414 Nicollet Mall
Minneapolis, Minnesota 55401-1993

January 30, 2013

Burl W. Haar
Executive Secretary
Minnesota Public Utilities Commission
121 7th Place East, Suite 350
St. Paul, MN 55101

—Via Electronic Filing—

RE: COMMENTS
PRIVACY POLICIES OF RATE-REGULATED ENERGY UTILITIES
DOCKET NO. E,G-999/CI-12-1344

Dear Dr. Haar:

Northern States Power Company, doing business as Xcel Energy, submits the enclosed Comments in response to the Minnesota Public Utilities Commission's January 8, 2013 NOTICE OF COMMENT PERIOD ON CUSTOMER DATA PRIVACY.

We have electronically filed this document with the Commission, which also constitutes service on the Department of Commerce and the Office of the Attorney General. A copy of this filing has been served on all parties on the official service list in this docket.

Please contact Jody Londo at (612) 330-5601 or jody.l.londo@xcelenergy.com if you have any questions regarding this filing.

Sincerely,

/s/

CHRISTOPHER B. CLARK
REGIONAL VICE PRESIDENT
RATES AND REGULATORY AFFAIRS

Enclosures

c: Service List

STATE OF MINNESOTA
BEFORE THE
MINNESOTA PUBLIC UTILITIES COMMISSION

Beverly Jones Heydinger	Chair
Phyllis Reha	Commissioner
David C. Boyd	Commissioner
J. Dennis O'Brien	Commissioner
Betsy Wergin	Commissioner

IN THE MATTER OF A COMMISSION INQUIRY INTO PRIVACY POLICIES OF RATE-REGULATED ENERGY UTILITIES	DOCKET NO. E,G-999/CI-12-1344 **COMMENTS**

INTRODUCTION

Northern States Power Company, doing business as Xcel Energy, submits to the Minnesota Public Utilities Commission these Comments responding to the Commission's January 8, 2013 NOTICE OF COMMENT PERIOD ON CUSTOMER DATA PRIVACY.

We believe that our customers have reasonable expectations of privacy related to the individually-identifiable information we collect and maintain. We also believe that providing appropriate access to customer usage data is in the public interest – and that a reasonable balance between data access and customer privacy can be achieved. We look forward to working with interested parties and the Commission to develop clear "rules of the road" for utilities, customers, and those who seek the data that only the utilities hold.

We believe it is appropriate for the Commission to focus on creating a general framework for access and use of customer energy usage data applicable to all energy utilities. We support a practical approach that facilitates constructive dialogue, provides flexibility within a framework, achieves timely resolution, addresses costs, and balances privacy interests with public policy objectives dependent on reasonable access to data.

We appreciate the Commission's continued interest in this important topic, and provide these comments toward advancing the dialogue among interested parties.

COMMENTS

We respond below to the questions posed in the Commission Notice:

1. *Do current service standards provide adequate customer data privacy protection and redress for customers in the event of the data breach?*
    a) *Who is liable (or should be) and to what degree in the event of stolen identity or financial harm to customers?*
    b) *Is there already state (or federal) redress in the event of customer identity theft or privacy intrusion? Please cite specific rules or laws.*
    c) *What additional measures (if any) should the Commission require of all rate-regulated energy utilities to protect customer data at this time?*

No, not fully. In our response, we summarize current protections provided by various statutory, regulatory, common law, and policy protections. While privacy protections for some types of customer information are addressed in current statutes or exist as part of other legal constructs, gaps exist for certain types of customer information collected and maintained by energy utilities. We believe that Commission action in the area of Customer Energy Usage Data (CEUD) would fill a critical gap in current privacy protections for Minnesota energy utility customers.

Summary – Liability and Redress

The Commission's questions seek information regarding liability and redress in the case of data breach, identity theft, privacy intrusion, and financial harm to customers. In considering these issues, it is important to recognize that there are a variety of state and federal laws that identify different requirements and remedies by data type. These laws create a high level of regulation for specific data that falls within their scope, but they do not address other types of data. We summarize below Xcel Energy's definitions of various type of customer information, and outline relevant legal protections by customer information category in Table 1:

- *Personal Data:* Individually-identifiable information relating to an individual, in particular by reference to an identification number such as Social Security Number (SSN), state issued identification number, or financial account information. This is comparable to the definition of "Personal Information" contained in Minn. Stat. § 325E.61.
- *Account Data:* Individually-identifiable information that is not Personal Data or Customer Energy Usage Data. Account Data includes customer contact information, payment history, and amount billed, but does not include

company-proprietary information such as meter number or an Xcel Energy billing identifier (Premise Number).

- *Customer Energy Usage Data (CEUD):* Customer-specific data or information that: (1) is collected from the meter and stored by the utility in its systems; and, (2) is received from the customer or derived by the utility, identifying regulated utility program participation, such as renewable energy, demand-side management, load management, and energy efficiency.

Table 1: Summary – Relevant Sources of Protection By Customer Information Category

Personal Data	Account Data	Customer Energy Usage Data
• Utility policies • Minn. Stat. § 325E.61 (data breach) • Minn. Stat. § 325E.59 (SSN protection) • FTC and MN OAG enforcement actions • Payment Card Information Data Security Standard (PCI DSS) • Potential private actions	• Utility policies • FTC enforcement actions • Potential private actions	• Utility policies • Potential private actions

Only under common law is there a general privacy intrusion remedy, and only if the customer can show a causal connection between specific facts and actual harm. Otherwise, Minnesota law currently addresses identity theft and other specific privacy-related incidents involving Personal Data. Additionally, the FTC has brought enforcement actions related to companies' mishandling of Personal Data and, Account Data as a result of their failure to follow their own privacy policies. However, neither Minnesota law nor the FTC has addressed the privacy issues inherent to a customer's energy usage, creating a significant gap in current guidance and protection of CEUD.

We provide as Attachment A to these Comments, further discussion of the various legal protections outlined in Table 1.

As discussed further in our response to Question No. 2 below, we believe there is a critical gap in Minnesota privacy protections for CEUD. We note that we discuss general policy measures the Commission may want to consider taking at this time in our response to Question No. 3.

2. *Should the Commission establish uniform customer data collection and privacy policies for rate-regulated utilities?*
    a) *If yes, what process should be employed? For example, should the Commission host a technical conference or workshop in addition to comment periods before enacting general policy measures or temporary moratoriums?*
    b) *If no, should each utility/company be required to file a privacy tariff for Commission approval as to how it solicits, retains, discloses and otherwise protects customer data? Why or why not? For example, how might the filed rate doctrine or doctrine of primary jurisdiction influence your answer?*
    c) *Because the filed rate doctrine and doctrine of primary jurisdiction applies to regulated telecommunications companies as well as energy utilities, should the Commission include telecommunications companies on this topic? Why or why not?*
    d) *What other method or measures might be beneficial to examine the issues surrounding the collection, use and handling of customer data? For example, should the Commission open a Rulemaking? Why or why not?*
    e) *Should utilities and third parties receiving customer data adopt Codes of Conduct, and companies that breach the Codes of Conduct can be subject to Federal Trade Commission (FTC) enforcement?*

As discussed in our response to Question No. 1, a robust, comprehensive framework exists to protect Personal Data, and the FTC is actively engaged in enforcement actions regarding both Personal Data and Account Data. At this time, however, there is little legal or regulatory oversight of CEUD. However, the Commission has broad authority over the reasonableness and standards of utility service.[1] Based on this authority and the current gap for CEUD in federal and Minnesota law, we believe the Commission can and should adopt generally-applicable privacy principles relating to CEUD.

A common framework established by the Commission would:

- Establish clear guidance and expectations for customers, energy utilities, and third-parties;
- Ensure consistency for all Minnesota energy utility customers; and
- Facilitate appropriate access for customers and third parties seeking access to CEUD for public policy reasons.

We believe filling this critical gap in Minnesota privacy protections would provide immediate value for Minnesota energy utility customers.

[1] Minn. Stat. §§ 216B.04, 216B.09, 216B.23.

Establishing a CEUD Privacy Framework

We believe the Commission's authority over the reasonableness of utility service, as codified in Minn. Stat. §§ 216B.04, 216B.09, and 216B.23, supports the promulgation of either rules or a general policy regarding CEUD. Taking such action would be consistent with past Commission actions addressing the reasonableness of service, including safety (Minn. R. 7826.0300), reliability (Minn. R. 7826.0600), and service quality (*In the Matter of An Investigation and Audit of Northern States Power Company's Service Quality Reporting*, Docket No. E,G-002/CI-02-2034).

The framework we suggest the Commission establish would relate to all aspects of the CEUD lifecycle, namely: Notice, Collection and Use, Disclosure, and Access. Importantly, the privacy framework should be specific enough to act as a useful, substantive set of privacy protections, while also providing sufficient flexibility that allows individual utilities to develop and adapt their operations and processes to meet the framework. We believe the Commission could achieve this outcome through a General Order or through a Rulemaking. To the extent the Commission determines that its Order- or Rule-based framework needs further specificity, the Commission could require utilities to submit Tariffs that implement the Commission's CEUD framework.

The tariffs we suggest the Commission consider would complement a General Order or Rule, which differs from the Tariff we proposed in Docket No. E,G002/M-12-188. In that proceeding, we proposed a Customer Data Privacy Tariff to codify our privacy practices for *all* customer information categories. Parties expressed concern that substantive privacy protections in a tariff could potentially foreclose customer remedies. We appreciate these concerns, and believe filed rate doctrine and primary jurisdiction concerns would be mitigated by the inclusion of substantive protections in the form of a General Order or Rule that is focused in an area of privacy protections not otherwise addressed in law – providing customers an independent, non-tariff based source of privacy protection.

Table 2 provides an illustrative example of how an Order/Rule and Tariff option could work for elements associated with the CEUD lifecycle.

Table 2: Illustrative Example – General Order/Rule and Tariff Interplay

Topic	Potential Substantive Protection to be Adopted by Commission	Potential Implementation Measures for Tariff
Notice	Utilities must give customers annual notice of: • What information they collect; • How the information is used; • Customers' choices regarding their information; • How to access information; and • How to contact the utility with questions.	• Identify how the notice can be accessed by customers, the frequency and process for any updates and alternative formats or languages.
Collection and Use	By requesting service, customers consent to the collection and use of CEUD, but only for the purpose of providing that regulated service. If a utility wishes to collect or use CEUD for non-regulated purposes, then it must collect the customer's informed consent.	• Identify the process that the utility will use to obtain consent that incorporates the elements listed in the tariff.
Disclosure	A utility should not disclose a customer's CEUD unless: • the customer provides informed consent to the disclosure; or • the disclosure is to a Contracted Agent with a contract in place with the utility requiring privacy protections at least as strong as those used by the utility; or • such disclosure is required by law.	• Specify the process for obtaining customer consent to the release of CEUD; • Specify the process for subsequently revoking any previously granted consent; and • Identify how the customer may obtain information regarding its past consents.
Access	Customers must have access to their CEUD that is consistent with the regular provision of utility service.	• Identify how customers can access their CEUD. • Specify what level of access would be considered "regular" or provided without a charge. • Identify any options for obtaining specialized data reports with any associated cost.

Procedural Considerations

We believe it is essential to engage stakeholders in an open process that considers the perspectives and impacts on utilities, customers, regulators, and third parties seeking greater data access. As a first step, we believe the information sought in this Notice will be helpful to inform the scope, framework, and way-forward for such a proceeding. We also believe workshops and/or technical conferences involving all stakeholders are effective means of determining how certain issues impact different

stakeholders and could establish areas of potential consensus related to a privacy framework for CEUD.

However, there may also be circumstances in which it is more practical to task stakeholder sub-groups to work on specific issues. For example, the Commission may want to determine the utility impacts and costs involved in implementation of a "standard" CEUD practice that supports public policy goals. In this circumstance, a practical approach may be to task a utility stakeholder group to share and assess data capabilities across the utilities, and propose a common "standard," as well as outline any implementation considerations, such as information system implications and related costs. The Commission may then want this information brought to the broader workgroup for further development of a CEUD practice or policy, or alternatively back to the Commission for further action or guidance.

We discuss general policy measures or temporary moratoriums in our response to Question No. 3.

Combined Proceeding with Telecommunications

In these Comments, we suggest the Commission focus on creating a framework for access and use of CEUD, which is category of data that does not exist in the telecommunications industry. We also note that the electric industry is not similarly-situated to the telecommunications industry, in terms of privacy regulation. For example, the area of privacy regulations may be more developed in the telecommunications area, such as the development of law relating to CPNI (Customer Proprietary Network Information). A federal statute, 47 U.S.C. § 222, requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure. The FCC strengthened its privacy rules by adopting additional safeguards to protect customers' CPNI against unauthorized access and disclosure.[2]

Additionally, we believe combining disparate industries and stakeholders in a single docket would greatly complicate the proceeding, and impede timely resolution for both industries.

Codes of Conduct

Xcel Energy has established a comprehensive privacy policy that applies to all of its natural gas and electric customers, which is consistent with the intent behind recent

[2] *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services,* CC Docket No. 96-115, WC Docket No. 04-36, FCC 07-22, Released: April 2, 2007.

Department of Energy actions in this area.[3] Codes of Conduct in the area of data privacy can be helpful, as they may deliver the following benefits:

- Establish baseline privacy expectations for both customers and regulators – a baseline that could be used to measure a utility's or third party's subsequent performance and behaviors;
- Implement privacy protections in a precise, clear manner that is tailored to the operations of each utility or third party; and
- Create industry norms that help influence the behaviors of other, non-regulated entities that may have relationships with customers.

It is the public adoption of a privacy policy or code of conduct that also allows the FTC to regulate both utilities and third parties in areas of CEUD. A privacy policy or code of conduct is therefore an important vehicle for expanding the universe of entities reviewing any company's privacy practices.

While privacy policies and codes of conduct may deliver the benefits mentioned above, they do not resolve all privacy-related concerns, and may be more appropriate as an interim consideration while more robust privacy protections are being developed and implemented. Xcel Energy's Privacy Policy is available at http://www.xcelenergy.com/staticfiles/xe/Admin/Xcel%20Online%20Privacy%20Policy.pdf.

3. *Should the Commission enact or prohibit certain practices immediately; for example, prohibit the sale of customer data pending the outcome of this proceeding? What other practices should be encouraged or enacted immediately; for example, should the Commission require that all utilities receive informed, explicit customer consent before releasing customer data for any purpose other than that used in the ordinary course of utility service?*

Xcel Energy supports a full examination of the privacy issues related to collection, use and access to CEUD, and the establishment of related privacy principles for utilities. With the exception of affirming that CEUD cannot be sold, we believe that any general policy measures or temporary moratoriums adopted by the Commission on an interim basis should be carefully examined with input from stakeholders to ensure:

---

[3] *See* Smartgrid.gov, *U.S. Department of Energy Initiates Multistakeholder Process for Smart Grid Data Privacy*, http://www.smartgrid.gov/federal_initiatives/featured_initiatives/us_department_energy_initiates_multistakeholder_process_smart_grid_data_privacy (stating the Department of Energy "will facilitate a multi-stakeholder process to develop a Voluntary Code of Conduct (VCC) for utility and third parties providing consumer energy use services."). Xcel Energy has been an active participant in this initiative.

- Costs and operational impacts are understood, and there is path for utility cost recovery;
- Impacts on customers and authorized others that rely on customer information are understood and mitigated; and
- Unintended consequences are avoided.

Rather than temporary or immediate actions to address the areas of greatest concern to the Commission, another option for the Commission to consider would be to prioritize the issues, or use parallel paths to address multiple issues concurrently. We believe the structured and collaborative process we discussed in our response to Question No. 2 would also support either of these options.

One issue that we believe would benefit from a more immediate review is utility provision of aggregated data reports. Historically, Xcel Energy has provided municipalities, counties, and other government agencies with energy consumption reports. These reports are typically aggregated at a very high level (e.g. city, county, state, etc.) and support important public policy goals, such as benchmarking and measuring environmental initiatives. We receive similar requests for "whole building" data from building owners and managers, as well as for "neighborhoods" that seek to understand their carbon footprint or energy consumption.

A City of Minneapolis City Council Panel recently approved rules requiring an energy rating mandate for all commercial buildings larger than 50,000 square feet to submit their energy usage data to Energy Star for rating.[4] Action by the full City Council is scheduled for the week of February 4, 2013. Pending approval, we would expect Xcel Energy requests for "whole building" data to increase, to aid building owners' compliance with the mandate. As has already occurred, we expect issues of privacy to be triggered, as we consider the sufficient minimum level of aggregation for such reports, without informed customer consent. Any interim guidance or prioritized consideration the Commission can offer regarding a minimum level of aggregation would be helpful as we work with Minneapolis businesses to comply with, what seems to be, this likely City mandate.

4. *With the advent of 'smart grid' and increasing awareness of energy usage in general the presumption seems to be that there is a public interest to allowing greater access to customer energy usage data: do you agree? If so, what would be a reasonable balance between allowing greater access and protecting customers from the risk of identity theft or privacy intrusion?*

[4] *See* Minneapolis City Council Panel Passes Energy-Rating Mandate, Minneapolis Star Tribune (January 28, 2013), *available at* http://www.startribune.com/business/188767471.html?refer=y.

In determining the appropriate access requirements for CEUD, we believe it will be important for the Commission to balance the benefits of data access with customers' rights of privacy, independent of "smart grid" or any specific equipment that may enable greater data capabilities and information. Xcel Energy draws a distinction between different types of customer-specific data for purposes of this analysis, and in this response, discusses data access by parties other than our contracted agents, who provide service to our customers as an extension of regulated utility service.

CEUD presents different risks and access issues from Personal Data. First, while CEUD may provide some insight into certain activities involving energy usage, it does not present the same potential financial risks and cannot be used for the same type of fraudulent purposes as the customer's Personal Data. Second, unlike Personal Data, which can be obtained directly from a customer, often utility cooperation is needed to access CEUD.

We believe that customers benefit from access to their CEUD, and can use such access to better understand their consumption patterns and make informed decisions regarding energy use. Additionally, we recognize that third-party access to CEUD can also play an important role in advancing conservation efforts. For example, third-party providers in the energy efficiency services market are another resource for customers to gain education, participate in energy audits and purchase energy monitoring devices. We believe that the use of such information by third-parties should generally be allowed, if made contingent upon obtaining informed customer consent, and with the removal of potential ongoing liability for the utility once it affirms the customer's consent to release the data.[5]

As we touched on in our response to Question No. 3, aggregated energy usage data also has a role in supporting public policy initiatives and objectives. Aggregated data reports can help governmental or other entities benchmark and measure energy usage for purposes of supporting conservation or environmental initiatives and requirements. Additionally, aggregated energy usage data reports can inform building-level analysis of energy saving investments and efficiency programs. We recognize the importance of providing access to such information for purposes of setting local and national conservation and environmental goals, as well as measuring progress toward those goals.

There are, however, some issues that must be resolved with this type of information

[5] Both the California and Colorado Commissions have adopted explicit rule provisions providing for such liability limitations once the utility has performed its due diligence to validate the customer's consent. *See* 4 Colo. Regs. 723-3 Part 3, section 3026(g) *and* Cal. Pub. Util. Code, section 83809(f).

sharing, such as: (1) what level of aggregation will result in reports that are sufficiently anonymous; (2) who can request and receive such reports; (3) who pays for the costs associated with developing the information systems necessary to create the reports; and (4) the extent of the utility's liability for the data once the data is outside its control. For this reason, we have added this issue to the Commission's proposed list of issues outlined in Question No. 5.

5. *What issues should be include or excluded as to the scope of this proceeding? Possible issues include:*
    a) *Collection, handling, retention, purging of customer data;*
    b) *Validity and purpose, means to correct inaccuracies, customer access;*
    c) *Data use limitation, consumer profiling;*
    d) *Company privacy and security practices, enforcement mechanisms;*
    e) *Data ownership, inferred asset transfer value to third parties;*
    f) *Cost causation, pricing for data requests (if allowed);*
    g) *Auditing and accountability, internal and external oversight;*
    h) *Risk assessment, corrective measures, proactive prevention to guard against misuse;*
    i) *Liability and indemnification, responsibility for unauthorized use, customer redress.*

    Should any of the items listed above be excluded? Why?

We generally support the list outlined in Question No. 5, and as we asserted earlier, that any framework the Commission establishes must allow for individual utility differences and flexibility in implementing and meeting the requirements. Specifically, we believe the issue of data ownership (item e) is secondary to the issues of access and use when establishing a privacy framework around CEUD. Additionally, as noted in our response to Question Nos. 3 and 4, we believe that the Commission will need to consider questions related to the utility's creation and provision of aggregated data reports.

6. *Are there whitepapers, federal guidelines or other state proceedings that have addressed the topics identified in Question No. 5, which should be incorporated into this docket or possible rulemaking?*

Yes. We provide as Attachment B, a list of resources that may be helpful in the Commission's consideration of the issues raised in this Notice.

CONCLUSION

We appreciate the opportunity to respond to the Commission's Notice, and look forward to working together with interested parties and the Commission to develop clear "rules of the road" regarding the important issue of customer data privacy. We believe that providing appropriate access to customer usage data is in the public interest – and that a reasonable balance between data access and customer privacy can be achieved.

We believe it is appropriate for the Commission to focus on creating a general framework for access and use of customer energy usage data applicable to all energy utilities. We support a practical approach that facilitates constructive dialogue, provides flexibility within a framework, achieves timely resolution, addresses costs, and balances privacy interests with public policy objectives dependent on reasonable access to data.

Dated: January 30, 2013

Northern States Power Company

Respectfully submitted by:

/s/

CHRISTOPHER B. CLARK
REGIONAL VICE PRESIDENT
RATES AND REGULATORY AFFAIRS

Discussion: **Relevant Sources of Protection by Customer Information Category**

The following represents a high-level discussion of current Minnesota and Federal law that applies to customer information possessed by utilities. These laws typically apply to specific data types; we have therefore organized our overview into the three categories of customer information described in our response to Question No. 1 of the Commission's Notice: (1) Personal Data; (2) Account Data; and (3) Customer Energy Usage Data (CEUD).

A. Personal Data

At Xcel Energy, we ask customers to provide Personal Data as part of the set-up of their account. This information is consistent with the definition of "Personal Information" under Minnesota law.[1] Specifically, we ask customers to provide us with their Social Security Number (SSN) and bank account number. The provision of both of these pieces of information is voluntary.

This section will discuss the various legal protections for this type of customer-specific information under Minnesota and Federal law.

1. Data Breach

An important obligation for any company collecting Personal Data in Minnesota is to provide notice to impacted individuals in the event of a data breach. The phrase "data breach" is a statutory term describing a specific type of data incident, namely the unauthorized access to personal information.[2] When a data breach occurs, the company maintaining the protected information is required to provide notice to the affected individuals.[3] The Minnesota Attorney General is authorized by statute to bring enforcement actions against companies that violate Minnesota's data breach statute, and affected individuals may bring their own private suits.[4] Minnesota's data breach statute forces companies to implement steps to prevent unauthorized access to personal information.

---

[1] Minn. Stat. § 325E.61, subd. 1 (e).
[2] Minn. Stat. §§ 325E.61, subd. 1 (d) (defining "breach of the security of the system," to mean "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business).
[3] Minn. Stat. § 325E.61, subd. 1 (b).
[4] Minn. Stat. §§ 325E.61, subd. 6. (citing Attorney General's investigation and enforcement power under Minn. Stat. § 8.31); 8.31, subd. 3a (private right of action).

2. Social Security Numbers

An SSN is a specific type of data that receives specialized protection under Minnesota law. While Minnesota's data breach statute indirectly protects Personal Data through threatened enforcement and civil lawsuits, Minnesota's SSN law directly imposes privacy protections for this data. For example, Minnesota law prohibits the following actions relating to SSNs:

- Publicly post or display SSNs;
- Include SSNs on identification or access cards;
- Transmission of unencrypted SSNs over an unsecured Internet connection;
- Requiring an individual to use a SSN to access a website unless a password or unique personal identification number or other authentication device is also required to access the website;
- Include SSNs in mailed materials unless required to do so by law;
- Use SSNs as account numbers except in conjunction with an employee or member retirement or benefit plan or human resource or payroll administration; or
- Sell SSNs obtained from individuals in the course of business.[5]

Minnesota law also requires companies to limit employees' access to SSNs to those with a legitimate business need to know such information.[6]

3. FTC and MN OAG Enforcement Actions

As discussed above, the Attorney General is authorized to enforce Minnesota's data breach statute. This power complements the Attorney General's general power to investigate and prosecute unlawful, unfair, and discriminatory business practices.[7] Recently, this power has been used to pursue actions against a Minnesota company that failed to reasonably protect Personal Data in its possession.[8] Federal regulators have similar authority to prevent unfair business practices,[9] and have used this power

[5] Minn. Stat. § 325E.59, subd. 1 (a)(1)–(7).
[6] Minn. Stat. § 325E.59, subd. 1 (d).
[7] Minn. Stat. § 8.31.
[8] *See* The Office of the Attorney General, *Attorney General Swanson Sues Accretive Health for Patient Privacy Violations* (Jan. 19, 2012) (reporting a lawsuit brought by the Minnesota Attorney General under, among other statutes, Minn. Statute § 8.31 over a data breach caused by a stolen, unencrypted laptop that revealed personal health information of about 23,500 hospital patients), *available at* http://www.ag.state.mn.us/Consumer/PressRelease/120119AccretiveHealth.asp.
[9] 15 U.S.C. § 45(a).

to punish companies that do not comply with their stated privacy protections.[10] While these enforcement actions do not impose any substantive privacy requirements on non-offending companies, they do work to incentivize businesses to protect data and provide guidance consistent with regulators' expectations.

4. Payment Card Information Data Security Standard (PCI DSS)

In addition to government actions, certain private actors have used their market power to implement protections for Personal Data. American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. all require participating merchants to adopt the PCI DSS requirements. These requirements are designed "to help organizations ensure the safe handling of cardholder information at every step."[11] According to the Payment Card Industry Security Standards Counsel, "[t]he keystone [of its program] is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process – including prevention, detection and appropriate reaction to security incidents."[12]

5. Potential Private Actions

Minnesota law provides for private actions against companies that violate the data breach statute.[13] Based on the facts and circumstances of a specific case, an affected individual may also be able to bring a private suit for a data incident involving Personal Data that is not covered by the data breach statute.[14] Like regulatory enforcement actions, private suits act as an incentive for companies to adopt proactive privacy measures.

---

[10] *See, e.g., In re TJX Companies, Inc.*, FTC Docket No. C-4227 (2008), *available at* http://www.ftc.gov/os/caselist/0723055/index.shtm; *FTC v. Wyndham Worldwide Corp.*, No. 12-cv-01365-SPL (D. Az. 2012), *available at* http://ftc.gov/os/caselist/1023142/120626wyndamhotelscmpt.pdf; *In re SettlementOne Credit Corp.*, FTC Docket No. C-4330 (2011), *available at* http://www.ftc.gov/os/caselist/0823208/index.shtm. Companies that have settled with the FTC have agreed to implement comprehensive information security programs, undergo annual independent data security assessments, and paid civil fines.

[11] PCI Security Standards Counsel, *PCI SSC Data Security Standards Overview*, https://www.pcisecuritystandards.org/security_standards/index.php.

[12] *Id.*

[13] Minn. Stat. § 8.31, subd. 3a.

[14] *See Lake v. Wal-Mart Stores, Inc.*, 582 N.W. 2d 231 (Minn. 1998) (recognizing cause of action for privacy torts). *See also Bodah v. Lakeville Motor Express, Inc.*, 663 N.W. 2d 550, 556 n.5 (Minn. 2003); *Yath v. Fairview Clinics, N.P.*, 767 N.W. 2d 34, 46 (Minn. Ct. App. 2009).

6. Identity Theft

Identity theft is a statutorily-defined crime relating to the use of an identity for unlawful activity.[15] Both Personal Data and Account Data (discussed below) held by the Company (or any utility) could theoretically be used to commit the crime of identity theft.[16] By statute, the person who commits the crime of identity theft is the responsible party and is subject to both penalties and restitution.[17] Criminalizing identity theft lends further protection to Personal Data by deterring direct wrongdoers and by forcing businesses to implement safeguards against identity theft in order to avoid aiding and abetting liability.[18]

B. Account Data

In addition to Personal Data, Xcel Energy also collects other individually-identifiable information from customers, such as phone numbers, email addresses, etc. While this information is unique to the customer, it does not come within the definition of "Personal Information" under Minnesota statute, and does not have the same potential risk of identity theft. For this reason, we distinguish this type of data from Personal Data, and call it "Account Data."

Account Data is increasingly seen as a category of customer information that requires some level of privacy protection. As one's electronic identity becomes a larger part of a person's overall interaction with the commercial world, information like email addresses and cell phone numbers have gained heightened attention from regulators. For example, the FTC has brought enforcement actions against companies for failing to protect email addresses and social network accounts.[19] At the same time, there is no direct statutory or regulatory duty to adopt substantive privacy protections for Account Data. However, given the recent enforcement actions, we anticipate that this

---

[15] Minn. Stat. § 609.527, subd. 2.

[16] Minn. Stat. § 609.527, subd. 1 (d) (defining an identity as "any name, number, or data transmission that may be used, alone or in conjunction with any other information, to identify a specific individual or entity, including any of the following: (1) a name, Social Security number, date of birth, official government-issued driver's license or identification number, government passport number, or employer or taxpayer identification number; (2) unique electronic identification number, address, account number, or routing code; or (3) telecommunication identification information or access device.").

[17] Minn. Stat. § 609.527, subds. 3 and 4.

[18] *See* Minn. Stat. § 609.05, subd. 1.

[19] *See. e.g.*, *In re CBR Systems, Inc.*, FTC File No. 112 3120 (2013), http://www.ftc.gov/opa/2013/01/cbr.shtm (citing company for failing to protect several types of customer information, including email addresses); *In re Twitter, Inc.*, FTC File No. 092 3093 (2011), http://www.ftc.gov/opa/2011/03/twitter.shtm (Twitter accounts); *In re Facebook, Inc.*, FTC File No. 092 3184 (2011), http://www.ftc.gov/opa/2011/11/privacysettlement.shtm (Facebook accounts).

data type will likely be further regulated at the federal and state level. For this reason, and because this information type is not unique to utility customers, we believe that the Commission should avoid creating potentially conflicting regulations, and instead monitor developments in this area.

C. Customer Energy Usage Data

There is a growing consensus that customer-specific energy usage data (CEUD), especially when collected in frequent intervals, is entitled to some level of privacy protection.[20] While this issue has more commonly been associated with the use of so-called smart meters or smart grid technology, the associated privacy concerns are not technology-dependent, and are not specific to electric utility operations. Xcel Energy utilizes different types of metering equipment for its natural gas and electric operations across its service areas, but from a privacy perspective, we treat all CEUD the same.

Currently, there is very little if any statutory or regulatory protection for CEUD in Minnesota.[21] While one could argue that all utilities must protect CEUD (and all customer information) as part of their duty to provide reasonable service,[22] neither the Commission nor any Minnesota court has provided sufficient guidance on the topic. As with Personal Data and Account Data, there may be factual circumstances where unauthorized access or disclosure of CEUD could support a private cause of action, though we note that we are unaware of any such example as of this date. The most substantive protection of CEUD that we are aware of in Minnesota to date, is our own privacy policy, which can be enforced by the FTC because it is publically available.

---

[20] U.S. Department of Energy, *Data Access and Privacy Issues of Smart Grid Technologies* at 1–3 (Oct. 5, 2010), *available at* http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf.

[21] Other states have developed regulations for CEUD. *See* Okla. Stat. tit. 17, §§ 710.1 et seq; 4 Colo. Code Regs. §§ 723-3026 et seq; *Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company*, California Public Utilities Commission Docket No. 08-12-009, DECISION 11-07-056 (July 28, 2011), *available at* http://docs.cpuc.ca.gov/word_pdf/FINAL_DECISION/140369.pdf.

[22] Minn. Stat. § 216B.04.

6. *Are there whitepapers, federal guidelines or other state proceedings that have addressed the topics identified in Question No. 5, which should be incorporated into this docket or possible rulemaking?*

State Proceedings or Tariffs

Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's Own Motion to Actively Guide Policy in California's Development of a Smart Grid System, California Public Utilities Commission Docket No. 08-12-009 (Dec. 18, 2008), *available at* http://docs.cpuc.ca.gov/word_pdf/FINAL_DECISION/95608.pdf.

Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company, California Public Utilities Commission Docket No. 08-12-009, Decision 11-07-056 (July 28, 2011), *available at* http://docs.cpuc.ca.gov/word_pdf/FINAL_DECISION/140369.pdf.

Reply Comments of the Center for Democracy & Technology to Assigned Commissioner's Ruling of September 27, 2010, California Public Utilities Commission Docket No. 08-12-009 (Nov. 8, 2010), *available at* http://docs.cpuc.ca.gov/efile/CM/126209.pdf.

In the Matter of the Proposed Rules Relating to Smart Grid Data Privacy for Electric Utilities, 4 Code of Colorado Regulations 723-3, Colorado Public Utilities Commission Docket No. 10R-799E, Decision C11-1144, ORDER ON EXCEPTIONS (Oct. 26, 2011), *available at* http://www.dora.state.co.us/pls/efi/efi_p2_v2_demo.show_document?p_dms_document_id=134683&p_session_id=.

Staff Report, Michigan Public Service Commission, Docket No. U-17000 (June 29, 2012) *available at* http://efile.mpsc.state.mi.us/efile/docs/17000/0455.pdf.

Oklahoma Electric Utility Data Protection Act, *available at* http://www.oklegislature.gov/cf_pdf/2011-12%20ENR/hb/hb1079%20enr.pdf and codified at Okla. Stat. tit. 17, §§ 710.1 et seq.

Oklahoma Gas & Electric Company, Terms and Conditions of Service, Part II, Section 218, *Ownership and Use of Smart Meter Data* (July 19, 2012), *available at* http://www.oge.com/Documents/OK/100%20Terms%20and%20Conditons.pdf.

DOE Reports

U.S Department of Energy, *Data Access and Privacy Issues of Smart Grid Technologies* (Oct. 5, 2010), *available at* http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf.

U.S. Department of Energy, *Smart Grid Privacy Workshop Summary Report* (January 31, 2012) *available at* www.smartgrid.gov/document/us_department_energy_smart_grid_privacy_workshop_summary_report.

FTC Guidance

Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

Federal Trade Commission, *Fair Information Practice Principles*, *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

White Papers

National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid* (Aug. 2010), *available at* http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

North American Energy Standards Board, NAESB REQ.22, *available at* http://www.naesb.org/retail_request.asp

Information and Privacy Commissioner of Ontario, Canada, *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid* (June 2010), *available at* http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf.

Information and Privacy Commissioner of Ontario, Canada and Future of Privacy Forum, *Privacy by Design and Third Party Access to Customer Energy Usage Data* (January 2013), *available at* http://privacybydesign.ca/content/uploads/2013/01/pbd-thirdparty-CEUD.pdf.

State & Local Energy Efficiency Action Network, *A Regulator's Privacy Guide to Third-Party Data Access for Energy Efficiency* (December 2012), *available at* http://www1.eere.energy.gov/seeaction/pdfs/cib_regulator_privacy_guide.pdf.

Vermont Law School Institute for Energy and the Environment, *A Model Privacy Policy for Smart Grid Data* (Nov. 4, 2011), *available at* http://www.vermontlaw.edu/Documents/Model%20Privacy%20Policy%20_%20APPA%20Legal%20Seminar%202011%20%5Bfinal%20draft%5D.pdf.

Codes of Conduct

Future of Privacy Forum and TRUSTe Smart Grid Privacy Seal Program, *available at* http://www.futureofprivacy.org/issues/smart-grid/.

CERTIFICATE OF SERVICE

I, SaGonna Thompson, hereby certify that I have this day served copies or summaries of the foregoing document on the attached list of persons.

xx by depositing a true and correct copy thereof, properly enveloped with postage paid in the United States Mail at Minneapolis, Minnesota

xx electronic filing

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

Dated this 30th day of January 2013

/s/

SaGonna Thompson

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Tamie A.	Aberle	tamie.aberle@mdu.com	Great Plains Natural Gas Co.	400 North Fourth Street Bismarck, ND 585014092	Paper Service	No	SPL_SL_12-1344_Interested Parties
Julia	Anderson	Julia.Anderson@ag.state.mn.us	Office of the Attorney General-DOC	1800 BRM Tower 445 Minnesota St St. Paul, MN 551012134	Electronic Service	Yes	SPL_SL_12-1344_Interested Parties
Scott	Bohler	scott.bohler@ftr.com	Frontier Communications Corporation	2378 Wilshire Blvd Mound, MN 55364-1652	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Cesar	Caballero	Cesar.Caballero@windstream.com	McLeodUSA Telecommunications Services, LLC	4001 Rodney Parham Little Rock, AR 72212	Paper Service	No	SPL_SL_12-1344_Interested Parties
Brent	Christensen	bchristensen@mnta.org	Minnesota Telecom Alliance	1000 Westgate Drive, Ste 252 St. Paul, MN 55117	Electronic Service	No	SPL_SL_12-1344_Interested Parties
James R	Denniston	james.r.denniston@xcelenergy.com	Xcel Energy	414 Nicollet Mall 5th Floor Minneapolis, MN 55401	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Ian	Dobson	ian.dobson@ag.state.mn.us	Office of the Attorney General-RUD	1400 Bremer Tower 445 Minnesota Street St. Paul, MN 55101	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Sharon	Ferguson	sharon.ferguson@state.mn.us	Department of Commerce	85 7th Place E Ste 500 Saint Paul, MN 551012198	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Burl W.	Haar	burl.haar@state.mn.us	Public Utilities Commission	Suite 350 121 7th Place East St. Paul, MN 551012147	Electronic Service	Yes	SPL_SL_12-1344_Interested Parties
Jim	Hawley	jhawley@technet.org	Technology Network (TechNet)	1215 K Street, Suite 1900 Sacramento, California 95818	Paper Service	No	SPL_SL_12-1344_Interested Parties

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Nikki	Kupser	nkupser@greatermngas.com	Greater Minnesota Gas, Inc.	202 South Main Street P.O. Box 68 Le Sueur, MN 56058	Paper Service	No	SPL_SL_12-1344_Interested Parties
Douglas	Larson	dlarson@dakotaelectric.com	Dakota Electric Association	4300 220th St W Farmington, MN 55024	Electronic Service	No	SPL_SL_12-1344_Interested Parties
John	Lindell	agorud.ecf@ag.state.mn.us	Office of the Attorney General-RUD	1400 BRM Tower 445 Minnesota St St. Paul, MN 551012130	Electronic Service	Yes	SPL_SL_12-1344_Interested Parties
David	Moeller	dmoeller@allete.com	Minnesota Power	30 W Superior St Duluth, MN 558022093	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Andrew	Moratzka	apm@mcmlaw.com	Mackall, Crounse and Moore	1400 AT&T Tower 901 Marquette Ave Minneapolis, MN 55402	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Richard	Savelkoul	rsavelkoul@martinsquires.com	Martin & Squires, P.A.	444 Cedar St Ste 2050 St. Paul, MN 55101	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Kevin	Saville	KSaville@czn.com	Citizens Telecommunications Company of MN,LLC	2378 Wilshire Blvd Mound, MN 55364	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Peggy	Sorum	peggy.sorum@centerpointenergy.com	CenterPoint Energy	800 LaSalle Avenue PO Box 59038 Minneapolis, MN 554590038	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Ron	Spangler, Jr.	rlspangler@otpco.com	Otter Tail Power Company	215 So. Cascade St. PO Box 496 Fergus Falls, MN 565380496	Electronic Service	No	SPL_SL_12-1344_Interested Parties
SaGonna	Thompson	Regulatory.Records@xcelenergy.com	Xcel Energy	414 Nicollet Mall FL 7 Minneapolis, MN 554011993	Electronic Service	No	SPL_SL_12-1344_Interested Parties

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Jason	Topp	jason.topp@centurylink.com	CenturyLink	200 S 5th St Ste 2200 Minneapolis, MN 55402	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Gregory	Walters	gjwalters@minnesotaenergyresources.com	Minnesota Energy Resources Corporation	3460 Technology Dr. NW Rochester, MN 55901	Paper Service	No	SPL_SL_12-1344_Interested Parties
Robyn	Woeste	robynwoeste@alliantenergy.com	Interstate Power and Light Company	200 First St SE Cedar Rapids, IA 52401	Paper Service	No	SPL_SL_12-1344_Interested Parties