UNITED STATES DEPARTMENT OF ENERGY (US DOE)
DATA PRIVACY AND THE SMART GRID: A VOLUNTARY CODE OF CONDUCT (VCC)

Draft: ~~***8/12/2014***~~***11/24/14***

MISSION STATEMENT

The purpose of the Privacy Voluntary Code of Conduct, facilitated by the United States Department of Energy's Office of Electricity Delivery and Energy Reliability and the Federal Smart Grid Task Force, is to describe principles for voluntary adoption that:

(1) encourage innovation while appropriately protecting the privacy and confidentiality of Customer Data and providing reliable, affordable electric and energy-related services;

(2) provide customers with appropriate access to their own Customer Data; and

(3) do not infringe on or supersede any law, regulation, or governance by any applicable federal, state, or local regulatory authority.

The VCC's recommendations are intended to apply as high level principles of conduct for both utilities and third parties.

The VCC is intended to be applicable to, and voluntarily adopted by, both utilities and third parties. However, it is envisioned that the VCC could be most beneficial to either entities that are not subject to regulation by applicable regulatory authorities, or entities whose applicable regulatory authorities have not imposed relevant requirements or guidelines.

The intent is for utilities and third parties to consider adopting the VCC in its entirety. However, a utility or third party could ~~potentially~~ adopt the concepts and principles of the VCC with some limited ~~exception,~~ exceptions (such as when laws, regulatory guidance or frameworks, governing documents, policies, and/or ~~prevailing~~consensus-driven state~~/~~, local, or utility industry business practices ~~indicate~~require a different approach~~. In these instances, utilities or third parties~~). Such exceptions, however, should be consistent with the overall purposes of the VCC and should be explicitly ~~note the reason for the deviation(s) and prominently indicate such~~noted and explained in any depiction ~~that they have adopted the~~of VCC adoption, such as in a privacy policy or other notice ~~of adoption~~. Nothing in this VCC is intended to change, modify, or supersede federal, state, or local laws or regulatory guidance.

Overview of the Voluntary Code of Conduct

How the customer learns what he or she needs to know to exercise informed choice. Describes requirements for practices that explain data collection policies and procedures to customers, focusing on customer options and responsibilities.

How the customer controls his or her data and under what limitations. Describes requirements for processes that allow the customer to control access to his or her data for Secondary Purposes (i.e., to authorize differential access to multiple Third Parties, limit the duration of access, keep a record of data releases, rescind authorizations, and dispose or de-identify data once authorization or the need for the data has expired). Identifies data types and disclosures that do not require customer consent. Includes a requirement requiring certain data to be obtained directly from the customer.

How the customer's data is accessed. Describes requirements for procedures that allow customers to access their data, identify possible inaccuracies, and request they be corrected. Includes the potential for fees for non-standard requests.

How customer data is maintained. Describes requirements for a cyber security risk management program, and methodologies for creating Aggregated or Anonymized Data.

How the VCC is followed. Describes requirements for actions by Service Providers who voluntarily adopt the Voluntary Code of Conduct to ensure that they comply with it.

KEY DEFINITIONS

Account Data

The following elements, when identified with a specific customer, are considered to be Account Data:

i. Names

ii. All geographic subdivisions smaller than a state, including street address, city, county, precinct, census block, zip code, and their equivalent geo-codes;

iii. Dates of service provided to a customer by the utility or third party or information specific to identifying an individual's utility service;

iv. Telephone or fax numbers;

v. Electronic mail addresses;

vi. Utility or Third Party Account numbers (excluding financial account numbers, such as credit card numbers, bank account numbers, etc.); and

vii. Device identifiers (e.g., meter numbers, HAN numbers, etc.) and serial numbers.

Aggregated data

Aggregated Data is a combination of data elements for multiple customers to create a data set that is sufficiently anonymous so that it does not reveal the identity of an individual customer.

Anonymized Data

A data set containing individual sets of information where all identifiable characteristics and information, such as, but not limited to, name, address, account number, or social security number, are removed (or scrubbed) so that one cannot reasonably re-identify an individual customer based on, for example, usage, rate class, or location.

Contracted Agent

An entity providing support to a Service Provider in the provision of service to the customer for a Primary Purpose (without consent) or Secondary Purpose (with consent) who: (1) has access to Customer Data; and (2) has contractually assumed obligations comparable to those of the Service Provider to protect and keep confidential Customer Data and to use it only for the identified Primary or Secondary Purpose. To the extent a Contracted Agent wishes to use Customer Data for its own independent Secondary Purpose, it is treated as a Third Party, meaning that it has to receive customer consent to use the data.

Customer Data
The combination of customer energy usage data (CEUD) and Account Data. Customer Data is treated as private and has specific requirements outlined elsewhere in the VCC. CEUD without Account Data is considered anonymous data, which is discussed separately in the VCC, and referred to specifically as "anonymous data." Aggregated CEUD is also discussed separately, and referred to specifically as "aggregated data." Publicly available information about a customer is not treated as private, unless it is combined with other non-public information.

Customer Energy Usage Data (CEUD)
Customer Energy Usage Data reflects an individual customer's measured energy usage but does not identify the customer.

Primary Purpose
The use of Account Data or CEUD that is reasonably expected by the customer: (1) to provide or reliably maintain customer-initiated service; and (2) including compatible uses in features and services to the customer that do not materially change reasonable expectations of customer control and third party data sharing.

Secondary Purpose
The use of Account Data and CEUD that is materially different from the Primary Purpose and is not reasonably expected by the customer relative to the transactions or ongoing services provided to the customer by the Service Provider or their contracted agent.

Service Provider
A Service Provider is an entity that collects Customer Data directly from individuals to support a Primary Purpose. Where the Service Provider is a corporation, this definition includes all legal entities or agents within the corporation's structure that are involved in fulfilling that Primary Purpose.

Third Party
An entity requesting access to Customer Data from a Service Provider for a Secondary Purpose.

The VCC is expressed through five core concepts, as follows.

1.0 CUSTOMER NOTICE & AWARENESS - The concept that customers should be given notice about privacy-related policies and practices as part of providing service. Service Providers should provide materials in various formats that are easily understandable by the demographics they serve, and as may be reasonably appropriate. Notice should be given at the start of service, on some reoccurring basis (e.g., annually) thereafter, and at the customer's request. Notice also should be given when there is a substantial change in procedure or ownership that may impact customer data. ~~Notice should address the following:~~This could include, for example, timing disclosures to coincide with the time and place that customers have the ability to exercise choices (e.g., push notifications for software downloads) regarding the use of their CEUD for new purposes materially different than those for which it was originally collected. Notice should be clear and conspicuous, and should address the following:

a. The specific types of Information that are being collected by the Service Provider, and containing a statement that the Service Provider has committed to only collecting that Customer Data needed to support a Primary Purpose.

b. At a high level and in easy to understand language, the Service Provider should explain how the Customer Data is being used, and should specifically:
   i. Explain the means by which Account Data is collected (application for service, online, consumer hotline, mail, credit report, etc.)
   ii. Explain the means by which CEUD is collected (e.g., meters)
   iii. Provide an overview of the Primary and Secondary Purposes
   iv. Explain how individual level Customer Data will be used
   v. Explain that data they collect may be used in conjunction with or merged with other data to create Aggregated or Anonymized Data reports and under what circumstances those reports typically will be used and shared.

c. How the customer can access his or her Customer Data, and the process by which the customer can identify possible inaccuracies and request correction.

d. The circumstances under which the Service Provider will share Customer Data without first obtaining consent. Specifically, the notice should:
   i. Notify customers of the types of Contracted Agents with whom the Service Provider is sharing the data to support a Primary Purpose (e.g., service providers, contractors, etc.).

ii. Notify customers of the types of supporting services (e.g., credit reporting agency, government entity, etc.) with whom the Service Provider is sharing the data to support a Primary Purpose or as mandated by law/regulation.
iii. Inform customers of instances where the Service Provider will release Customer Data without consent, as identified in concept # 2, Customer Choice and Consent, *Consent Not Required* exceptions.
iv. Inform customers of the purpose of sharing the data.

e. How the customer can approve Third Party access to their Customer Data for a Secondary Purpose, or revoke access previously granted.

f. How the data is secured
   i. Service Providers should describe for customers how their Customer Data will be secured throughout its lifecycle, in accordance with any requirements of applicable regulatory authorities.

g. Retention & Disposal
   i. Customers should be informed that Customer Data will be retained and disposed of consistent with applicable local, state, and federal record retention rules and regulations, as well as applicable company policies.

h. Minimum Notice Inclusions:
   i. An effective date for the initial notice and any subsequent policy changes
   ii. A point of contact for customer questions about the Service Providers privacy-related policies and data access procedures.
   iii. A summary of changes to the previous version, as applicable, or a means by which previous versions can be obtained.

i. Customers should be made aware of their responsibilities as a customer (e.g., providing accurate data, giving notification of changes in Account Data, etc.) in support of responsible data practices.

2.0 CUSTOMER CHOICE AND CONSENT – The concept that customers should have a degree of control over access to their Customer Data. Service Providers and their Contracted Agents require Customer Data to support Primary Purposes. For Secondary Purposes, however, customers should be able to control access to their Customer Data ~~by other parties~~ via a customer consent process which is convenient, accessible, and easily understood~~,~~. This could include, for example, timing disclosures to coincide with the time and place that customers have the ability to exercise choices (e.g., push notifications for software downloads) regarding the use of their CEUD for new purposes materially different than those for which ~~has~~it was originally collected. The customer consent process should have the following functional characteristics:

a. Explains how the customer can exercise his or her choices to share Customer Data.

b. Explains specifically which elements of the Customer Data are proposed to be shared with a Third Party, for what purpose, and for how long.

c. Allows the customer to authorize different types of disclosures of his or her Customer Data among multiple Third Parties.

d. Allows the customer to rescind disclosure authority previously granted to a specific Third Party.

e. Requires the customer's consent for disclosure of Customer Data for Secondary Purposes to be specifically and affirmatively expressed before data is shared with Third Parties.

f. Limits disclosure to that data which the customer has authorized for a specific Third Party for a specific purpose.

g. Is secure so that the customer is reasonably protected against disclosures based on fraudulent consent. (Note: on-line processes may be secure without additional validation. To the extent a process is needed to ensure the validity of customer authorizations, privacy policies should clearly define the party responsible for performing such validations.)

h. Ceases disclosure when: (1) the customer rescinds his or her authorization, (2) the authorization expires, or (3) the customer terminates service. (Note: When a Third Party receiving duly authorized Customer Data is sold, the Service Provider providing the Customer Data is not required to notify the customer of the change in ownership, and the new owner can continue receiving Customer Data without the need for a new disclosure authorization. However, the Third Party receiving Customer Data must notify the customer of the change in ownership.)

i. Allows Service Providers to charge a fee, subject to regulatory oversight and approval, for non-standard requests (e.g., requests that data be in a custom interval, and/or a custom format). This applies to requests for individual Customer Data, and requests for Aggregated Data and Anonymized Data.

j. Is efficient. The business processes supporting consumer choice and consent should be cost-efficient and utilize standard formats.

Record Retention and Disposal:

(1) Service Providers should retain Customer Data only as long as needed to fulfill the purpose it was collected for, unless they are under a legal obligation to do otherwise.

(2) Service Providers should securely and irreversibly dispose of or de-identify Customer Data once it is reasonably determined by the Service Provider to be no longer necessary to achieve the purposes for which it was collected, unless they are under a legal obligation to do otherwise.

(3) Service Providers should maintain records identifying what type of Customer Data has been shared previously with Third Parties, when the sharing occurred and with whom the data was shared for as long as the data exists in the Service Providers' systems or as long as legally required.

Consent Not Required: Prior customer consent is not required to disclose Customer Data in the case of:

(1) Third Parties responding to emergencies that pose imminent threats to life or property;

(2) Law enforcement or other legal officials to whom disclosure is authorized or required by law;

(3) As directed by Federal or State law, or at the direction of appropriate regulatory authority; or

(4) Aggregated or Anonymized Data. Service Providers can share Aggregated or Anonymized data with Third Parties without first obtaining customer consent if the methodology used to aggregate or anonymize Customer Data strongly limits the likelihood of reidentification of individual customers or their Customer Data from the aggregated or Anonymized data set.

i. Aggregated and Anonymized Data may be shared via a contract between the Service Provider and Third Party that requires that the Third Party not attempt to re-identify customers.

ii. The service provider may decline a request for Aggregated or Anonymized Data release if fulfilling such a release would cause substantial disruption to the day-to-day activities of its personnel.

(5) Activities conducted in order to preserve the safety and reliability of the electric grid and critical infrastructure or the integrity or security of other systems containing Customer Data.

Access to Data Other Than Customer Data: Except as required by law, Service Providers will not share with a Third Party the customer's: social security number; state or federal issued identification number; financial account number in combination with any security code providing access to the account; Consumer report information provided by Equifax, Experian, TransUnion, Social Intelligence or another consumer reporting agency; individually identifiable biometric data; or first name (or initial) and last name in combination with any one of the following: (1) date of birth; (2) mother's maiden name; (3) digitized or other electronic signature; and (4) DNA profile. Such information should be obtained directly from the customer.

Data Access Exclusions:

(1) Aggregated or Anonymized Data that is reasonably likely to allow identification of the Service Provider's trade secrets, confidential or proprietary data even when aggregated or anonymized, may not be released.

(2) Overlapping data requests from the same requestor should not be permitted if ~~the Service Provider is aware that it may~~granting such requests is reasonably likely to compromise the aggregation and reveal information that could be used to identify or re-identify customers or Customer Data.

3.0 CUSTOMER DATA ACCESS AND PARTICIPATION – The concept that customers should have access to their own Customer Data and should have the ability to participate in its maintenance. The process by which customers access their Customer Data should have the following attributes:

a. Is reasonably convenient, timely, and cost-effective.

b. Allows the customer to identify possible inaccuracies and request that they be corrected.

c. Allows the Service Provider to charge a fee, subject to applicable laws and regulations, to the extent the Service Provider offers a method of data access that is different from the method it generally offers to its customers, or is not based on commonly used data formats or standards.

d. Allows the Service Provider to recover costs for Aggregated Data requests that are different from the method or format in which it generally offers aggregated data, represents the fulfillment of multiple requests, or is not based on commonly used data formats or standards.

4.0 INTEGRITY AND SECURITY – The concept that Customer Data should be as accurate as reasonably possible, and secured against unauthorized access. Data should be maintained in a reasonably accurate and complete form, considering the circumstances and environment in which it has been collected (e.g., recognizing the difference between raw meter data and bill-ready data). Data should be protected via a cybersecurity risk management program which has the following attributes:

a. Identifies, analyzes, and mitigates cybersecurity risk to the Service Provider's organization with respect to Customer Data.

b. Implements and maintains process, technology, and training measures to preserve data integrity and reasonably protect against loss and unauthorized use, access, or dissemination.

c. Maintains a comprehensive data breach response program for the identification, mitigation and resolution of any incident that causes or results in the breach of Customer Data security.

d. Provides complete, accurate, and timely notice to customers whose Customer Data may have been compromised while within the Service Provider's control or within the control of Service Provider's Contracted Agent, and remedies those conditions which led to the breach.

e. In the event that a Service Provider has modified or enhanced data that it initially received from another source (e.g., a utility or a different third party), the customer receiving the enhanced or modified data should generally be made aware that such data may differ from the original data.

Aggregated Data Methodologies: When developing an Aggregation methodology that will meet the requirements of Concept 2.0 Customer Choice and Consent, subheading *Consent Not Required,* item (4), the following variables should be considered:

(1) **Customer Identifiers**: the aggregated data set should not include an individual customer's Account Data, or other identifying data.
(2) **Number of Customers**: A sufficient number of customers should be included in the data set to reduce the ability to re-identify a customer.
(3) **Customer Load**: If the load of a particular customer represents an outlier (e.g. greater or less than a percent of the ratio) when compared to other customers in the data set, consideration should be given to whether the size of the customer's load can be masked to prevent identification or re-identification, or if not possible, that customer's data should be excluded from the data set.
(4) **Customer Class**: differences in energy usage patterns between customer classes should be considered when deciding whether to aggregate multiple classes into one aggregated data set.
(5) **Timescale**: the ability to identify or re-identify customers or attribute to those customers specific Customer Data may vary based on the interval of energy reading, creating differences in methodologies used for hourly, monthly, quarterly and yearly data.
(6) **Geographic Identifiers**: the relative size of the geographic area associated with the selection of customers for the data could result in reidentification.

Methods by which data can be aggregated should be reviewed every 2 years or more frequently if needed to account for changes in technology and risk related to data aggregation.

Anonymized Data Methodologies: When creating a methodology to anonymize Customer Data, the following variables should be considered as applicable to the specific situation:

(1) **Customer Identifiers**: the Anonymized data should not include an individual customer's Account Data, or other identifying data.
(2) **Customer Load and Energy Pattern**: the customer's load and/or energy pattern should be examined to determine if it is so unique among other customers that it could compromise the anonymization.
(3) **Customer Class**: the data should be homogenous; mixing of residential, commercial, industrial or agricultural customers in the same data set could compromise the anonymity of individual customers.
(4) **Timescale**: the customer's time series data should be assigned a random identification number and listed randomly.
(5) **Energy Pattern**: customers with unique energy patterns should be removed.
(6) **Masking Data**: explore masking techniques that enhance the anonymity of data without negatively impacting the validity of the data set.

5.0 SELF ENFORCEMENT MANAGEMENT AND REDRESS - the concept that there should be enforcement mechanisms to ensure compliance with the foregoing concepts and principles. Service Providers who voluntarily adopt this Voluntary Code of Conduct commit to the following:

a. To regularly review their Customer Data practices, including customer notice practices, for accuracy, compliance, and process improvement opportunities.

b. To take action to meet legal and regulatory data protection mandates and, when necessary, to ensure compliance with the foregoing principles.

c. To provide a simple, efficient, and effective means for addressing customer concerns. Customer processes should be easily accessed, and should provide timely review, investigation, documentation, and resolution of the customer's concerns. Existing procedures for addressing other types of customer complaints may be adequate.

d. To conduct regular training and ongoing awareness activities for relevant employees on the Service Provider's privacy policies and practices.