Privacy Protections for Consumer Information Held by Minnesota Rate Regulated Utilities

Prepared by:

Roger D. Colton
Fisher, Sheehan and Colton
Public Finance and General Economics
34 Warwick Road * Belmont, MA 02478**

January 30, 2013

---

1. **Do current service standards provide adequate customer data privacy protection and redress for customers in the event of a 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?**

Minnesota utilities should be "liable" for providing specified consumer protections in the event of a data breach rather than having liability exclusively directed toward providing compensation for "damages."[1] Liability should not be limited to the "event of a stolen identity." Nor should liability be limited to the demonstration of a "financial harm" to customers. No current service standards provide adequate customer data privacy redress in the event of a breach.[2]

[1] The scope of the question posed by the Commission limits the issue of liability to one of liability "to customers." We thus set aside the growing body of law that allows ***businesses*** who suffer financial harm to collect compensation. Thus, for example, if a retail store incurs expenses due to a data breach by a local utility, whether in improperly granted credit or because of the need to close compromised accounts and reopen new ones, the extent to which such stores might be owed compensation is set aside.

[2] Whether consumers may gain redress or compensation for damages, direct or indirect, financial or non-financial, associated with the release of personally identifiable information under statutory or common law provisions unrelated to Commission jurisdiction is set aside as not relevant to this proceeding.

Minnesota utility liability for data breaches should not be limited to instances where a consumer can demonstrate a "stolen identity." The inability to draw a reasonable nexus between specific data breaches of personally identifiable information (PII) and stolen identities has been repeatedly documented. Damages from stolen identity do not arise immediately upon experiencing a data breach. There may well be a substantial lapse of time before the information is used to generate a stolen identity. Moreover, even after identity theft occurs, a consumer may not become immediately aware of it. Instead, consumers may not become aware of their plummeting credit rating unless and until they apply for new or additional credit. According to one study by the federal General Accounting Office (GAO):

> law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[3]

Even when identity theft occurs, neither consumers nor government authorities may be able to associate it with a specific data breach by a public utility. A consumer is more likely to contact the bank or credit card issuer (for example) who holds the account that has been compromised rather than contacting the utility who experienced the data breach with which to begin. In addition, identity theft is not always identified as a stand-alone "crime" resulting in harm to the consumer, "but rather a component of one or more complex crimes, such as computer fraud, credit card fraud, or mail fraud. For example, with the theft of identity information, a perpetrator may commit computer fraud when using a stolen identity to fraudulently obtain credit on the

[3] GAO (June 2007). "Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown," at 28 – 29.

Internet."[4] The focus of enforcement, in other words, is on the fraud, not on the underlying data breach which enabled the fraud.

Nor should Minnesota utility liability be limited to instances where "***financial*** harm to consumers" (emphasis added) can be demonstrated. Aside from the difficulty in proving financial harms, and in relating those financial harms to specific data breaches, harms to consumers from data breaches can be both financial and non-financial, both direct and indirect. For example, one harm to consumers that is direct but ***non***-financial involves simply the hours needed to respond to the identity theft. In 2006, victims spent, on average, 40 hours responding to the theft of their identity; 10% of victims spent more than 100 hours. In addition, consumers may experience harassment by consumer credit agencies, collection agencies, retail stores or credit card issuers. They may be called upon to respond to civil and criminal judicial proceedings. These direct, albeit non-financial, harms are above and beyond the indirect harms of the anxiety, embarrassment and humiliation associated with the identity theft.

While utility liability for data breaches should not be limited by direct financial harm or a documentation of resultant identity theft, Minnesota utilities ***should*** be liable for providing specific consumer protections in the event of a data breach. More specifically, in the event of a data breach, utilities should fund both consumer notification of data breaches and the offer of consumer credit counseling monitoring. The first utility liability should be to provide notification in the event of a data breach. When information holders experience a data breach, both the incidence of identity theft and the extent of harms arising from such identity theft are "significantly smaller" if the data breach is discovered quickly.[5]

[4] GAO (2009). "Identity Theft: Governments Have Acted to Protect Personally Identifiable Information but Vulnerabilities Remain," at 6.
[5] Federal Trade Commission (June 16, 2005). "Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft," at 10.

Notification of data breaches serves several functions, thus justifying the imposition on utilities of liability for providing such notification:

- Requiring breach notification incentivizes security on the part of utilities, either to minimize legal liability or to minimize the public relations risk associated with the breach;
- Requiring breach notification alerts consumers to a breach and warns them to take the actions necessary to prevent or mitigate identity theft. Consumers may, for example, cancel credit cards. They may, in the alternative, simply monitor credit card statements and bank statements. They may order credit reports.
- Requiring breach notification mitigates the potential risk of resulting identity theft. The notification deters any resulting identity theft by making it clear that the breach has been identified and investigated and that affected consumer accounts will be monitored.

Finally, in addition to these affirmative functions served by data breach notification, consumers have a fundamental right to know when their personal information has been compromised.

In addition to liability for providing data breach notification, utilities should be liable for providing supportive consumer services when data breaches represent a significant risk of identity theft. The primary consumer service should involve the provision of consumer credit monitoring counseling. As the source of the data breach, the utility should be the source of the service to help minimize any potential identity theft that might occur, as well as to prevent or minimize the financial costs to consumers resulting therefrom.

Seeking to impose liability for compensation to consumers for their direct financial harms is difficult, if not impossible, to fully accomplish in the event of a data breach. Limiting compensation only to “financial harm” would be too narrow in any event. Moreover, limiting

compensation only to "customers" would be inappropriate. LSAP urges an imposition of "liability," but one not directed toward "compensation"[6] but rather to the provision of specified consumer protections. Data breach notification is the first such consumer protection. Providing consumer credit monitoring services when a data breach represents a significant threat of identity theft is a second such service the cost of which should be borne by utilities.[7]

Beyond these steps, LSAP recommends additional actions that Minnesota utilities should be required to undertake with respect to privacy and consumer information, as set forth in response to the Commission's Question No. 3 below.

---

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?**

[6] But see, note 2, supra.
[7] These costs should be borne by utilities, and not utility ratepayers. The expense incurred to perform functions served by these two tasks should, in other words, be borne by those who are most able to develop reasonable mechanisms to prevent the need for the tasks in the first instance. Those functions would be impeded if the costs were simply passed-through to ratepayers.

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?

LSAP does not recommend that the Commission establish uniform customer data collection and privacy policies for rate regulated utilities. Instead of such a "uniform" approach, the recommendation advanced by LSAP is set forth in response to Commission Question No. 3 below.[8] LSAP recommends that the action it proposes below be applicable to all types of rate-regulated utilities, including energy utilities, telecommunication utilities, and water/wastewater utilities.

Given the LSAP recommendation below, no privacy tariff is required. No rulemaking is required. While technical workshops might be merited as educational, given the available guidance and models that are available in the public domain, such technical workshops would not be essential to decision-making.

LSAP does not recommend uniform data collection and privacy policies because the propriety and reasonableness of privacy actions depends on a host of utility-specific factors that will virtually certainly differ between utilities. The reasonableness and adequacy of data collection and privacy protection actions by each utility will depend on factors such as what information is collected; what types of systems are used to retain such data; to what extent does the utility out-source (in whole or part) services; how large is the utility; and what risks are presented by the collection and retention of data by the utility. Particular problems are presented by downstream out-sourcing; even more substantial problems are presented by down-stream, off-shore out-sourcing.

[8] In addition, issues specific to Smart Meter technology are separately addressed in response to Question 4 below.

Rather than imposing uniform data collection and privacy policies, LSAP recommends that the Commission focus on mandating the ***processes*** discussed below that would generate appropriate data collection and privacy policies. As each utility files its privacy plans (e.g., Red Flags Rule plan, PIA, ISP), the Commission can address specific questions posed by the specific utilities in separate proceedings. It is difficult, however, if not impossible, to comprehensively resolve such issues for all utilities in the abstract only on a policy-level basis.

LSAP agrees with the Commission that the Federal Trade Commission (FTC) has authority over public utility treatment of privacy issues pursuant to Section 5 of the Federal Trade Commission Act (15 USC §45). Indeed, the FTC can assert (and has asserted) authority under either component of Section 5: (1) "unfair" trade practices; and (2) "deceptive" trade practices. As the FTC has made clear with respect to "unfair" trade practices, asserting jurisdiction over companies that have failed to employ reasonable and appropriate measures to secure personal information is based on the philosophy that if a company is collecting information, it has a duty to protect the information collected.[9] As one commentator noted, "the FTC is certainly not trying to play "gotcha" on single security infractions or failures and is looking at the totality of the situation. . ."[10] The commentator continued on to observe that the FTC:

> has identified a select group of basic level protections that should be in place. It has characterized these as "reasonable and appropriate" protections. Typical

[9] FTC Chair Deborah Platt Majoras made numerous statements in connection with FTC enforcement actions indicating that companies have a duty to protect information they collect. *See* Press Release, *BJ'S Wholesale Club Settles FTC Charges* (June 16, 2005), *available at* http:// www.ftc.gov/opa/2005/06/bjswholesale.htm ("Consumers must have the confidence that companies that possess their confidential information will handle it with due care and appropriately provide for its security"); Press Release, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm ("Consumers' private data must be protected from thieves ... Data security is critical to consumers, and protecting it is a priority for the FTC, as it should be to every business in America."); Press Release, *CardSystems Solutions Settles FTC Charges* (Feb. 23, 2006), *available at* http://www.ftc.gov/opa/2006/02/cardsystems_r.htm ("Any company that keeps sensitive consumer information must take steps to ensure that the data is held in a secure manner.").

[10] Soloway and Covington, "Data Privacy and Security: Recent Developments Affecting Consumer Finance," 62 Bus.Law 631, 642 (2007).

> violations are as follows: (i) the failure to encrypt data while in transmission; (ii) a failure to use readily available security measures to protect wireless networks; (iii) the failure to have adequate passwords; (iv) the unnecessary storage of documents and records; (v) failure to have sufficient measures to detect unauthorized access; and (vi) not adequately assessing vulnerabilities for commonly known or foreseeable risks to data security. Thus, the message is that, at the very least, every security program should employ protections to address these concerns.[11]

The commentary above illustrates why LSAP believes that trying to mandate uniform practices and procedures would not only be inappropriate, but inadequate as well. Factors will differ by utility. What represents the "unnecessary" storage of documents and records will likely differ by utility. What represents "sufficient" measures to detect unauthorized access will differ. What represents "foreseeable" risks to data security will differ. Indeed, the types and amounts of information collected along with the types of systems in which that consumer information is retained will likely differ by company.

Aside from the FTC treatment of "unfair" trade practices, the FTC has also asserted its authority to control "deceptive" practices relating to data protection. A company engages in a deceptive practice if it fails to undertake the privacy protection and data security measures it has stated that it undertakes. In addition, a company engages in deceptive practices if it uses consumer information for purposes other than what its stated use was at the time of data collection. One primary basis for this control of deceptive practices is grounded in the notion of consumer sovereignty. One basic principle of consumer privacy is that a consumer should be told of the uses to which his/her information will be devoted and, in light of those uses, given the opportunity to choose whether to provide their information. If, however, information has been collected for one stated purpose, to which the consumer has agreed, but is then used for a

[11] Id, at 643 – 644 (internal citations omitted).

different purpose, the principle of consumer choice has been undermined. Under the FTC's authority to control "deceptive" practices, a company, therefore, may represent neither that it has certain privacy controls which, in fact, it lacks, nor represent that data collection is in furtherance of one stated purpose when, in fact, the data collection is used for a different purpose.

The FTC's authority over data protection and the privacy of consumer information – whether under the "unfair" trade practices rubric or under the "deceptive" trade practice rubric—of course does not depend on the Commission's affirmative recognition or acknowledgement of that FTC authority. Instead, the FTC's federal authority exists and can be exercised independently of any Commission action.

The role of the Commission is actually the opposite of that which appears to be implied in the Request for Comments. The Commission should hold that actions deemed by the Federal Trade Commission (or corresponding state laws and regulations) to be an "unfair" or a "deceptive" trade practice will, *a priori*, *also* be considered to be not "just and reasonable" under the Commission's utility regulatory authority. This incorporates the simple proposition that an "unfair" and/or "deceptive" trade practice is, by definition, neither just nor reasonable under utility regulatory principles.

---

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?

LSAP urges the Commission to take the following three specific actions relative to the collection and protection of personal information by Minnesota utilities:

First, the Commission should issue data requests, including docketing a proceeding if necessary, to ensure that Minnesota utilities have adequately and appropriately adopted Red Flags Rule plans pursuant to the Federal Fair and Accurate Credit Transactions Act (FACTA). Under the Red Flags Rule, promulgated by the FTC pursuant to FACTA, any business that is a "creditor" (as defined by the statute) must promulgate a Red Flags Plan. Under the statute and accompanying regulations, each Red Flags Plan is required to have four specific components:

- List specific indicators of risk ("red flags") commonly applicable to the company promulgating the plan;
- Create policies and procedures that will identify the risks identified by those Red Flags;
- Explain how the company will act to detect those risks; and
- Develop appropriate responses to all red flags, with the responses proportionate to the risks.

Under the Red Flags Rule, each utility –utilities are specifically considered to be "creditors" under the Red Flags Rule—is to have both a detection plan element and a response plan element in their Red Flags Plan. Moreover, under the Red Flags Rule, each utility is to undertake an annual evaluation of the effectiveness of its Red Flags Plan. Finally, under the Red Flags Rule, each utility must ensure that vendors using or having access to covered accounts,[12] in turn, must also have their ***own*** Red Flags Plans.

Second, the Commission should require each Minnesota utility to prepare and make public a Utility Privacy Impact Assessment (UPIA). The UPIA requirement should be modeled on the

[12] A "covered account" is a term defined by statute. It clearly extends to all utility customer accounts.

Privacy Impact Assessment (PIA) requirements imposed on federal agencies by the E-Government Act of 2002 (Section 208). The U.S. Department of Homeland Security describes a PIA as follows: "A PIA is a decision-making tool used to identify and mitigate privacy risks at the beginning of and through the development life cycle of a program or system. It helps the pubic understand what [personally identifiable information] the Department is collecting, why it is being collected, and how it will be used, shared, accessed and stored." A PIA is to cover the ***disposal*** of PII as well.

> GAO describes the federally-required PIA as follows:
>
> The E-Government Act of 2002 strives to enhance protection for personal information in government information systems by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to OMB guidance,[13] a PIA is an analysis of how information is handled (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
>
> Agencies must conduct PIAs (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form, or (2) before initiating any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. OMB guidance also requires agencies to conduct PIAs when a system change creates new privacy risks, for example, changing the way in which personal information is being used.[14]

[13]OMB, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," M-03-22 (Sept. 26, 2003). Multiple OMB guidelines have been issued on information privacy.
[14] GAO (January 2008). "Information Security: Protecting Personally Identifiable Information," at 9 - 10; see also, GAO (May 2008). "Privacy: Agencies Should Ensure that Designated Senior Officials Have Oversight of Key Functions," at 4 – 5.

GAO has testified to Congress:

> It is important that agencies identify the specific instances in which they collect and maintain personal information and proactively assess the means they intend to use to protect this information. This can be done most effectively through the development of PIAs, which. . .are required by the E-Government Act of 2002 when using information technology to process personal information. PIAs are important because they serve as a tool for agencies to fully consider privacy implications of planned systems and data collections before those systems and collections have been fully implemented, when it may be relatively easy to make critical adjustments.[15]

The rationale for preparing PIAs is as applicable to public utilities, if not more so, as it is to federal agencies.[16] LSAP is not asserting that the statutory PIA requirements of the E-Government Act are applicable to Minnesota public utilities. LSAP, however, *is* asserting that the PIA process offers as much benefit to Minnesota utilities as it does to federal agencies; that Minnesota utilities could draw substantive guidance on the promulgation of UPIAs from the manner in which the PIA requirement has been implemented at the federal level,[17] and that the promulgation of UPIAs should be required by the Commission.

Third, the Commission should require each Minnesota utility to adopt an information security plan modeled on the information security plans required of federal agencies by the Federal Information Security Management Act of 2002 (FISMA). FISMA requires federal agencies to develop, document and implement agency-wide programs to provide security for their

[15] GAO (June 2006). "Privacy: Preventing and Responding to Improper Disclosures of Personal Information," at 8.
[16] As with federal agencies, multiple PIAs might be required for each institution, if different departments, agencies, offices, etc. within the institution present different privacy issues. Within a public utility, for example, credit and collection offices might well present different privacy issues than do utility offices addressing smart meter data collection.
[17] Further information regarding OMB guidance on privacy issues can be found on the OMB Web site at http://www.whitehouse.gov/omb/inforeg/infopoltech.html.

information and information systems (which include personally identifiable information and the systems on which it resides). The act requires agencies, among other things, to develop risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level.[18]

Under FISMA, agencies are required to provide sufficient safeguards to cost-effectively protect their information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure (and thus to protect personal privacy, among other things). The statute also requires each agency to develop, document and implement an agency-wide information security program to provide security for information and information systems that support the operations and assets of the agency (including those provided or managed by another agency, contractor or other source).[19]

More specifically, according to GAO, FISMA requires that these information security plans include, among other things:

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;

[18] GAO (January 2008). "Information Security: Protecting Personally Identifiable Information," at 2 – 3.
[19] Id., at 10 – 11.

- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

As GAO concluded:

> Like protecting other information and systems, protecting personally identifiable information is dependent on agencies' having established security programs that include the elements described above. Among other things, agencies must identify the personally identifiable information in their information systems, determine the appropriate risk level associated with it, develop appropriate controls to secure it, and ensure that these controls are applied and maintained.[20]

In sum, as with PIAs, LSAP does not urge that FISMA's statutory requirements are directly applicable to Minnesota's public utilities. LSAP, however, ***does*** urge that the

[20] Id., at 12.

Commission need not independently, and anew, seek to consider and/or define what appropriate public controls and "regulation" of information security might look like. Federal agencies, including the National Institute of Standards and Technology (NIST), have invested considerable thinking (including public process) into the appropriate form and coverage of information security plans for personal information. LSAP believes that the Commission, and Minnesota's utilities, would be well-served to incorporate those processes into Minnesota utility regulation of personal information and information privacy.

---

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?**

The issue of privacy within the context of "smart grid" technology is an issue apart from the broader issue of the protection of utility customer privacy presented elsewhere in the Commission's request for comments. In addition to policy questions involving privacy protection, the smart grid presents technological issues of information security. In some ways, however, the cyber-security issues associated with Smart Meter technology have already been resolved. The 2010 release of the National Institute of Standards and Technology (NIST) Report on Cybersecurity emphasized the importance of developing methods to secure data usage systems as soon as possible:

> While integrating information technologies is essential to building the Smart Grid and realizing its benefits the same networked technologies add complexity and also introduce new interdependencies and vulnerabilities. Approaches to secure

these technologies and to protect privacy must be designed and implemented early in the transition to the Smart Grid.[21]

Within the context of the Smart Grid, the NIST report[22] went on to describe the generally-recognized right to keep personal information private as follows: "[T]he right to control when, where, how, to whom, and to what extent an individual shares their own personal information." In turn, it then defined the latter term as being "any information relating to an individual, who can be identified, directly or indirectly, by that information."[23] Even for Smart Grid-related personal information, LSAP agrees with the Privacy Rights Clearinghouse, which states that "the right to privacy refers to having control over this personal information. It is the ability to limit who has this information, how this information is kept, and what can be done with it."[24]

While LSAP acknowledges the Commission's comments that "the presumption seems to be that there is a public interest to allowing greater access to customer energy usage data," LSAP urges that there are (or should be) limits to such access. This Commission can – and should – control the flow of information generated by the Smart Grid to third parties. While enhancing energy savings and other green energy goals may be the Commission's objective in allowing third party access to the data the Smart Grid generates, one can be reasonably certain that some third parties view the data primarily as a marketing opportunity. Third parties will have products to sell, and Smart Grid data will give them the means of targeting the customers most likely to buy. To be clear, LSAP opposes any third party access to data – whether via customer consent or

[21] National Institute of Standards and Technology (NIST) (August 2010). Interagency Report 7628, vol. 2, at 2.
[22] The NIST report is presented in four volumes (an introduction and volumes 1 – 3). It can be accessed at: http://csrc.nist.gov/publications/PubsNISTIRs.html
[23] Interagency Report 7628.
[24] Privacy Rights Clearinghouse, Why Privacy?, available at http://www.privacyrights.org/why-privacy (last accessed January 24, 2013).

through the utilities, themselves – if such data is not necessary to achieve the State's energy goals.

The Smart Grid will give rise to large amounts of potentially revealing information, whether customers want it or not. The Smart Grid is thus easily distinguishable from situations in which customers choose to log onto the Internet, download an "app," or otherwise voluntarily opt to use technology with the potential to compromise their privacy. The customers here are captives of the monopoly utility and have no choice in what data about them is generated.

Consider that Smart Grid data does not just reveal information about energy usage. The data released may disclose intimate personal details related to customers' presence in or absence from the home, appliances in the home, health, and cohabitation arrangements. For example:

- Scant energy usage may allow third parties, and potentially criminals, to determine which homes are empty;
- Hackers have used poorly secured utility networks to pass their utility charges to other customers and disconnect customers from the grid;
- Landlords may be able to determine how many people live in a home, perhaps in violation of a leasing arrangement, leading to evictions;
- In-home devices may allow two-way communication and facilitate the reading of Radio Frequency Identification tags (RFIDs), disclosing, for example, occupants' prescription data to third parties;
- Data may be stored at the meter, so if a meter is not de-energized when one tenant leaves, the next tenant could have access to that data;
- Data sent over wireless devices is easily intercepted by drive-by data collectors and must be securely encrypted to prevent interception. All Smart Meters have Home Area

Network functionality, even if the meters are not yet activated; once activated they enable wireless transmission of data with the consequent risk of compromising data.

In short, an inadequate protection of customer information can harm those consumers: "Such information could reveal personal details about the lives of consumers, such as their daily schedules (including times when they are at or away from home or asleep), whether their homes are equipped with alarm systems, whether they own expensive electronic equipment such as plasma TVs, and whether they use certain types of medical equipment."[25]

Based on the above, LSAP urges that the Commission has both the right and the duty to limit the commercial use of such data by utilities and by third parties. Fortunately, the Commission has legal means at its disposal to limit access to Smart Grid data to uses genuinely associated with Minnesota's energy goals.

There is, of course, an analog in the telecommunications context. The Federal Communications Commission's "customer proprietary network information" (CPNI) rules prohibit access to or use of customer account data except in certain limited circumstances.[26] The FCC required telecommunications carriers to obtain opt-in consent from a customer before disclosing that customer's CPNI to a carrier's joint venture partner or independent contractor for the purpose of marketing communications-related service to that customer.

Moreover, federal legislation restricts the transfer of data on library usage and on cable television usage.

---

[25] U.S. Department of Energy (October 5, 2010). "Data Access and Privacy Issues Related To Smart Grid Technologies," at 2. http://www.gc.energy.gov/documents/Broadband_Report_Data_Privacy_10_5.pdf

[26] *Report and Order and Further Notice of Proposed Rulemaking, in the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information (CPNI) and Other Customer Information*, CC Docket 96-115: IP Enabled Services, WC Docket No. 04-36, *Report and Order and Further Notice of Proposed Rulemaking*, FCC 07-22, adopted March 13, 2007 *(Report and Order)*. CPNI includes personally identifiable information derived from a customer's relationship with a provider of communications services. Section 222 of the Communications Act of 1934, as amended establishes a duty of every telecommunications carrier to protect the confidentiality of its customers' CPNI. 47 U.S.C. § 222. *Report and Order*, ¶ 37. The opt-in rule has survived appeals since 2007.

Based on the above, LSAP urges that several consumer protections march forward from a recognition of a consumer's fundamental right to privacy:

1. Customer data should be released to third parties only upon customers giving affirmative consent to such release.[27]
2. Customers should be fully informed of the rights they are conceding if and when they consent to the release to the third party before granting consent, and the consent should expire at reasonable intervals so that customers have an opportunity to withdraw that consent.
3. In order to control the spread of their energy usage data beyond the utility, customers must be given an opportunity to specify how it will be used, if at all. The customer should be fully informed of the justification for gathering their usage data, the uses that may be made of the data, and their right to give or deny consent to its release to a third party.
4. When an energy utility uses an advanced metering infrastructure where the customer can access his or her data, the customer shall not be coerced into allowing the utility or a third party access to the customer's data as a condition for that access.
5. The Commission should require that contracts between a utility and a third party be filed with the Commission and approved, before they take effect. The filing should include a copy of any consent document the customer is provided and a copy of the notice given to the customer which solicits the customer's consent.
6. Any contract with a third party should include, within the contract, a requirement that the third party implement and maintain reasonable security procedures and practices

[27] In addition, where a third party seeks customer information from the utility, as a condition of that dissemination, the Commission should require the third party to provide the utility with data explaining how many customers have signed up with the third party and how often customer data is being accessed.

appropriate to the nature of the information. Any waiver of such a commitment should be void and unenforceable.

Finally, notwithstanding LSAP's comment above about the possible release of information to third parties given customer "consent," LSAP urges that strict limits be placed on the possible uses for which "consent" may be sought so that the possibility of consent does not swallow the limitations sought to be created. The "consent model" of privacy protection is increasingly viewed as being ineffective. The "consent model" often results in lengthy legal documents that customers do not understand, or brief general statements that do not adequately inform customers to what they are agreeing. One staff member at the U.S. Department of Commerce has noted that "[t]here are essentially no defenders any more of the pure notice-and-choice model."[28]

Accordingly, LSAP urges that the Commission should not allow third parties or utilities (or their agents) to ask customers to consent to ***any*** use of Smart Grid data that does not relate to the energy goals of the state.[29] Indeed, the Commission should define appropriate uses of customer data, and limit the use of energy usage data to purposes necessary to achieving the state's energy savings goals. Since the Smart Grid is intended to save energy, increase electricity reliability, and reduce greenhouse gases, allowed uses should be limited to these same purposes.

[28] Steve Lohr, "Redrawing the Route to Online Privacy," N.Y. Times, February 27, 2010, at BU4 ("'There are essentially no defenders anymore of the pure notice-and-choice model," said Daniel J. Weitner, a senior policy official at the National Telecommunications and Information Administration of the Commerce Department. 'It's no longer adequate.'"

[29] In referring to the "energy goals of the state," it would be inappropriate to equate "the state" with "the PUC." The "energy goals of the state," for example, also include the pursuit of energy affordability through the state-administered, federal block grant Low-Income Home Energy Assistance Program (LIHEAP) (and the corresponding utility-administered affordability supplements). The "energy goals of the state" would also include not only the state-administered, federal block grant Weatherization Assistance Program (WAP) (and the corresponding utility-administered supplements), but the usage reduction programs such as the Conservation Improvement Program (CIP), including low-income CIP. The sharing of utility information with the state, and with nonprofit entities charged with implementing these affordability and usage reduction goals of the state, do not fall within the rubric of contracts about which LSAP is expressing concern. To the extent that existing CIP contractors have contracts that specify privacy protections, it would be reasonable to grandfather such existing contracts.

The data may only be used to achieve Minnesota's energy goals made possible by the Smart Grid. The Commission should define this to include the furtherance of the state's energy goals:

- by reducing energy use;
- by increasing use of renewable energy;
- by producing energy savings;
- by facilitating demand response;
- by reducing greenhouse gas output;
- by enhancing energy reliability or security.

In furtherance of the above restrictions, third parties should certify that:

- The data is actually necessary to achieve articulated state energy goals. If third parties do not need customer-specific data, but can instead develop products without it, they should not seek or receive access to it.[30]
- The data will not be used for marketing or other activity not related to the foregoing uses.
- The data should actually be produced by the Smart Grid itself. Data the utilities otherwise develop or use is irrelevant to this proceeding, and third parties should not request or receive such data (although should specific data-sharing arrangements have already been authorized by the Commission, they may continue).

---

5. What issues should be included 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;

[30] For example, third parties may seek to develop or sell smart appliances like refrigerators or dishwashers that do not require customer data to develop. If they do not need the data, the Commission should make clear they cannot seek or receive the data either from customers or utilities.

c. Data use limitations, 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).

LSAP's comments on questions "a" through "d" above are presented in response to other sections of these comments. LSAP urges specific consideration of one additional specific privacy issue: the collection and use of Social Security Numbers.

In this section, LSAP urges that, in response to the growing use of Social Security Numbers (SSNs) in enabling the crime of identity theft, the Commission should join the growing consensus that institutions (such as public utilities) that have collected SSNs in the past refrain from, or be prohibited from, collecting such SSNs in the future, and that Minnesota utilities be directed to seek out alternatives to the collection and use of SSNs.[31]

The use of SSNs by private entities is one of the leading causes of identity theft. SSNs, along with a person's date of birth and name, are the three most sought-after pieces of personal information sought by identity thieves. Indeed, according to the 2007 report of the Presidential Task Force on Identity Theft, a person's SSN is the ***single*** most important piece of personally identifiable information available to identity thieves. Unlike names and addresses, which can change over a person's lifetime, it is "virtually impossible" for a person to change his/her SSN.[32]

[31] According to the FTC: "Concerns about over-use of SSNs and their role in identity theft have increased in recent years. In a recent consumer survey, 66 percent of the respondents stated that companies should stop using SSNs to identify customers and 64 percent perceived that they were more vulnerable to identity theft when a business had their SSN." FTC (November 2007). "Staff Summary of Comments and Information Received Regarding the Private Sector's Use of Social Security Numbers," at 2.

[32] Unlike a lost key, the social security number cannot be changed merely because it has been lost or stolen. "Identity Theft and Your Social Security Number," Social Security Administration, Pub. No. 05-10064, Oct. 2007, at 6, available at http://www.ssa.gov/pubs/10064.pdf. There must be evidence that (1) someone is in fact wrongfully using the number, and (2) that the individual to whom the number belongs is being disadvantaged by the wrongful

SSNs are the key to help create false identities. A person's SSN is viewed as a "breeder document" by identity thieves. With a Social Security Number, an identity thief can create other false documents supporting a false identity, including a driver's license, retail credit account, credit card account, bank account, and similar papers. Indeed, given the lack of a standard protocol for truncating SSNs, even truncated SSNs are not helpful in preventing identity theft. While some businesses truncate the first five digits of an SSN, other businesses truncate the last four. Not only can SSNs thus be reformulated with information from multiple sources, those multiple sources need not be illicitly gained. Public documents such as tax liens, driving histories, voter registrations, bankruptcies, and the like, are all publicly-available information which might be used to match all or part of an SSN obtained from a utility record with a specific individual.

The clear direction today is to reduce, and eliminate where possible, the unnecessary collection of SSNs. In 2007, the federal Office of Management and Budget (OMB) issued a memo requiring federal agencies to examine their use of SSNs in systems and programs in order to identify and eliminate instances in which collection or use of SSNs is unnecessary. OMB required agencies to explore alternatives to their use of SSNs.

Like OMB's guidance to federal agencies, the Federal Trade Commission (FTC) has urged a reduction in the use of SSNs in the private sector. FTC testified to Congress that there was a need to eliminate the unnecessary use of SSNs. The FTC cited the observation of the Presidential Task Force on Identity Theft that it is not clear whether the use of SSNs by the

---

use.

private sector was a necessity, or a result of "convenience and habit."[33] The President's Task Force stated quite simply in its 2007 report that: "More must be done to eliminate unnecessary uses of SSNs." The General Accounting Office agreed. According to GAO:

> Limiting the collection of personal information, among other things, serves to limit the opportunity for that information to be compromised. For example, key identifying information –such as Social Security numbers—may not be needed for many agency applications that have data bases of other personal information. Limiting the collection of personal information is also one of the fair information practices which are fundamental to the Privacy Act and to good privacy practice in general.[34]

Utilities would be hard-pressed to provide legitimate reasons to collect SSNs in today's world.[35] For example, SSNs should not be needed to identify customers who seek to present

[33]President's Identity Theft Task Force (2007). Combating Identity Theft: A Strategic Plan, at 24.
[34] GAO (June 2006). "Privacy: Preventing and Responding to Improper Disclosures of Personal Information," at 11.
[35] LSAP endorses the view expressed in the North Carolina Journal of Law and Technology:

> commentators have lamented that the social security number has become a "skeleton key" for identity theft criminals. Even more troubling, the availability of the number increases in direct proportion to its use as a key. Any organization that wishes to use an individual's social security number must make at least one copy of it; this copy is frequently stored in a computer system that may be accessible by a global workforce of employees. Given that thousands of organizations collect the number and share it with affiliates, contractors, government entities and others, the number's vulnerability to loss, employee misuse, or theft by third parties quickly becomes apparent. The advent of the Internet and the proliferation of outsourcing have only magnified the speed and extent of dispersal of the social security number. Just as the weakest link will make a chain give way, the institution with the most lax security procedures or least honest employees may be the only thing standing between a thief and the contents of an individual's bank account and private records.
>
> How secure would one feel if she gave the key to her home to every government agency, health care provider, credit card company, and other business organization with whom she had a direct or indirect relationship? What would one do if a copy of this key could be located, inexpensively or even for free on the internet, by anyone with basic information who is willing to look for it? Yet this is exactly the system that has been created via the use of the social security number as a password that can provide the holder with access to an individual's financial resources, retirement accounts, private health information, and more. Worse yet, unlike locks which can be changed if a key is lost or falls into the wrong hands, the social security number is virtually unchangeable.

Darrow and Lichtenstein. "'Do You Really Need my Social Security Number?' Data Collection Practices in the Digital Age," 10 N.C. J. L. & Tech. 1, 4 – 5 (Fall 2008) (internal citations omitted).

themselves as someone other than who they really are. Under the Federal FACTA statute, described above, each Minnesota utility should by now have prepared its federally-prescribed Red Flags Plan in compliance with the statute and the FTC's Red Flags Rule. Given the ***mandatory*** nature of the Red Flags Rule as applied to public utilities, the need to ***also*** collect SSNs to authenticate that a person is who he/she purports to be has become minimized.

Limiting the collection of personally identifiable information such as SSNs is particularly important when faced with companies that operate over multiple jurisdictions, as some Minnesota utilities do. Use of SSNs in this respect is like pollution. Once the use spills over into another jurisdiction, the state of Minnesota loses control over it. The "next" state, however, may have inconsistent protections for personal information, if any. The only way to effectively control the use of customer data, therefore, is to control it at its source, to prevent it from being collected in the first instance.

No reason exists for the Commission to lag behind in eliminating or minimizing the use of SSNs. At the state and federal level, as well as at the regulatory level for businesses other than public utilities (e.g., educational institutions, financial institutions), there is a distinct move to find alternatives to the use of SSNs to help reduce the threat of identity theft. The Commission should join in those efforts.

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?

LSAP urges the Commission to adopt the policy that Minnesota utilities should adopt Fair Information Practices (FIPs) as the basic foundation for the privacy protection of personal information. In both the public and private sectors, Fair Information Practices are not seen as a set of legal requirements, but rather as a "framework of principles."[36] FIPs have been "widely adopted as the standard benchmark for evaluating the adequacy of privacy protections."[37] Indeed, GAO has referenced FIPs as a "universal benchmark of privacy protections."[38] The FIPs "in many ways represent the international consensus on what constitutes honest and trustworthy

[36] The National Research Council / National Academy of Sciences, describes FIPs as follows: "Fair information practices are standards of practice required to ensure that entities that collect and use personal information provide adequate privacy protection for that information. These practices include notice to and awareness of individuals with personal information that such information is being collected, providing individuals with choices about how their personal information may be used, enabling individuals to review the data collected about them in a timely and inexpensive way and to contest that data's accuracy and completeness, taking steps to ensure that the personal information of individuals is accurate and secure, and providing individuals with mechanisms for redress if these principles are violated. Fair information practices were first articulated in a comprehensive manner in the U.S. Department of Health, Education, and Welfare's 1973 report *Records, Computers and the Rights of Citizens*.[23] This report was the first to introduce the Code of Fair Information Practices, which has proven influential in subsequent years in shaping the information practices of numerous private and governmental institutions and is still well accepted as the gold standard for privacy protection. From their origin in 1973, fair information practices "became the dominant U.S. approach to information privacy protection for the next three decades." The five principles not only became the common thread running through various bits of sectoral regulation developed in the United States, but they also were reproduced, with significant extension, in the guidelines developed by the Organisation for Economic Co-operation and Development." National Research Council (2008). Engaging Privacy and Information Technology in a Digital Age, at 48, 50 (National Academies Press).

[37] See, e.g., GAO (June 8, 2006), "Privacy: Preventing and Responding to Improper Disclosures of Personal Information," at 5.

[38] GAO (April 2006). "Personal Information: Agency and Reseller Adherence to Key Privacy Principles," at 6, 65.

treatment of personal information."[39] A summary of the Fair Information Practice principles is set forth in tabular form immediately below:[40]

Fair Information Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

It is not merely GAO that recognizes FIPs as the "universal benchmark" or "international consensus" on what represents the proper treatment of personal information. FIPS were endorsed by the U.S. Department of Commerce in 1981.[41] The Office of Management and Budget (OMB), as early as 1998, issued a memorandum to all federal agencies saying that it "shall be the policy of the Executive Branch" that "personal information contained in Privacy Act systems of records be

[39] Id., at 66.
[40] These comments do not seek to expound on any particular one of these FIPs.
[41] National Institute of Standards and Technology (April 2010). "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," at Section 2.3 (PII and Fair Information Practices).

handled in full compliance with fair information practices as set out in the Privacy Act of 1974."[42] In 2004, the Chief Information Officers (CIO) Council issued the Security and Privacy Profile for the Federal Enterprise Architecture that links privacy protection with a set of acceptable privacy principles corresponding to the Fair Information Practices.[43] The Securities and Exchange Commission (SEC), the National Archive and Records Administration (NARA), the U.S. General Services Administration (GSA), have all, to one degree or another, endorsed and adopted Fair Information Practices.

According to the National Research Council, "the principles of fair information practices are as relevant today—perhaps more so—for the protection of personal information as they were when they were first formulated."[44]

In addition to the Fair Information Practices presented above, LSAP believes the Commission should take notice of, and incorporate, the lessons of extended inquiry into privacy protections principles. The U.S. Department of Energy (DOE), in its 2010 report "Data Access and Privacy Issues Related to Smart Grid Technologies," included an extensive discussion of Fair Information Practices.[45]

[42] OMB (May 14, 1998). "Memorandum for the Heads of Executive Departments and Agencies: Privacy and Personal Information in Federal Records."
[43] NIST Guide, supra, at Section 2.3.
[44] National Research Council, supra, at 337.
[45] US DOE, supra, at 30 – 34.

Summary of Recommendations

In sum, LSAP urges that the Commission need not, and should not, promulgate uniform privacy practices for Minnesota utilities. Instead, the Commission should require each Minnesota utility, irrespective of whether it is an energy, telecommunications, or water/wastewater utility, to:

- Document its compliance with the FTC's Red Flags Rule;
- Promulgate an appropriate 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 guidelines, to be filed with the Commission;
- Promulgate an appropriate risk-based Information Security Plan (ISP), or set of ISPs, consistent with the federal ISP requirements of FISMA and resulting regulations and guidelines, to be filed with the Commission;
- 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.

In addition, Minnesota's energy utilities will face their own unique issues relating to the privacy protections to be applied to customer data generated by the use of Smart Grid technology. For energy utilities operating within the Smart Grid environment, LSAP recommends that:

- The Commission can –and should—control the flow of information generated by the Smart Grid to third parties;
- Strict limits should be placed on the possible uses for which consent may be sought so that the possibility of consent does not swallow the limitations sought to be created. The data may only be used to achieve Minnesota's energy goals made possible by the Smart Grid.[46]

[46] The Commission should define this to include the furtherance of the state's energy goals: by reducing energy use; by increasing the use of renewable energy; by producing energy savings; by facilitating demand response; by reducing greenhouse gas output; and by enhancing energy reliability of security.

- Customer data should be released to third parties only upon customers giving affirmative consent to such release.[47] Customers should be fully informed of the rights they are conceding if and when they consent to the release to the third party before granting consent, and the consent should expire at reasonable intervals so that customers have an opportunity to withdraw that consent. The customer should be fully informed of the justification for gathering their usage data, the uses that may be made of the data, and their right to give or deny consent to its release to a third party.
- When an energy utility uses an advanced metering infrastructure where the customer can access his or her data, the customer shall not be coerced into allowing the utility or a third party access to the customer's data as a condition for that access.
- The Commission should require that contracts between a utility and a third party be filed with the Commission and approved, before they take effect. The filing should include a copy of any consent document the customer is provided and a copy of the notice given to the customer which solicits the customer's consent.
- Any contract with a third party should include, within the contract, a requirement that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information. Any waiver of such a commitment should be void and unenforceable.

In furtherance of understanding of privacy-related issues, both relating to the Smart Grid and generally, LSAP urges the Commission to base its decision-making in part on the following publications:

- U.S. Department of Energy (October 5, 2010). "Data Access And Privacy Issues Related To Smart Grid Technologies," accessible at the following URL (accessed January 24, 2013): http://www.gc.energy.gov/documents/Broadband_Report_Data_Privacy_10_5.pdf

- National Institute for Standards and Technology (September 2010). "Guidelines for Smart Grid Cybersecurity," (4 volumes), accessible at the following URL (accessed January 24, 2013): http://csrc.nist.gov/publications/PubsNISTIRs.html

- President's Identity Theft Task Force (2007). Combating Identity Theft: A Strategic Plan (2 vol.), accessible at the following URL (accessed January 24, 2013): http://www.idtheft.gov/about.html

[47] In addition, where a third party seeks customer information from the utility, as a condition of that dissemination, the Commission should require the third party to provide the utility with data explaining how many customers have signed up with the third party and how often customer data is being accessed.

As models for specific recommendations that LSAP has advanced, it recommends consideration of the law and regulations with respect to the following:

- Protection against identity theft: The Federal Trade Commission's Red Flags Rule (and enabling legislation);
- Privacy Impact Assessments (PIAs): The E-Government Act of 2002 (Section 208).
- Information Security Plans (ISPs): Federal Information Security Management Act (FISMA).

Finally, LSAP recommends that the Commission immediately prohibit Minnesota utilities from henceforth collecting individual Social Security Numbers from residential customers; prohibit Minnesota utilities from publishing, transmitting, or otherwise communicating SSNs they currently hold to any entity other than the utility, including affiliates and out-sourcing contractors; and prepare and deliver to the Commission within a timeframe deemed to be reasonable by the Commission (e.g., six months) a report containing recommendations on alternatives to the collection and use of SSNs in the future.