and market access and innovation are important values that must not only be balanced among themselves, but also weighed against the costs of various options for realizing concepts and principles. An approach to consumer-privacy should afford electric companies the appropriate flexibility to tailor practices to appropriately protect consumers' privacy interests in a cost-efficient manner.

D. EEI supports a principled-based approach to privacy that establishes reasonable privacy outcomes

Below, EEI provides comments on the RFC's proposals for certain "user-centric" privacy outcomes:

1. Transparency and clarity

For customers to make informed and meaningful choices, transparency and clarity of an electric company's consumer data policy and practices are essential.[9] Transparency without clarity does not help the customer understand how an electric utility collects, stores and shares their PII or other customer information to form the basis for informed consent, but clarity and

[9] *See* RFC, 83 Fed. Reg. at 48601.

transparency can be enabled by various means. A Federal approach to consumer-privacy should encourage companies to consider how the average customer interacts with a product or service in determining a reasonable way to convey information about privacy to customers.

2. Control

Customer control over collection, use, storage, and disclosure of their PII should depend on the "business context" of electric service and controls should be made available in ways that allow users to exercise informed decision-making in that context.[10] A Federal approach to consumer-privacy should provide customers with the ability to exercise reasonable control of the collection, use, storage and disclosure of the PII and other customer information. Which controls an electric company should offer, when to offer them, and how they are offered should (i) depend on the electric company's use and the sensitivity of the information, and (ii) should be developed after considering ease of use, affordability and accessibility. Electric companies should also have reasonable flexibility in the controls used to withdraw the consent or limit activity previously permitted by a customer so long as they are as readily accessible and usable as the controls used to permit the activity.

3. Reasonable minimization of risk

Electric companies should have reasonable flexibility to determine which means to use to reduce the risk of privacy harm.[11] Data collection, storage length, use and sharing should be minimized in a reasonable manner consistent with the relevant context of the electric business and the risk of privacy harm. Reasonable data collection, storage, and sharing practices also

[10] *See* RFC, 83 Fed. Reg. at 48601.

[11] *Id.*

support good security practices in the electric industry. Similarly, electric companies should have flexibility to implement reasonable and appropriate data retention periods.

4. Security

Maintaining data security is critical to avoiding harm to consumers, negative publicity for businesses and law enforcement action.[12] Consequently, electric companies that maintain information about consumers should employ reasonable safeguards to protect that information. Electric companies also should use reasonable security measures commensurate with the level of risk associated with their practices including collection, computation, storage, and transfer of raw and processed data. Further, the level of security required should depend on the sensitivity of the data, the intended use of the data, the size and nature of an electric company's business operation, and the types of risks an electric company faces.

5. Access and correction

Any Federal approach to access to and correction of consumer data must recognize that there are both cost and benefits to allowing consumers to access and correct a company's data.[13] Electric companies should take reasonable steps to ensure the accuracy of the data they collect in view of the sensitivity of data and its intended use. Electric company customers similarly should have reasonable access to PII or other customer data to have opportunity to correct it in view of the context and risk of privacy harm.

6. Risk management

Electric companies typically implement monitoring and compliance programs, consistent

[12] *See* RFC, 83 Fed. Reg. at 48601.

[13] *See* RFC, 83 Fed. Reg. at 48602.

with applicable regulatory requirements, to ensure compliance with data policies. Electric companies also typically assign privacy responsibilities to appropriate personnel with sufficient authority to ensure that (i) internal awareness activities are conducted and (ii) data policies are documented, adhered to and updated from time to time as needed.

A Federal consumer-privacy policy should adopt a risk management-based, approach to ensuring privacy outcomes by which companies take reasonable steps to manage and/or mitigate risk of disclosure or other harmful uses or exposure of PII and other customer information.[14] Within the context of their business model, companies should have some reasonable flexibility to develop or maintain reasonable risk management programs that include privacy.

7. Accountability

Companies that handle PII and other customer data should be held accountable for appropriately collecting and safeguarding such data.[15] Companies that manage customer information should have flexibility to create accountability that is consistent with their own policies and practices for the use of customer information collected, maintained, and used in their systems. Given customers' interest in privacy, third-party service providers must be subject to similar obligations to ensure consistency in privacy protections for this information.

E. EEI supports an Administration approach to privacy that establishes reasonable privacy outcomes high-level goals for Federal action

EEI appreciates that the Administration is seeking feedback on the high-level goals outlined in the RFC and should establish high-level goals for potential future Federal action on

[14] *See* RFC, 83 Fed. Reg. at 48602.

[15] *Id.*

customer privacy.[16] Among the goals described in the RFC, the most important is harmonizing the regulatory landscape for consumer-privacy protection so as not to create duplicative or inconsistent requirements for companies to implement. The RFC is correct that a patchwork of competing and contradictory baseline Federal laws and regulations does not serve the economy or provide a structure for improving the privacy outcomes for customers.[17] Ultimately, this situation makes it more difficult for electric companies to protect consumer-privacy and does not serve the customer. The regulatory environment for consumer-privacy protection should therefore be balanced to be flexible, strong, predictable, and harmonized. Proposed goals or Federal actions either should not conflict with current State regulations or should supersede them.

Improving legal clarity helps provide businesses with the regulatory certainty needed to better plan and implement policies, including consumer-privacy protection programs.[18] In seeking to improve legal clarity, the Administration should avoid overly prescriptive approaches in favor of providing businesses the flexibility to innovate using a variety of methods to achieve consumer-privacy outcomes. To strike this balance of interests, the key for the Administration is to adopt a risk and outcome-based approach to consumer-privacy.

One-size-fits-all methodologies do not work well for businesses like electric companies that have tangible differences in assets and workforce and operate in differing regulatory environments. Overly prescriptive requirements would inappropriately limit flexibility to innovate. Instead, the Administration should seek to create more clarity and consistent

[16] *See* RFC, 83 Fed. Reg. at 48602.

[17] *Id.*

[18] *Id.*

application of consumer-privacy outcomes between similarly-situated organizations that would enable data practices in similar contexts to be treated comparably. With such an approach, it makes sense to address consumer-privacy comprehensively for all private sector organizations that collect, store, or share personal data to the extent these activities are not covered by sectoral laws.[19]

Electric companies, as owners and operators of transmission and distribution, must comply with enforceable reliability standards that are generally outcome- and risk-based. This has provided experience with implementing such regulatory requirements that address cybersecurity and reliability. Electric companies, as public utilities, must balance business needs, consumer and regulator expectations, legal obligations and potential privacy harms, among other factors, to evaluate how to approach consumer-privacy. A risk-based approach to consumer-privacy would allow electric companies to consider what customer information must be secured and give the business the discretion to determine how best to secure that information and how to document and audit compliance.

The RFC is correct that governments of different nations will approach privacy differently.[20] With respect to interoperability, it makes sense that the Federal government would seek to develop a regulatory landscape that is "consistent" with international norms and frameworks in which the U.S. participates, but the Federal government should not subject U.S. businesses to international laws or requirements for consumer-privacy.[21]

[19] *See* RFC, 83 Fed. Reg. at 48602.

[20] *Id.*

[21] *Id.*

Finally, EEI agrees that just as organizations should employ outcome- and risk-based approaches when developing privacy protections for their customers, the government should do the same with its approach to privacy enforcement. The RFC recognizes that some businesses collect little PII and do not maintain sensitive customer information about their customers and likewise that there is a valid distinction between organizations that control PII and third-party vendors that may process that data on behalf of other organizations.[22] As a result, an outcome- and risk-based approach will be easier for the Federal government to develop and implement across the many, different business sectors.

CONCLUSION

EEI respectfully requests that NTIA consider these comments and ensure that any recommendations regarding consumer-privacy is consistent with them.

Respectfully submitted,
EDISON ELECTRIC INSTITUTE

/s/ Aryeh B. Fishman
Aryeh B. Fishman
Associate General Counsel, Regulatory Legal Affairs
Edison Electric Institute
Washington, D.C. 20004
(202) 508-5023

Dated: November 9, 2018

[22] *See* RFC, 83 Fed. Reg. at 48602.