STATE OF NORTH CAROLINA
UTILITIES COMMISSION
RALEIGH
DOCKET NO. E-100, SUB 161

BEFORE THE NORTH CAROLINA UTILITIES COMMISSION

In the Matter of	)	ATTORNEY GENERAL'S OFFICE
Commission Rules Related to Electric	)	PROPOSED RULE R8-51 AND
Customer Billing Data	)	INITIAL COMMENTS

The North Carolina Attorney General's Office ("AGO") respectfully submits these initial comments regarding the AGO's Proposed Rule R8-51, "Customer and Third Party Data Access and Privacy," which is attached here as Appendix A (hereinafter, the "AGO Proposed Rule"). This proceeding was initiated to create rules that would provide customers or an authorized third party access to customer data while protecting the privacy and security of those data. These Initial Comments explain the need for a rule comprehensively dealing with data access and privacy and provide a draft of such a rule.

The AGO and other parties have exchanged drafts of proposed rules. The AGO makes a separate proposal because it is important to develop a rule that both allows access to customer data and protects the privacy of the data. In the AGO Proposed Rule, the AGO incorporated the substantive provisions of draft rules prepared by other parties regarding access and aggregation of data, then placed those provisions within the privacy framework necessary to protect North Carolina consumers.

Procedural History

In prior dockets and proceedings, the Commission has repeatedly indicated its interest in potential rulemaking regarding data access and data privacy. See 2016 Smart Grid Technology Plans Order at 23 (March 29, 2017) (recognizing "customer

privacy" among the factors that stakeholders must consider for "rule changes to provide easy access to granular energy consumption data") (emphasis added). See also Order Approving Manually Read Meter Rider with Modifications and Requesting Meter-Related Information, Docket No. E-100, Sub 1115, Sub 147 and Sub 153 at 15 (June 22, 2018) (requiring, in response to public comments that smart meters could "represent an invasion of [customers'] privacy," that DEC annually file "a verified statement . . . providing a comprehensive list of all the ways DEC is using customer-related smart meter data, and the procedures DEC uses to keep that data secure and to protect customer privacy") (emphases added).

Most recently, in the February 2019 order that initiated this proceeding, the Commission quoted with approval language from the Public Staff about the

> need for rule-making to create rules that would provide customers or a third party with customer permission appropriate access to customer data, while protecting customers and their personal and energy consumption data.

Order Requiring Information, Requesting Comments and Initiating Rulemaking, Docket E-100, Sub 153, Sub 157 and Sub 161 (Feb. 4, 2019) at 3 (hereinafter, the "Order Initiating Rulemaking") (emphasis added). The Commission also quoted the Public Staff's recommendation that the proposed rulemaking not only establish data access, but also data protections: the rules should

> establish a definition of "customer data," who should have access to that data, how access should be granted, customer data protections, liability for parties who breach the confidentiality of data, and who pays for the access. . . .

Id. The Commission and Public Staff suggested that because of "the deployment of smart meters and a new customer information and billing platform, a greater emphasis on customer data regulation is necessary." Id. The order suggested that the rule that

emerges from this proceeding should "ensure that customers understand . . . how their data is used and made available to third parties, and who will be responsible for the integrity and security of that data." Id.

The Commission granted the Public Staff's request to initiate rule-making regarding customer data issues, but declined to address those issues within the ambit of Sub 153 because the cited issues implicated policies and parties well beyond the scope of that rule-making. The Commission instead initiated Sub 161 as a separate docket for the consideration of the noted issues and related rule-making. Id. at 3-4. See also Order Accepting Smart Grid Technology Plans and Requiring Additional Information, Docket No. E-100, Sub 157 (July 22, 2019) at 8-9 (noting with approval Public Staff comment that 2018 conversations with DEC, DEP and DENC "highlighted the need for a better framework to address . . . a rulemaking to establish rules regarding data ownership, access to the data, security and privacy, and costs") (emphasis added). In accordance with the Order Initiating Rulemaking, proposed rules and comments were due April 15, 2019. Pursuant to further Commission orders, the deadline has been extended to February 10, 2020.

The Attorney General respectfully submits for the Commission's consideration the attached AGO Proposed Rule R8-51 dealing with customer access and data privacy. The AGO is not submitting its own versions of proposed Rules R8-7 and R8-8. The AGO is substantially in agreement with the Public Staff's draft versions of those rules most recently reviewed by this office.

Comments

The AGO Proposed Rule is designed to facilitate customer and authorized third-party access to customer usage data generated by smart meters, while simultaneously providing privacy and security protections for that access. The Attorney General's proposal incorporates aspects of the Public Staff's proposed rule regarding access[1] and the treatment of aggregated data. The Attorney General's proposal places those provisions within the privacy and security framework necessary to protect North Carolina consumers.

In short, the AGO Proposed Rule gives customers the choice to have their data be shared with third parties, while requiring that any third-party data sharing be limited to a specific, stated purpose and use. See AGO Proposed Rule (Appendix A to these comments) § (e), (f). The proposed rule allows utilities to use customer data to provide regulated utility service, but it requires utilities to get the customer's consent before using or sharing customers' data for any other purpose. See id. § (d).

Providing options for customers and authorized third parties to access customer usage data will enable customers to employ cost saving measures and energy efficiency programs. The AGO Proposed Rule outlines processes by which customers can access their own data or, working with their utility, securely authorize a third party to access or receive those data.

[1] While the parties generally refer to this rule as one authorizing access, the rule drafts submitted by the parties in this matter more accurately provide for both access and portability. Access pertains to a customer's right to obtain his or her own information. Portability refers to a customer's ability to have his or her data shared by a utility with an authorized third party.

This access should be permitted under processes that preserve not only the security of customer information, but also customers' privacy. This is because of the highly granular nature of the data collected and communicated by smart grid technology and the sheer quantity of those data, often collected as frequently as every 15 minutes. The AGO Proposed Rule incorporates and is organized according to the globally recognized Fair Information Practices (FIPs), privacy principles that inform most of the privacy laws and regulations in the United States and the European Union. See pp.11-13 infra.

As these comments will illustrate, providing access in the context of privacy and security is the approach supported by numerous federal agencies, federal standards bodies, and industry groups, including the Department of Energy, the Department of Commerce, the Federal Trade Commission, and the National Institute for Standards and Technology. Moreover, analogous federal legislation demonstrates the need for privacy protections to accompany data access, disclosure and portability. In the health context, the Health Insurance Portability and Accountability Act (HIPAA) enables data sharing but protects privacy. In the financial industry, the Gramm-Leach-Bliley Act does the same. The AGO Proposed Rule is also informed by the treatment of access and privacy in the context of utilities' adoption of smart grid technologies in Colorado, Michigan and California. Finally, the lack of existing privacy legislation pertaining to smart meter data at both the federal and state levels magnifies the need for the Commission to adequately protect privacy in a rule designed to promote data disclosure.

In drafting this rule, the AGO reviewed and incorporated substantive aspects of the provisions proposed by the Public Staff and collaborated with Mission:data, NCSEA and other entities interested in access. The AGO also sought input on its proposed rule from the Public Staff, Duke Energy, and Dominion.

The AGO's comments are divided into four sections. Section I explains how broad access to smart meter data can create privacy risks for consumers. See pp. 6-10 infra. Section II discusses approaches to these risks taken by federal agencies, industry groups, and other states. See pp. 11-19 infra. Section III illustrates the gaps in the current system that can leave customers' data at risk unless this Commission pairs access with privacy protections in this proceeding. See pp. 19-26 infra. Finally, Section IV discusses how the AGO Proposed Rule pairs access with privacy protection. See pp. 27-30 infra.

I. The Privacy Implications of Smart Meter Data

Utilities using smart grid technologies collect two types of customer data: personally identifiable information (usually associated with accounts—address, name, date of birth, social security number, etc.) and consumer-specific energy usage data generated by smart meters. Privacy concerns arise when energy "usage information is linked with personal details of consumers, households or businesses." Constance Douris, Balancing Smart Grid Data and Consumer Privacy, Lexington Institute (2017) at 6.[2] The granularity of the data collected by smart meters, the quantity of the data

[2] This article is available at www.lexingtoninstitute.org/wp-content/uploads/2017/07/Lexington_Smart_Grid_Data_Privacy-2017.pdf. Douris provides guidance for states allowing data access by analyzing and comparing state data-access policies and the federal principles in the DataGuard Energy Data Privacy Program.

collected, and the collection frequency for the data (every 15 minutes in some cases), pose substantial risks to individual privacy. At the very least, these data "may enable the persistent monitoring of individual electricity usage patterns and appliance use."[3] Dana Rosenfeld and Sharon Kim Schiavetti, Third Party Smart Meter Analytics: The FTC's Next Enforcement Target?, Antitrust Source (Oct. 2012) at 3 (hereinafter "Rosenfeld & Schiavetti").[4]

> But smart meter data may also reveal
>
> > . . . a consumer's behavioral patterns, habits and activities taking place inside the home, including activities like sleeping, eating, showering and watching TV. Energy use patterns over time may reveal the number of occupants in the household, work schedules, sleeping habits, health, affluence or other lifestyle details and habits.

Id. (footnotes omitted). The data may also show when people are not at home, daily schedules, the presence of alarm systems, the use of medical devices, condition, age and use of appliances, and more. Congressional Research Service, Smart Meter Data: Privacy and Cybersecurity (Feb. 3, 2012) at 3-6, available at fas.org/sgp/crs/misc/R42338.pdf.[5]

---

[3] Appliances have "load signatures" that allow them to be identified with particularity from smart grid meter data. Congressional Research Service, Smart Meter Data: Privacy and Cybersecurity (Feb. 3, 2012) at 4-5, available at fas.org/sgp/crs/misc/R42338.pdf.

[4] The Rosenfeld & Schiavetti article was originally published in the American Bar Association's Antitrust Source periodical. An authorized reproduction of the article is freely available at www.kelleydrye.com/getattachment/b861d210-ea64-4254-9b93-2dcc77f65560/attachment.aspx.

[5] For further discussion of the risks associated with the collection and use of smart meter data, see National Institute of Standards & Technology, Interagency Report: Guidelines for Smart Grid Cybersecurity, NISTIR 7628, rev. 1, vol. 2, § 5.11, "Emerging Smart Grid Privacy Risks" (Sept. 2014), available at nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

Privacy issues arise in the collection, transmission, use, disclosure, and retention of customers' energy usage data and other personal information. The usage data are valuable because they are highly granular and consumer-specific, and because they may feature both real-time and historical information. Utilities and other entities that have access to such usage data could elect to sell or share the data or to use the data in ways not required to provide electricity.

When considering access to and use of smart meter data, the actions of the following parties need to be considered: utilities, utility affiliates, entities that contract directly with utilities to provide services, the Commission, law enforcement,[6] customers, authorized third parties, and other third parties.[7] Some third parties may seek to obtain data directly from utilities when authorized by customers, or third parties may obtain smart meter data directly from customers when utilities have provided customers access. Different privacy concerns arise in each of these situations. While the Commission does not have jurisdiction over all of these entities, a properly structured access and privacy rule can help prohibit unauthorized access to energy usage data and other customer information entrusted to or held by utilities.

[6] The AGO Proposed Rule does not address the issues raised by access to customer energy usage data for law enforcement or national security purposes.

[7] Other third parties could include advertisers, applications, insurance companies, data brokers, landlords, hackers, and criminals. These other third parties may use the data for secondary purposes unknown to and unauthorized by customers. While the AGO Proposed Rule does not purport to deal with these types of third parties, the privacy and security protections provided in the Proposed Rule will help minimize unauthorized disclosure and minimize general risks to customer data posed by many of these parties.

In this context, public interests include:

- Helping a customer control and access her data;
- Protecting a customer's ability to know and understand how—and for what purposes—data about her are used;
- Creating clear rules about permissible and impermissible disclosure and sharing of customer data;
- Creating clear rules about how personal data may be used in aggregated, anonymized sets of data;
- Preventing monetization of personal data; and
- Ensuring security for those data.

Therefore, the AGO suggests that any rule governing data access and portability should be accompanied by privacy guidelines that:

- Establish standards to protect the privacy and security of energy usage data and customer information;
- Clearly define and limit both authorized and unauthorized access to and use of personal data; and
- Permit customers to understand the privacy risks posed by smart meter data and the various obligations (or lack thereof) of the different parties who can access those data.

These principles are the foundation of the AGO Proposed Rule. The proposed rule allows customers to access their data generated by smart meters—or authorize a third party to access those data—by a process and under guidelines designed to

protect the privacy and security of customers' personal information.[8] See AGO Proposed Rule § (e), (f). The proposed rule identifies information that utilities are not permitted to share, as well as the data utilities may disclose and the circumstances under which they may do so. Id. § (a)(9), (d). Utilities do not need to obtain customer consent to share or disclose customer data with contractors in order to provide regulated utility service—what the rule calls "primary purposes." Id. § (a)(6), (d)(1), (d)(3), (d)(4)(ii). However, the proposed rule does require utilities to obtain customer consent to use customer data for any purpose other than providing utility service—what the rule calls "secondary purposes." Id. § (a)(7), (d)(6). Utilities also must obtain customer consent before sharing customer data with third parties for secondary purposes. Id. The proposed rule sets standards for the notice that utilities must provide to consumers about the use, disclosure and protection of their information; these standards are designed to illuminate the access process. Id. § (b)-(c). Finally, the proposed rule permits the use of aggregated data that has been sufficiently de-identified to protect consumers' personally identifiable information. Id. § (a)(1), (j). Section IV of these comments describes the provisions of the AGO Proposed Rule in more detail.

[8] The privacy and security risks associated with the collection, use, disclosure and portability of smart meter data will escalate as smart meter use rises and as Internet of Things and Home Area Network (HAN) devices and applications proliferate.

II. Federal and Industry Guidelines, Utility Commission Action in Sister States, and the Interests of North Carolina Consumers Support the Provision of Access within a Privacy Framework

A. Federal Guidance Supports Incorporation of Privacy Protections

The foundational principles for modern privacy regulation are the Fair Information Practices, or "FIPs."[9] The FIPs establish a core set of rights and obligations associated with the transfer and use of personal information. Solove and Schwartz, Information Privacy Law 664 (6th ed. 2018). The FIPs, as articulated in the OECD Guidelines, establish eight key principles for the protection of personal information: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[10] Countries around the world rely on these principles in crafting data privacy rules and regulations.

A variety of federal and national standards and guidelines recommend or support the use of the FIPs to govern the collection and use of data generated by

---

[9] The Fair Information Practices, also referred to as the Fair Information Practice Principles, were originally set out in a 1973 report issued by the United States Department of Health, Education and Welfare. See Ware, Records, Computers and the Rights of Citizens (Aug. 1973) at 4 (describing initial development of the FIPs), available at www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf. In September 1980, the Organisation for Economic Cooperation and Development (OECD) promulgated guidelines drawing on the FIPs. See OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, "Part Two, Basic Principles of National Application," available at www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. The FIPs, particularly as articulated by the OECD Guidelines, have informed the development of information privacy law and policy globally.

[10] The AGO Proposed Rule is organized around these concepts in the following order: transparency or notice (openness principle); purpose specification; use and disclosure limitations; access and control (individual participation principle); data minimization (a reflection of the collection limitation principle); data quality and integrity; data security; and accountability and auditing.

smart meters and to guide third party access to customer usage information. These standards and guidelines include:

- The U.S. Department of Energy's 2010 report entitled Data Access and Privacy Issues Related to Smart Grid Technologies (hereinafter, the "DOE Report").[11]
- The Guidelines for Smart Grid Cybersecurity developed in 2014 by the National Institute of Standards and Technology ("NIST") within the U.S. Department of Commerce (hereinafter, the "NIST Report"). Volume 2 of the NIST Report pertains to privacy and the smart grid.[12]
- The Voluntary Code of Conduct facilitated by the U.S. Department of Energy in coordination with the Federal Smart Grid Task Force in 2015, branded as "DataGuard." DataGuard is the nation's first energy data privacy program.[13]

Each of these resources recommends the implementation of the FIPs' core privacy protections in the collection, use and disclosure of smart meter data.

---

[11] U.S. Department of Energy, Data Access and Privacy Issues Related to Smart Grid Technologies (Oct. 5, 2010), available at www.energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf.

[12] National Institute of Standards & Technology, Interagency Report: Guidelines for Smart Grid Cybersecurity, NISTIR 7628, rev. 1, vol. 2 (Sept. 2014), available at nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

[13] The DataGuard terms are available at www.dataguardprivacyprogram.org/downloads/DataGuard_VCC_Concepts_and_Principles_2015_01_08_FINAL.pdf. DataGuard provides companies with a way to show their commitment to protecting customer energy usage data. "With Data Guard, a utility or third-party energy services company commits to a Voluntary Code of Conduct (VCC). If a company violates the VCC, it could be subject to an action for misrepresentation under section 5 of the Federal Trade Commission Act or state law." Advanced Energy Economy, Access to Data: Bringing the Electricity Grid into the Information Age (April 9, 2018) at 11, available at https://info.aee.net/hubfs/Access%20to%20Data_FINAL_4.9.18.pdf.

The Department of Energy clearly identified the interrelationship of access and privacy in its 2010 report:

> DOE believes that privacy and access, in the context of a Smart Grid, are complementary values rather than conflicting goals. The practical impact of a Smart Grid depends on its capacity to encourage and accommodate innovation while making usage data available to consumers and appropriate entities and respecting consumers' reasonable interests in choosing how to balance the benefits of access against the protection of personal privacy and security.

DOE Report at 2. Both the DOE and NIST "recommend that utilities and state agencies implement comprehensive privacy and data security measures to protect [customer-specific energy usage data] made available through smart meters." Rosenfeld and Schiavetti at 5.[14] The NIST Report's recommended privacy practices for smart grid data obtained by third parties, like the AGO Proposed Rule, are based on the FIPs. See NIST Report § 5.7 at 57 (providing a concise overview of NIST's recommendations) and NIST Report Appendix D ("Recommended Privacy Practices for Customer/Consumer Smart Grid Energy Usage Data Obtained Directly by Third Parties").

The National Association of Regulatory Utility Commissioners (NARUC) and industry groups also support adoption of general privacy principles for the smart grid at the state level, especially for access and disclosure. NARUC resolved,

[14] NIST's "August 2010 Guidelines for Smart Grid Cybersecurity . . . concluded that an effective 'full suite of fair information practices protections was necessary to protect consumers against the unauthorized collection and use of [customer energy usage data] by [customer energy usage data] management services.'" Rosenfeld & Schiavetti at 5 (quoting National Institute of Standards & Technology, Interagency Report: Guidelines for Smart Grid Cybersecurity, NISTIR 7628 vol. 2 at 36 (original edition, Aug. 2010), available at nvlpubs.nist.gov/nistpubs/ir/2010/NIST.IR.7628.pdf).

> When considering or implementing smart grid investments, State commissions should review existing privacy policies and, if necessary, adopt or update their policies to ensure that they properly address the concerns created by smart meter data collection and transmission and track national privacy best practices. Commissions should require utilities and any relevant third parties to comply with those policies.

Resolution on Smart Grid Principles (July 20, 2011), available at pubs.naruc.org/pub.cfm?id=53985C3E-2354-D714-51A8-281C62A21700. NARUC also urges that "privacy interests should be given substantial weight when commissions consider claims for access to and use of customers['] information." Resolution Urging the Adoption of General Policy Principles for State Commission Use in Considering the Privacy Implications of the Use of Customer Information (July 26, 2000), available at pubs.naruc.org/pub.cfm?id=539817D5-2354-D714-5129-92FBAA93B6A2. The Edison Electric Institute (EEI), an association of investor-owned utilities and industry associates worldwide, has noted "the key role that states play in the regulation of electric utilities and consumer privacy." EEI Letter to the FTC re "FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (Feb. 28, 2011).[15] See also North American Energy Standards Board (NAESB), Req. 22 "Third Party Access to Smart Meter-based Information," Version 3.2 (July 14, 2017) (reviewed in July 2019 with permission from NAESB).

The FTC's 2012 Privacy Report also emphasizes privacy by design along with choice and transparency. The best practices it describes generally reflect the FIPs

[15] A copy of this letter is available at www.ftc.gov/sites/default/files/documents/public_comments/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00418-58062.pdf.

and the privacy guidance included in the foregoing documents. Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change (2012) (applicable to "all commercial entities [including investor-owned utilities] that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties"). The Federal Trade Commission has jurisdiction over investor-owned utilities. See Congressional Research Service, Smart Meter Data: Privacy and Cybersecurity at 29.

Incorporating privacy protections into a rule designed to promote access and portability will also reflect the approach taken by Congress. The proposed rules for access in Sub 161 fundamentally enable data access and portability. Historically, when a law or regulation enables the disclosure or sharing of information, Congress has also required rules to protect privacy. Consider both the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act. These laws were passed to enable information sharing in the health insurance and financial industries respectively. Both also have explicit provisions and rules designed to protect the privacy and security of information in the permitted disclosure and sharing.[16] Likewise, utilities' existing ability to share information, as well as rules enhancing sharing and portability, should be supported by privacy and security provisions.

[16] For more information about the privacy rules associated with these statutory schemes, see the HIPAA Privacy Rule, www.hhs.gov/hipaa/for-professionals/privacy/index.html, and the Gramm-Leach-Bliley Privacy Rule, www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm.

B. Smart Meter Data Experience in Sister States

1. California

While many states lack legal guidelines for smart meter data access,[17] other states have regulated privacy along with access in utilities' collection, use and disclosure of smart meter data. In a 2011 decision, the California Public Utilities Commission (CPUC) established the first rules to protect the privacy and security of the electricity usage data of California residents. Cal. Pub. Util. Comm'n, Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Elec. Co., S. Cal. Edison Co., and San Diego Gas & Elec. Co., No. 11-07-056 (July 28, 2011) at 163, available at docs.cpuc.ca.gov/published/Final_decision/140369.htm#P1315_289017 (enacting rules).[18] The CPUC undertook the rule-making on its own motion to actively guide policy in California's development of a smart grid system. During its rule-making process, the Commission heard comments from a wide variety of stakeholders, including electric and gas companies, communications companies, privacy advocates, and energy efficiency groups. The Center for Democracy and Technology, a nonprofit based in Washington, D.C. with extensive privacy expertise, provided substantial guidance for the Commission, providing a proposed rule that attempted to operationalize the FIPs. The Commission modified the proposed rule somewhat based on extensive input by the stakeholders. Since that time, California has approved minor modifications to the rules

[17] NIST Report at 21 ("Privacy subgroup research indicates that, in general, many state utility commissions currently lack formal privacy policies or standards related to the smart grid.")

[18] California's rules are Attachment D to this decision and are available at docs.cpuc.ca.gov/publishedDocs/published/Graphics/140370.PDF.

allowing click-through authorization and has dropped pen and ink signature requirements for customer authorization.[19] The AGO Proposed Rule reflects the process and lessons learned in the California experience.[20]

2. Colorado

The AGO Proposed Rule also draws on the experience of Colorado. The Colorado access and privacy rule has many provisions in common with California, but handles jurisdictional issues in a manner more appropriate to North Carolina by limiting its rule to utilities. 4 Colo. Code Regs. § 723-3 Rules 3025 to 3035, available at www.sos.state.co.us/CCR/GenerateRulePdf.do?ruleVersionId=6403&fileName=4%20CCR%20723-3, and Colo. Pub. Util. Comm'n Decision No. C11-1335 (2011), available at www.sos.state.co.us/CCR/Upload/AGORequest/BasisandPurposeAttachment2010-01028.PDF. Both the California and Colorado rules adopt the primary and secondary purpose distinction featured in the AGO's proposed rule. Compare California Rule 1 and Colorado Rule 3030(a)(ii) to AGO Proposed Rule § (a)(6)-(7), (d)(3) and (d)(6).[21]

3. Michigan

In Michigan, the Public Service Commission entered an Order requiring the regulated electric utilities to file proposed customer data privacy tariffs for gas and

---

[19] See Cal. Pub. Util. Comm'n, Resolution E-4868 (Aug. 24, 2017), available at docs.cpuc.ca.gov/PublishedDocs/Published/G000/M194/K746/194746364.PDF.

[20] Extensive collaboration with Mission:data has allowed the AGO to incorporate recommendations based on Mission:data's considerable experience participating in and observing the implementation of access rules in other states.

[21] For more information on the processes undertaken in California and Colorado, the rules adopted by the utilities commissions in those states, and the distinctions between the two rules, see NIST Report Appendix C ("Changing Regulatory Frameworks") at 63.

electric service. The Commission required the proposals to comport with the privacy framework set out in its Order. That framework took into account the comments that the Center for Democracy and Technology filed in California, as well as comments from the Future of Privacy Forum and from the stakeholders in Michigan, both of which incorporated FIPs. Mich. Pub. Serv. Comm'n, Order in Case No. U-17102, 2013 Mich. PSC Lexis 165, *25-*27, 306 P.U.R. 4th 146 (2013).

4. Ohio

Ohio, a state where Duke Energy operates, considered customer access and privacy issues in 2012. It chose to let national standards develop and to allow a less formal, multi-stakeholder contribution process before taking official action. Pub. Util. Comm'n of Ohio, Finding and Order, Case No. 11-277-GE-UNC (May 9, 2012). Duke Energy indicated in that proceeding that it was appropriate to begin to consider customer access and data privacy protection issues and described specific topics it thought the Commission should study. Id. at 7. Duke suggested the Commission conduct a series of workshops to gain input and then draft proposed rules and guidelines to circulate for comment. Id. at 17.

C. Promoting North Carolina Values and Protecting North Carolina Consumers

Allowing customers to access their energy usage data and authorize third parties to access those data will open opportunities for customers to be more energy-efficient and to save money. In 2019, Governor Roy Cooper issued a Clean Energy Plan for our state. N.C. Governor's Office and N.C. Dep't of Envt'l Quality, North Carolina Clean Energy Plan (hereinafter "Plan"), available at files.nc.gov/ncdeq/climate-change/clean-energy-plan/NC_Clean_Energy_Plan_OCT_2019_.pdf. The

Plan identifies two relevant objectives as part of its effort to modernize the grid to support clean energy sources: (1) "[i]ncreased customer access to their usage data and sources of energy," and (2) "[e]nabl[ing] customers to have greater access to their energy data through new functionalities, such as those available through Green Button['s] "Download My Data" Button." Plan at 83, 129. The AGO Proposed Rule is consistent with the goals and values expressed in that plan, particularly as they relate to customer access to energy usage data.

The AGO also has an obligation to protect North Carolina consumers. Access to and portability of customer data and energy usage information without the requisite privacy protections would place North Carolinians' data at risk. The AGO cannot support a rule that does not include such protections.

III. Existing Federal and State Laws, Utility Privacy Policies, and the Duke Code of Conduct Do Not Adequately Protect the Privacy of Customer Data

A. Federal Law and Privacy Policies

It is especially important for the Commission to adopt a privacy-protective access rule because there are few privacy protections for smart meter data in the current legal environment.[22] Currently, misuse or abuse of consumer smart meter data must be addressed under federal or state unfair and deceptive trade practices authority. Even that authority is limited to whatever protections the utilities or third

[22] Limitations on access to smart meter data that may be posed by the Fourth Amendment are beyond the scope of this rule as currently drafted. See Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018) (Fourth Amendment protects energy consumption data generated by smart meters). This rule also does not address the limitations on access or disclosure to law enforcement that may be posed by the Stored Communications Act, the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act or the Computer Fraud and Abuse Act.

parties see fit to offer in their privacy policies. Further, any enforcement by the AGO or the FTC is ex post, i.e., when a privacy harm has already occurred. One of the goals of the AGO Proposed Rule is to craft a regulatory framework that will prevent disclosure-related harms from happening in the first place.

Moreover, no existing federal privacy law requires utilities to have privacy policies.[23] The utilities in North Carolina do have privacy policies, but the content of those policies is not dictated by federal law and is determined by the utilities themselves.

A general privacy policy drafted by a utility does not sufficiently protect customer data in the context of access and portability. First, if the content of a company's privacy policy is determined by the company without regulatory oversight, the policy will protect the privacy of customer data to whatever degree the utility chooses, and the policy may be changed at any time. Second, a company's privacy policy tends to describe the panoply of ways the company plans to collect, use, and share customer information. The AGO Proposed Rule, on the other hand, imposes certain specific notice and non-disclosure obligations that the utility must follow even when engaging in otherwise permissible disclosure (i.e., primary purpose disclosure or customer-authorized sharing with third parties).

In the United States' privacy law landscape, which is primarily premised on industry self-regulation, consumers typically have few choices and lack both

[23] For purposes of comparison, both the Children's Online Privacy Protection Act and the Gramm-Leach-Bliley Act require covered entities to have privacy policies. No similar federal law requires utilities to have privacy policies or dictates what protections must be offered to consumers.

information and bargaining power when dealing with companies' use of their data. In most cases, even when choices seem illusory—"choosing" to use Google Search, for example, because of the perceived comparative inadequacies of other search engines—there is nevertheless a choice. In the utilities environment, consumers literally do not have a choice. They must get service from the regional provider if they want service at all. In this circumstance, heightened protections for privacy are imperative. It is crucial to ensure that utilities protect the privacy and security of customer data and that any authorized access to those data is permitted in the context of a privacy protective framework. Utilities should be legally prohibited from selling customers' data, and must be prevented from using or disclosing customer data for secondary uses without explicit, affirmative, voluntary customer consent. Customers should not have to rely solely on utilities' good will and promises to protect privacy, particularly in a landscape where the highly granular, comprehensive data that smart meters are generating and utilities are collecting is valuable, voluminous, and increasingly susceptible to monetization. The AGO Proposed Rule protects North Carolina consumers' personal and usage data by prohibiting the sale and unauthorized disclosure of those data and by making sure permissible disclosure happens in a privacy-protective context.

B. State Law

Today, state law incompletely regulates utilities' handling, use, and disclosure of smart meter data, principally covering only a violation of a privacy policy or a data breach. The same is true for third parties' use of customer energy usage data and personal information. North Carolina's unfair and deceptive trade practices law could provide a basis for suit in some contexts, but this cause of action is typically tied to

representations utilities or third parties choose to make in privacy policies. Moreover, this enforcement option is an ex post response to a problem that should be prevented in the first place.

Federal guidelines encourage state utility commissions to take the lead in providing frameworks in which smart meter technology can continue to thrive and specifically encourage access to be permitted in the context of the FIPs. See supra § II.A.

The Commission, as the state agency charged with regulation of utilities, has the authority to require utilities to protect customer data. As the Department of Energy has explained, utilities have protected the privacy of customer data historically, and regulating issues associated with data privacy is a "traditional responsibility of state utility commissions." DOE Report at 3. See N.C. Gen. Stat. §§ 62-30 (granting this Commission with general power and authority to supervise and control public utilities), 62-31 (granting power to administer and enforce reasonable and necessary rules and regulations), 62-32 (granting general supervision over rates charged and service rendered by public utilities and all power necessary to require and compel reasonable service), 62-41 (granting authority to adopt reasonable rules and regulations for the safety of the public as affected by public utilities), and 62-130 (granting authority to establish or allow just and reasonable rates including the compensation and the contracts, rules, or practices affecting the compensation for services offered to the public).

The Commission has exercised its authority to review utilities' privacy practices in previous proceedings, requiring DEC to "include in its Smart Grid Technology Plan

filing . . . a verified statement about its smart meter data privacy procedures," among other items. Order Approving Manually Read Meter Rider with Modifications and Requesting Meter-Related Information, Dockets E-7, Sub 1115, E-100, Sub 147 and E-100, Sub 153 (June 22, 2018) at 16. In that Order, the Commission directed DEC to provide a "comprehensive list of all the ways DEC is using customer-related smart meter data, and the procedures DEC uses to keep that data secure and to protect customer privacy." Id. at 15. In addition, the Commission has repeatedly referenced the need to protect the privacy and security of customer data from emerging smart grid technologies. See discussion supra at 1-3.

C. Duke Energy Code of Conduct

Some of the utilities that would be subject to the AGO Proposed Rule operate under an established Code of Conduct. See, e.g., Order Approving Merger Subject to Regulatory Conditions and Code of Conduct, Docket No. E-2, Sub 1095, No. E-7, Sub 1100, and No. G-9, Sub 682, Appendix A (Sept. 29, 2016). This Duke Code of Conduct primarily regulates the relationships among the Duke family of companies (Duke Energy, DEC, DEP, Piedmont, affiliates and nonpublic utility operations), and it is not a document designed or intended to broadly protect the privacy of customer data.

A few provisions included in the Code of Conduct do touch on covered entities' practices regarding customer data. The Code imposes some guidelines about the affiliates' maintenance of separate books and records and provides some limited direction about the disclosure of customer information. Code of Conduct §§ III.A.1, III.A.2. The section pertaining to disclosure of information primarily provides that customer information can be shared with affiliates under the same terms and conditions as non-affiliates. Section III.A.2(f) details when covered entities are

permitted to disclose a customer's information without the customer's consent. While the majority of these provisions address the sharing of information among the affiliated entities covered by the Code of Conduct, section (f)(1) also permits disclosure of customer information to non-affiliated third parties without consent "to the extent necessary . . . to provide goods or services to DEC, DEP, or Piedmont and upon the written agreement of the . . . non-affiliated third party to protect the confidentiality of such Customer Information."

The AGO Proposed Rule handles this type of disclosure in a way that more thoroughly protects the privacy of customers. The AGO Proposed Rule allows utilities to disclose standard customer data to utility contractors if the contract between the utility and contractor sets out the utility contractors' obligations to protect the data in accordance with the proposed rule's requirements. See AGO Proposed Rule § (d)(4)(ii). Critically, the AGO Proposed Rule also requires customer consent unless a disclosure to a utility contractor is for a "primary purpose": providing regulated utility service. See id. § (a)(6) (defining primary purposes), (a)(7) (defining secondary purposes as any uses that are not for a primary purpose), and (d)(6) (banning disclosures to any party, including contractors, for a secondary purpose). Third parties, including contractors, could be contracted to provide goods or services that are not related to providing utility service. A utility's disclosure of data without consent under the AGO's Proposed Rule is limited to utility contractors, and the disclosed standard customer data can be disclosed and used only for primary purposes. §§ (d)(4)(ii).

Moreover, the definition of "Customer Information" in the Code of Conduct broadly includes "[n]onpublic information or data specific to a Customer or a group of Customers," including a non-exclusive list of data points that have been obtained or compiled by DEC, DEP or Piedmont "in connection with the supplying of Electric Services. . . ." Code of Conduct § I. This broad definition would allow the disclosure of personally identifiable information to third parties that is categorized as "unshareable information" under the AGO Proposed Rule in order to protect customer privacy. See AGO Proposed Rule § (a)(9), (d)(9).

The Code of Conduct also includes a provision describing when the covered entities need customer consent to disclose data and how to go about obtaining consent, Code of Conduct § III.A.2(b), but the scope of this provision is defined by the application of Section III.A.2(f) discussed above. To the extent that section (f) permits disclosure without consent for other than primary purposes, it correspondingly reduces the universe of situations in which consent is required for disclosure under section (b). The Code of Conduct also contains a provision apparently intended to prohibit discrimination requiring the covered entities to offer customers the opportunity to provide data to non-affiliates whenever the customer allows or directs sharing among the covered entities, Section III.A.2(c). Because of the broad definition of "Customer Information," this provision would also lead to sharing that is prohibited under the AGO Proposed Rule. Under the AGO Proposed Rule, "unshareable information" is only ever disclosed to the customer. See AGO Proposed Rule § (d)(9). The remaining provisions about disclosure in Section III of the Code of Conduct pertain largely to interactions between the covered entities and their employees.

Finally, the Code of Conduct also contains a brief provision requiring the disclosure of customer information to third parties on a nondiscriminatory basis. Id. at § III.B.(9) (providing that "[d]isclosure of Customer Information to Duke Energy, another Affiliate, a Nonpublic Utility Operation, or a non-affiliated entity shall be governed by Section II.A.2 of this Code of Conduct").

The Code of Conduct is a document designed primarily to deal with cost and competition issues and, while it makes a good start at protecting the confidentiality of customer information in limited circumstances, it does not mention privacy. Moreover, the Code does not appear (1) to limit a utility's own use of "Customer Information" without consent to primary purposes, (2) to require a utility to obtain consent to use customer information for secondary purposes, or (3) to provide privacy protective provisions or detailed guidance for a utility's disclosure of customer data to third parties.

The AGO Proposed Rule, in contrast, would (1) require utilities to obtain customer consent before they use customers' data for a purpose unrelated to electric service, see AGO Proposed Rule § (d)(6); (2) limit unconsented disclosure to utility contractors who are using the data for a primary purpose and whose use of the data is governed by contractual provisions incorporating the rule's protections, see id. § (d)(4)(ii), and (3) provide a privacy protective framework in which to facilitate consented disclosure to authorized third parties, see id. § (f).

Neither existing federal or state laws, utility privacy policies, nor the Code of Conduct applicable to the Duke entities, adequately protect customer data in the context of customer access and portability.

IV. The AGO Proposed Rule Enables Access in a Manner Designed to Protect Consumer Data

The AGO Proposed Rule allows access in a framework of privacy and security protections, mitigating privacy and security risks and simultaneously creating additional privacy benefits for consumers.

A. Notice to Consumers

The AGO Proposed Rule requires utilities to provide informative notices to their customers that include both general provisions of the type that would typically be included in a privacy policy, see § (b)(5)(i)-(iv), and notice provisions specifically designed to provide a consumer the information she needs to make an informed decision about sharing data with a third party, see § (b)(5)(vii)-(ix), (xi)-(xv). Customers electing to share their data with third parties need to be aware, in particular, of the privacy implications of smart meter data, the risks of disclosure to a third party not regulated by the Commission, and the fact that following transfer, the utility is no longer responsible for the privacy and security of their data. The notice required by the AGO Rule conveys this information and other details pertinent to the issue of access. See § (b)(5)(vii)-(ix).

B. Sharing with Contractors

The AGO Proposed Rule allows a utility to disclose customer data without consent if it is sharing the data with a contractor for a primary purpose. See § (d)(4)(ii). However, the rule also requires that the utility contractually require those parties to protect the privacy of the data to the same or greater extent as the utility itself protects the data. Id. The rule thus facilitates access and disclosure for routine business purposes but protects privacy at the same time. The rule also permits a utility to ask

for consent to use customer data for a secondary purpose should such a need arise, but requires the utility to continue to protect the privacy and security of the data in that context. See § (d)(6), (d)(8)(v).

C. Sharing with Authorized Third Parties

Sharing with an entity that is not providing services to the utility pursuant to a contract raises different privacy concerns. It is important that consumers understand that, when a utility allows an authorized third party to access a customer's data at the customer's request, the utility no longer has the ability or the obligation to protect the privacy or security of those data. The notice provisions of the proposed rule ensure that this and related privacy information will be conveyed to customers authorizing access to their data. See § (b)(5). The use and disclosure limitations authorize access and use, but tie those concepts closely to specification of purpose and limits on use that are consonant with the specified purposes. See § (d)(6) (requiring customer authorization "for each distinct secondary purpose"), (f)(1) (allowing the utility to share data with third parties at the direction of the customer), and (f)(4)(ii) (requiring the customer to specify purpose for this third-party sharing). Requiring the specification of purpose helps make sure all of the parties are on the same page with respect to the intended use for the data.

Moreover, utilities can promote (although not ensure) the protection of the privacy and security of the data after transfer by implementing the proposed rule's eligibility criteria, under which utilities shall require third parties to meet designated technical standards and to comply with the Department of Energy's "DataGuard" Voluntary Code of Conduct or similar national standard. See § (f)(9). Companies that adopt the DataGuard standard agree to use personal data only for the purpose for

which it was obtained, unless they obtain consent for additional uses.[24] Accordingly, a company that obtains consent to access a consumer's data for the purpose of helping the consumer conserve energy should not also sell those data to a data broker without obtaining consent.[25] Indeed, a third party's violation of the Voluntary Code of Conduct after adoption would arguably constitute an unfair or deceptive trade practice under Section 5 of the FTC Act and of NC's Unfair or Deceptive Trade Practices Act, thus providing the consumer with an avenue of redress. See Rosenfeld & Schiavetti at 6.

This is another example of embedding privacy-protective principles into an access process. While the utility will not have the ability or obligation to oversee a third party's compliance with the DataGuard Voluntary Code of Conduct, a utility will have the ability to terminate its relationship with a third party if a violation of the code is brought to its attention. Importantly, the Commission need not have or exercise jurisdiction over any party other than the utilities to enforce this rule.

D. Unshareable Information

The AGO Proposed Rule prohibits the sharing of data classified as "unshareable information" in any context except with the customer. § (a)(9), (d)(9). The Rule promotes access by permitting the sharing of limited information at the

[24] The DataGuard section on customer choice and consent is a specific example of the ways the FIPs are incorporated into customer access provisions. DataGuard Voluntary Code of Conduct, supra note 13, at 7-9.

[25] Here, the Commission arguably does not have the jurisdiction over third parties that would be necessary to support a rule directly imposing requirements on third parties, but incorporation of the eligibility requirements in the AGO Proposed Rule (application of which requires jurisdiction over only the utilities) comes as close as possible to ensuring this level of protection of customer data.

customer's request including account number and billing information, but explicitly protects the privacy of other personally identifiable information. § (a)(8)-(9), (f).

E. Ban on Selling Customer Data

To the AGO's knowledge, North Carolina utilities do not currently sell customer information. To ensure that this practice does not arise in the future, the AGO Proposed Rule provides, "Utilities may not sell information about customers or covered information, other than aggregated data, for consideration of any kind." § (d)(2).

F. Privacy Practices

Finally, the AGO Proposed Rule requires utilities to implement the following privacy practices: data minimization, data quality and integrity, data security, and accountability and auditing. See § (*l*)-(u). The utilities currently incorporate some of these principles into privacy policies they have crafted for their businesses. By incorporating these important privacy practices into a Commission rule, these obligations to protect data, in addition to those requiring notice, purpose specification, and use and disclosure, will be officially recognized guidelines. Because utilities are required under the AGO Proposed Rule to contractually obligate utility contractors to provide at least as much protection for customer data as they do themselves, these practices should also be adopted by utility contractors, providing additional protections for consumers. Each of these practices is based on the FIPs as articulated by the OECD Guidelines and represents a privacy best practice.

The foregoing are just a few illustrations of the manner in which privacy protections entwined with access provisions more effectively protect consumers' interests.

Conclusion

The Attorney General's Office has incorporated substantive aspects of provisions recommended by other parties into a comprehensive access and privacy rule designed to protect North Carolina consumers. This proposal directly responds to the Commission's request that Sub 161 be used to "create rules that would provide customers or a third party with customer permission appropriate access to customer data, while protecting customers and their personal and energy consumption data." Order Initiating Rulemaking at 3.

The Commission and North Carolina consumers will realize the following benefits as a result of the implementation of the AGO Proposed Rule:

1. The rule will establish a baseline set of privacy obligations, minimizing the risks associated with issues of access and portability.
2. The rule's protections will serve to guide companies' practices as smart grid technologies develop and expand, building consumer trust and confidence necessary for the successful adoption of new technologies and innovations to flourish.
3. The rule will enable customer and authorized third-party access to usage data, which promise to promote energy efficiency, conservation, and cost savings for customers within a privacy framework.
4. The rule will be consistent with the Fair Information Practices and national guidance provided by the National Institute of Standards and Technology, the Department of Energy, the Department of Commerce, and the Federal Trade Commission; moreover, it will reflect the primary and secondary purpose

paradigm included in rules adopted by California and Colorado and incorporated in the DataGuard Voluntary Code of Conduct. It will contribute to a uniform regulatory approach that will be preferable for utility companies operating in multiple states.

The AGO respectfully requests that the Commission consider and adopt the AGO's Proposed Rule R8-51. Prior to the Commission's final determination, the AGO respectfully asks that the Commission issue an order that requests reply comments on all parties' proposed rules, grants a period of 30 days to respond, and provides the AGO with an opportunity to reply to comments.

Respectfully submitted this the 10th day of February, 2020.

JOSHUA H. STEIN
ATTORNEY GENERAL

/s/
Jolynn Dellinger
Special Counsel for Privacy Policy & Litigation
N.C. Department of Justice
Post Office Box 629
Raleigh, N.C. 27602-0629
Telephone: (919) 716-6042
Facsimile: (919) 716-6050
jdellinger@ncdoj.gov

/s/
Blake Thomas
Deputy Attorney General
N.C. Department of Justice
Post Office Box 629
Raleigh, N.C. 27602-0629
Telephone: (919) 716-6414
Facsimile: (919) 716-6050
Bthomas@ncdoj.gov

/s/
Margaret A. Force
Assistant Attorney General
N.C. Department of Justice
Post Office Box 629
Raleigh, NC 27602
Telephone: (919) 716-6053
Facsimile: (919) 716-6050
pforce@ncdoj.gov

CERTIFICATE OF SERVICE

The undersigned certifies that she has served a copy of the foregoing ATTORNEY GENERAL'S OFFICE INITIAL COMMENTS ON PROPOSED RULE R8-51 upon the parties of record in this proceeding by email or by depositing a copy of the same in the United States Mail, postage prepaid, this the 10th day of February, 2020.

/s/
Margaret A. Force
Assistant Attorney General