# Smart Meter Global



December 19, 2019

Gregory Kopta
Administrative Law Judge
Washington Utilities and Transportation Commission
P.O. Box 47250 1300 S. Evergreen Park Drive S.W.
Olympia, Washington 98504-7250

Re: Docket U-180525: Response to WUTC Proposed Language for data privacy and security (WAC 480-100, sections 23 and 153)

Thank you for this opportunity to late file comments in Docket U-180525, regarding privacy and data security language proposed in the third mark up. Smart Meter Texas, an initiative of Good Company Associates was created to promote the advancement of secure, permissioned data-sharing as a way to improve utility transparency with respect to activities on the edge of the distribution grid, animate markets for enhanced customer services, stimulate innovation, improve efficiency, and support the integration of new resources. In this role, I've been working with several state commissions and stakeholder groups like the one that has been meeting in Washington, as well as software providers that serve utilities. My brief comments follow:

Regarding WAC 480-100-023

1.) The definition of "Aggregate data" (page 1) conflates the meaning and intention of the rule to address anonymous data, which includes a subset of aggregated data. Anonymous data would be "data from which identifiable information has been removed or modified so that the information cannot be attributed to any individual customer" <u>including through combination with other publicly available data</u>. Many policy, planning, university or marketing research, or performance validation studies require access to anonymized individual account data to have any value. Some states require an NDA from research organizations for anonymized individual data that may pose a greater risk of re-identifying individual customer information.

Another, subcategory of Anonymous data, however, is data sets that have been aggregated sufficiently to make reidentification of individual customer information impossible. There is no need for special handling of truly anonymous, aggregated data sets.

2.) Related to the first point above, the definition of "Customer Information" (page 2) may prove problematic as written. First, the definition should be modified as shown here:

> "Customer Information" means personal, private, or proprietary information that, either alone or in combination with other <u>publicly available</u> information, identifies, describes, or ~~is~~ <u>can</u> otherwise <u>be</u> associated with utility service provided to a specific customer"…etc.

"other information" is simply too broad, given that *any* information in combination with some other information could require protection. The other edits seem required to capture what I think was meant.

Regarding Section WAC 480-100-153

1) I am a little confused by the proposal's definition of third party, or have trouble telling which third party is addressed in different sections, or whether there are two standards for third parties acting as an agent of a utility, and third parties chosen by or acting as an agent of a customer.

So, in paragraph (2) (page 40), a utility must obtain consent from a customer to collect and retain data not strictly needed for the utility to meet its primary purpose. This is a not unreasonable policy.

Then paragraph (3) (page 41) would appear to progress logically to require the same consent be obtained for the utility to collect, retain and share data with an affiliate, subsidiary, or parent organization for purposes other than its primary purpose.

Paragraph (4) begins again addressing purposes other than the utility's primary purpose and appears to expand this consent requirement slightly to include third parties engaged by the utility to provide non-primary services. However, the second sentence refers to "all third parties." In fact, that second sentence requires "all third parties to which it provides access to customer information to have policies, procedures, and technological safeguards in place to protect customer information that are no less stringent than the utility's own standards." This language suggests that the paragraph applies only to third parties acting as agents of the utility itself, because it is such a high standard. It would eliminate a great number of third-party service providers that customers might choose to share their data with.

This interpretation is strengthened by reading paragraph (5) which simply calls for the utility to require third parties have "sufficient" policies, procedures, and technological safeguards. This implies that there are two levels or standard for policies, procedures and technology to protect customer information. Also, note, paragraph (5) again lumps in "affiliates, subsidiaries, and parent organizations," which I thought were to be required to have a higher standard. So, it isn't clear what organizations are being addressed in either (4) or (5), or whether the rule anticipates third-parties chosen or designated by the customer to receive their data from the utility.

Additionally, the term "sufficient" is vague, or encompassing, on the other hand, and invites confusion. Requiring a utility to enforce this by contract will probably lead to overly strict measures to protect the utility's liability.

If this rule is meant to also help set the boundaries for customer data sharing (*a la* Green Button Connect My Data), then perhaps it should clarify the various requirements for the three categories of organizations likely to need access to customer information: 1) affiliates, subsidiaries, and parent organizations, 2) third party providers that are engaged by the utility to serve customers on its behalf, or as an agent of the utility, and 3) third parties that are

designated by the customer, and may be acting as an agent of the customer, and are not an affiliate, subsidiary, or parent, or agent of the utility.

Then the levels of requirement imposed on policy and process and technology imposed would also vary appropriately according to type. Category 1) and 2) organizations would likely expected to reflect the level of standard of the utilities itself, based on your proposal, and category 3) organizations having a lesser expectation for sophistication of policy, process, and technology. We would suggest requiring that category 3) organizations simply be required to accept terms and conditions which include an agreement to use reasonable care and best industry practices to protect the privacy of customer information. New York sidelined all data sharing with unaffiliated third parties for a year or more because such independent companies could not accept the same level of requirement or liability as the utility itself or its agents. At least one state is considering requiring that unaffiliated third parties adopt the US Department of Energy's voluntary DataGuard standard as a way to address practices of non-regulated third parties.

2) Paragraph (8) appropriately limits the liability of the utility if it responsibly releases data at the request of a customer to a class 3) third party. That one-sentence paragraph should end, however:

> "…the utility will not be responsible for the security of that information or its use or misuse, by the customer designated third party."

This modification clarifies the limits of liability and the responsibility of the customer to choose wisely, as with selecting any contractor.

We appreciate the opportunity to provide late-filed input to this docket. Please contact me at (512) 773-6458 for additional information about these comments or matters relating to data privacy or protection policy.

Best regards,

Robert J. King
Smart Meter Global Initiative
1201 Spyglass Drive, Suite 100
Austin, TX 78746
512(773-6458)
rking@smartmeterglobal.com