BEFORE THE MINNESOTA PUBLIC UTILITIES COMMISSION

Beverly Jones Heydinger	Chair
David C. Boyd	Commissioner
Nancy Lange	Commissioner
Dan Lipschultz	Commissioner
Betsy Wergin	Commissioner

In the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities

ISSUE DATE: June 24, 2014

DOCKET NO. E,G-999/CI-12-1344

ORDER REQUIRING UTILITIES TO ADOPT AND DOCUMENT PROCESSES REGARDING PERSONALLY IDENTIFIABLE INFORMATION AND OTHER ACTION

PROCEDURAL HISTORY

On June 17, 2013, the Commission issued an order seeking input from each electric and gas utility as to current utility data practices and privacy policies related to personally identifiable information (PII) including that related to the collection and handling of customers' Social Security numbers.

On July 19, 2013, the Commission issued a Notice of Comment period on the collection, maintenance, and use of such customer information by electric and gas utilities. Utilities and commenters were asked to focus, among other things, on the items listed in the Commission's June 17, 2013 Order, with a focus on:

- The possible adoption of privacy standards, risk assessment protocols, and/or filing requirements for rate-regulated gas and electric utilities with respect to customers' personally identifiable data;
- Issues related to the collection, maintenance, and sharing of customer data; and
- The collection and handling of customer Social Security numbers.

The Commission received comments and/or reply comments from the following utilities:

CenterPoint Energy (CenterPoint)	Minnesota Energy Resources Corporation
Dakota Electric Association	Minnesota Power
Great Plains Natural Gas Company	Otter Tail Power
Interstate Power and Light Company	Xcel Energy

The Commission also received comments from the Legal Services Advocacy Project (LSAP), the Minnesota Large Industrial Group, Opower, the Office of the Attorney General, and the Department of Commerce (the Department).

On May 29, 2014, the Commission met to consider the matter.

FINDINGS AND CONCLUSIONS

I. Summary of Commission Action

The Commission authorizes rate-regulated utilities to collect and use customer Social Security numbers only in a manner that complies with federal and state law, and specifically clarifies a customer's right to refuse to provide his or her Social Security number to the utility.

The Commission also defines "personally identifiable information (PII)" and requires utilities to adopt and document the processes used to collect and protect customer PII data, consistent with the protections set forth in the National Institute of Standards and Technology's (NIST's) *Guide to Protecting the Confidentiality of Personally Identifiable Information* (800-122; April 2010) and the principles set forth herein.

Further, utilities may not sell customer PII data; utilities may, however share such data for a regulated purpose with a contractor required to provide equivalent or greater protection so long as the utility retains responsibility to the customer in the event of unauthorized use.

Finally, utilities must annually review their privacy policies and processes.

II. Background

In December 2012 the Commission began an investigation of the possibility of opening a generic proceeding to address the collection, storage, and dissemination of customer data by rate-regulated energy utilities in response to an Xcel filing seeking approval of its customer data privacy policies.[1]

According to Xcel, the deployment of advanced metering infrastructure has resulted in increased focus on customer data privacy. In its March 2012 petition, Xcel asserted that although it has company policies and procedures in place concerning data privacy, a privacy tariff could clarify for customers how Xcel handles customer information.

In light of the record developed in Xcel's privacy tariff docket, the Commission established this docket to address, among other things, the collection, storage, and dissemination of customer data. After comments from parties, the Commission issued an order seeking further input on the treatment of personally identifiable information (PII) and on current utility data practices and privacy policies related to personal information, including the collection and handling of customers' Social Security numbers.

[1] *In the Matter of the Petition of Northern States Power Company for Approval of a Customer Data Privacy Tariff as an Amendment to the Electric and Natural Gas Rate Books*, Docket No. E, G-002/M-12-188 (December 13, 2012).

The Commission's June 17, 2013 order requested comments on a wide range of privacy and data security topics. (Attachment A)

III. Positions of the Commentors

Commenters addressed the broad scope of issues raised. Utilities generally focused their comments, however, on their internal data privacy practices and procedures, their collection, storage and dissemination of customer information, and their handling of customer Social Security numbers.

A. Customer Social Security Numbers

The utilities generally agreed that requesting Social Security numbers is useful in detecting identity fraud and bill collecting, and that prohibiting use of Social Security numbers would create significant difficulties in carrying out necessary business functions.[2] Most utilities, however, also acknowledged that they have alternative means of authenticating a customer's identity should a customer decline to provide a Social Security number.

The utilities also agreed that the use of a customer's Social Security number has not been a problem and the Commission should not prohibit the collection and use of customer Social Security numbers. Many utilities supported their position citing Minn. Stat. § 325E.59, which permits the collection and use of Social Security numbers with certain restrictions.[3]

CenterPoint argued that it is appropriate for utilities to collect and maintain customer Social Security numbers, arguing that it assists them: 1) to help identify individuals during the service initiation process, 2) to provide customers with one of several authentication options for account access, and 3) to help identify individuals in the Company's credit and collection process.

Xcel stated that limiting the company's ability to collect and maintain customer Social Security numbers would "severely hamper" its ability to prevent fraud in opening accounts and collection of past-due amounts.

The Office of the Attorney General, the Legal Services Advocacy Project (LSAP), and the Department all filed comments recommending that the Commission disallow utility collection and retention of Social Security numbers. These parties argued that the risks associated with the collection and use of customer Social Security numbers by utilities, and possible disclosure of highly sensitive customer-specific information, outweigh the benefits of use of such information as an easy identity

---

[2] E.g., Otter Tail Power stated that substantial effort and cost would be required to rework its system to avoid the use of Social Security numbers to validate identity for new accounts.

[3] Minn. Stat. § 325E.59 does not prevent the following uses of Social Security numbers:

> (1) the collection, use, or release of a Social Security number as required by state or federal law:
>
> (2) the collection, use, or release of a Social Security number for a purpose specifically authorized or specifically allowed by a state, or federal law that includes restrictions on the use and release of information on individuals that would apply to Social Security numbers; or
>
> (3) the use of a Social Security number for internal verification or administrative purposes.

verification for the utility or aid in reducing bad debt expenses.[4] Finally, the Department noted that while utility customers generally have a choice as to the companies with whom they choose to transact business, they have no choice as to their assigned utility carrier.

B. Personally Identifiable Information

The utilities generally disfavored the imposition of new requirements to adopt a privacy impact assessment or information security plan. Instead, they argued that they are already bound by numerous regulatory laws at the state and federal level and that adding additional policies or guidelines would not only be redundant but would also add cost and potential confusion to the plans they have in place. Importantly, the utilities asserted that they already have in place adequate internal company standards and corporate policies that protect sensitive customer data as a part of doing business.

Xcel recommended that the Commission forgo imposing the requirements of a specific privacy impact assessment on utilities at this time, reasoning that such requirements may not be necessary. Xcel urged the Commission to first secure and evaluate current utility practices and requirements, and then determine its customer data privacy priorities.

CenterPoint asserted that it has in place a robust Cyber Security Plan that helps protect the security of personally identifiable information of its customers. The company claimed that requiring a new regulatory regime of conducting and filing privacy impact assessments and information security plans is unnecessary and redundant.

CenterPoint also addressed the issue of sharing customer data with non-regulated affiliated companies. CenterPoint stated that in addition to its regulated operations, it also operates a non-regulated appliance sales and service business. CenterPoint asked that if the Commission chooses to explore the sharing of customer data with non-regulated affiliated companies, that it avoid disrupting the cost-sharing relationship between CenterPoint and its long-standing appliance repair business previously reviewed and approved by the Commission.[5]

Other utilities echoed the belief that their existing data privacy practices, whether required by law or company policy, are sufficient to safeguard sensitive customer information.

The Office of the Attorney General, the Legal Services Advocacy Project, and the Department of Commerce expressed the opinion that the Commission should act promptly to set policy guidelines or processes to protect sensitive customer data, which the utilities collect and hold. The Department recommended that utilities be asked to adopt reasonable processes (whether established in a privacy impact assessment or information security plan, or similar internal plan) to collect and protect customer data based on Commission-established principles such as the following:

---

[4] In lieu of Social Security numbers, LSAP recommended that utilities create a unique, long-term identifier by using "a computer algorithm to digitize a person's full name, date of birth, parent name, place of birth and/or other permanent personal characteristic." (LSAP initial comments at 15)

[5] *In the Matter of a Complaint of the Minnesota Alliance for Fair Competition Against Minnegasco, a Division of Arkla*, Inc., Docket No. G-008/CI-91-942, Order Establishing Accounting Procedures and Requiring Further Filings (November 10, 1992).

- Information collected and maintained is limited to the minimum amount needed to perform a regulated utility business function;
- Information is used only for the purposes for which it was collected, unless prior consent is clearly given by the affected customer based on accurate and complete information as to how the information would be used;
- Customers are able to review and correct erroneous information;
- Customers, the Commission, the Department, and the Office of the Attorney General are notified promptly in the event of a data breach;
- Access to the information is controlled and limited to those employees needing it for the identified business purpose; and
- Data privacy policies and processes are regularly audited for continued appropriateness and adequacy.

The Department also recommended that sharing of customer PII data with any other entity should be restricted to fulfilling an essential business purpose of the utility, and only after the utility obtains consent from the customer, and only upon condition that the receiver maintains equal or greater data protections measures.

IV. Commission Action

A. Personally Identifiable Information Defined

A threshold issue in this proceeding is the definition of "personally identifiable information." The Commission believes that its adaptation of the definition of personally identifiable information used by the National Institute of Standards and Technology (NIST) is appropriate for purposes of this docket. The definition is broader in scope than that used in Minn. Stat. § 325E.61, which defines specific categories of information such as driver's license or social security number. The NIST-based definition requires parties to pay attention to information that can be used to distinguish or trace the identity of an individual *when linked with* other personal or identifying information (emphasis added).

Accordingly, for purposes of this docket, the Commission will use the definition of personally identifiable information set forth below:

> Personally Identifiable Information (PII) shall be defined as "customer PII data which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.)." (Source: NIST's *Security and Privacy Controls for Federal Information Systems and Organizations*; 800-53; April 2013).

B. Customer Social Security Number

First, it is clear that Minnesota utilities have long collected and used customer Social Security numbers, apparently without incident, for purposes of customer identification and account verification and/or access. Minn. Stat. § 325E.59 directly addresses the use of Social Security numbers by Minnesota businesses and permits the collection and use of Social Security numbers with certain

restrictions not applicable here. From the record developed in this matter, and the knowledge that state utilities are generally subject to higher standards and increased accountability than other businesses, the Commission can ascertain no reason why state utilities should be subject to standards more restrictive than those imposed on other state businesses with respect to the use of Social Security numbers.

Accordingly, the Commission finds that rate-regulated electric and gas utilities may collect and use customer Social Security numbers, but only in a manner that complies with federal and state law.

Finally, the utilities have acknowledged that while state and federal law permit the collection and use of a customer's Social Security number, no law requires a customer to provide a utility with his or her Social Security number. Accordingly, a customer has the right to refuse to provide his or her Social Security number to the utility.[6] Recognizing this, the Commission's finding with respect to a utility's use of customers' Social Security numbers is in not intended to provide additional authority or rights to a utility than those granted by state or federal law.

C. Reasonable Processes to Collect and Protect Personally Identifiable Information

The Commission has considered the filings and comments of the parties, and incorporates many of the parties' recommendations and/or caveats in setting out the principles and guidelines that the Commission will require utilities to follow, as set forth below. These principles and guidelines are meant to ensure that utilities only collect the PII data that is needed for purposes of carrying out a regulated business purpose, and that customer information is protected such that it is not shared beyond the regulated purpose without notice and the explicit consent of the customer or the permission of the Commission.

First, the Commission will require utilities to adopt and document the internal processes used to collect and protect customer PII data, after ensuring that the processes used are consistent with the protections set forth in NIST's *Guide to Protecting the Confidentiality of Personally Identifiable Information* (800-122; April 2010), and based on the following Commission principles:

A) The utility shall collect and maintain only the customer PII data needed to perform its regulated utility business functions;

B) The utility shall give the customer clear and accurate information about how the customer PII data will be used and protected;

C) The utility shall use the customer PII data solely for the purposes for which it was collected, unless prior written consent is clearly given by the affected customer or with the approval of the Commission;

[6] The utilities have indicated that they have developed methods by which to address customer identification and account verification in those circumstances in which a customer has refused to provide a Social Security number.

D) Customers shall be able to review their own customer PII data and request deletion of their Social Security number and/or correction or deletion of any customer PII data improperly collected or retained. Disputes regarding the deletion of a Social Security number or customer PII data that remain unresolved for more than 45 days from the date of the request for deletion may be brought by the customer or the utility to the Commission for a determination;

E) The utility shall control and limit access to customer PII data to those employees who need it for an identified business purpose; and

F) The utility shall annually review its data privacy policies and processes for continued appropriateness and adequacy.

The Commission will require a utility to submit its customer notice to the Commission for review.

Second, utilities may not sell PII data. The Commission recognizes, however, that certain utilities make use of contractors in carrying out their regulated business functions, and that it is necessary to share customer PII data in that context. The Commission will allow a utility to share necessary customer PII data with a contractor for a regulated business purpose, so long as the contractor is required to provide equivalent or greater protection for the customer data. Importantly, the Commission will require that the utility retain ultimate responsibility to the customer in the event of the contractor's unauthorized use or release of data.

Third, the Commission will allow a utility to share customer PII data for a purpose other than related to regulated utility service only after the utility obtains explicit, written consent from the customer that includes a clear statement of the information to be shared and with whom it will be shared. The Commission will deem customer consent expressly given valid until revoked by the customer, but for no more than one year or the contract term, subject to renewal.

Fourth, the Commission recognizes that certain sharing of customer PII data may have previously been allowed by the Commission. The principles and findings set forth in those previous dockets remain in effect, but must be revised, if necessary, and resubmitted to the Commission within 60 days of this order for a determination that it complies with its terms.

Fifth, in the event of an unauthorized disclosure or use of customer PII data, a utility will be obligated to promptly notify its affected customers, the Commission, the Department, and the Office of the Attorney General. In its notice, the utility should include at least the following information: the number of customers affected; the date or period of the breach; the types of data inappropriately accessed; and whether the source or cause of the breach has been identified and provided to law enforcement officials.

If the utility has not informed law enforcement of the unauthorized disclosure, it must provide an explanation of why it has determined such notice was unnecessary. Importantly, the utility will be required to identify the steps necessary to redress the breach as well as the steps it has taken to prevent a similar breach in the future.

Finally, each rate-regulated utility will be required to make a compliance filing within 60 days of the order showing that it has policies consistent with this order.

ORDER

1. All rate-regulated electric and gas utilities may collect and use customer Social Security numbers only in a manner that complies with federal and state law. A customer has the right to refuse to provide his or her Social Security number to the utility.

2. Personally Identifiable Information (PII) shall be defined as "customer PII data which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.)" (Source: NIST's *Security and Privacy Controls for Federal Information Systems and Organizations*; 800-53; April 2013).

3. Each rate-regulated electric and gas utility shall adopt and document reasonable processes to collect and protect customer PII data, consistent with the protections set forth in NIST's *Guide to Protecting the Confidentiality of Personally Identifiable Informatio*n (800-122; April 2010), and based on the following Commission principles:

   A) The utility shall collect and maintain only the customer PII data needed to perform its regulated utility business functions;

   B) The utility shall give the customer clear and accurate information about how the customer PII data will be used and protected;

   C) The utility shall use the customer PII data solely for the purposes for which it was collected, unless prior written consent is clearly given by the affected customer or with the approval of the Commission;

   D) Customers shall be able to review their own customer PII data and request deletion of their Social Security number and/or correction or deletion of any customer PII data improperly collected or retained. Disputes regarding the deletion of a Social Security number or customer PII data that remain unresolved for more than 45 days from the date of the request for deletion may be brought by the customer or the utility to the Commission for a determination;

   E) The utility shall control and limit access to customer PII data to those employees who need it for an identified business purpose; and

   F) The utility shall annually review its data privacy policies and processes for continued appropriateness and adequacy.

4. Each rate-regulated electric and gas utility shall submit its customer notice to the Commission for review.

5. Each rate-regulated electric and gas utility may provide necessary customer PII data to a contractor for a regulated purpose, so long as the contractor is required to provide equivalent or greater protection for the customer data, and the utility retains responsibility to the customer in the event of the contractor's unauthorized use or release of data.

6. No rate-regulated electric or gas utility shall sell customer PII data.

7. Each rate-regulated electric and gas utility may share a customer's PII data for a purpose other than related to regulated utility service only after the utility obtains explicit, written consent from the customer that includes a clear statement of the information to be shared and with whom it will be shared. Customer consent shall be deemed valid until revoked by the customer, but for no more than one year or the contract term, and is subject to renewal.

8. Sharing of customer PII data previously authorized by the Commission remains in effect, but must be revised, if necessary, and resubmitted to the Commission within 60 days of the date of this order in this matter for a determination that it complies with the terms of this order.

9. Each rate-regulated electric and gas utility shall promptly notify affected customers, the Commission, the Department, and the Attorney General's Office in the event of an unauthorized use or release of customer PII data. Notice shall include the number of customers affected, date or period of breach, types of data inappropriately accessed, whether the source or cause of the breach has been identified and provided to law enforcement, steps taken to prevent similar breaches, and steps to redress the breach.

10. Each rate-regulated electric and gas utility shall file compliance filings within 60 days of this order that demonstrate it has policies consistent with this order.

11. This order shall become effective immediately.

BY ORDER OF THE COMMISSION

Burl W. Haar
Executive Secretary

This document can be made available in alternative formats (e.g., large print or audio) by calling 651.296.0406 (voice). Persons with hearing loss or speech disabilities may call us through their preferred Telecommunications Relay Service.

The Commission's June 17, 2013 order requested comments on a wide range of topics, including:

Whether it is appropriate to require rate-regulated utilities to:

> Adopt a reasonable Privacy Impact Assessment (PIA), or set of PIAs as appropriate, consistent with the federal PIA requirements of the E-Government Act of 2002 and resulting regulations, and to file it with the Commission;
>
> Adopt a reasonable risk-based Information Security Plan (ISP), or set of ISPs, consistent with the federal ISP requirements of the Federal Information Security Management Act of 2002 and resulting regulations and guidelines, and to file it with the Commission;
>
> Ensure that the PIAs and ISPs address, not by way of limitation, each of the following:
>
> 1. Notice to the customer of the data collected and the reasons for it, whether the customer must provide the data as a condition of service.
> 2. Limitations to assure that only the data that is relevant and necessary is collected.
> 3. The type and frequency of notice provided to the customer about the utility's privacy policy.
> 4. The utility's allowable uses of the data, with and without customer consent.
> 5. Customer access to one's own data.
> 6. Procedure for withdrawing consent.
> 7. Procedure for the customer to correct inaccurate or incomplete information.
> 8. Limitations on use by the utility.
> 9. How the data will be retained and secured.
> 10. How long the data will be retained and the steps taken to purge it.
> 11. Delineation of authorized and unauthorized use.
> 12. Protections and limitations in place to prevent unauthorized use, access, destruction, loss, modification, etc.
> 13. Procedures in place for documenting authorized use.
> 14. Notice to the customer of breach.
> 15. Redress and penalties for unauthorized (intentional or unintentional) disclosure.
> 16. Process, including frequency, of review and audit to assure that privacy policies are in place, are followed, and provide adequate protection for the customer, with the utility and its contractors.

Is it appropriate for the Commission to adopt the Fair Information Practices (FIPs) as the guiding set of privacy principles and as the standard benchmark against which utility privacy actions will be assessed?

Is it appropriate to allow utilities to share data with its contractors for energy efficiency programs so long as the utility assures that the contractor agrees to specified privacy protections equivalent to the utility's and accepts liability for breach?

Is it appropriate to require such contractors to register and to demonstrate that compliance with specified privacy protections?

Are there circumstances under which it would be appropriate to allow a utility to sell customer information?

Is it appropriate to collect and maintain customer Social Security numbers, and if so, the purpose for doing so, and specifying whether the utility could use the information solely to create a unique account identifier and then to purge the number from its records?

Should the Commission address the sharing of customer data with non-regulated affiliated companies?

Should the Commission develop a "privacy seal" initiative to certify the level of customer privacy provided?[1]

[1] Order Establishing Procedures for Further Comment and for Working Group, (this docket) (June 17, 2013) at Ordering Point 3.