DOE/EE-0828

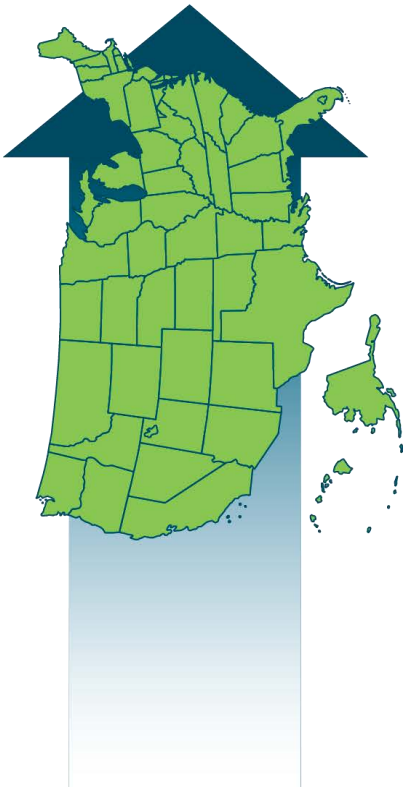
SEE Action

STATE & LOCAL ENERGY EFFICIENCY ACTION NETWORK

A Regulator's Privacy Guide to Third-Party Data Access for Energy Efficiency

Customer Information and Behavior Working Group

December 2012



The State and Local Energy Efficiency Action Network is a state and local effort facilitated by the federal government that helps states, utilities, and other local stakeholders take energy efficiency to scale and achieve all cost-effective energy efficiency by 2020.

Learn more at www.seeaction.energy.gov

A Regulator's Privacy Guide to Third-Party Data Access for Energy Efficiency was developed as a product of the State and Local Energy Efficiency Action Network (SEE Action), facilitated by the U.S. Department of Energy and the U.S. Environmental Protection Agency. Content does not imply an endorsement by the individuals or organizations that are part of SEE Action working groups, or reflect the views, policies, or otherwise of the federal government.

This document was final as of December 18, 2012.

If this document is referenced, it should be cited as:

State and Local Energy Efficiency Action Network. 2012. *A Regulator's Privacy Guide to Third-Party Data Access for Energy Efficiency*. Prepared by M. Dworkin, K. Johnson, D. Kreis, C. Rosser, J. Voegele, Vermont Law School; S. Weissman, UC Berkeley; M. Billingsley, C. Goldman, Lawrence Berkeley National Laboratory.

FOR MORE INFORMATION

Regarding *A Regulator's Privacy Guide to Third-Party Data Access for Energy Efficiency*, please contact:

Michael Li
U.S. Department of Energy
E-mail: michael.li@ee.doe.gov

Stacy Angel
U.S. Environmental Protection Agency
E-mail: angel.stacy@epa.gov

Regarding the State and Local Energy Efficiency Action Network, please contact:

Johanna Zetterberg
U.S. Department of Energy
E-mail: johanna.zetterberg@ee.doe.gov

Acknowledgments

A Regulator's Privacy Guide to Third-Party Data Access for Energy Efficiency is a product of the State and Local Energy Efficiency Action Network's Customer Information and Behavior (CIB) Working Group. The working group is co-chaired by Phyllis Reha, Minnesota Public Utilities Commission and Vaughn Clark, Office of Community Development, Oklahoma Department of Commerce. The federal staff leads for the working group are Stacy Angel, U.S. Environmental Protection Agency and Michael Li, U.S. Department of Energy.

This report was prepared by Michael Dworkin, Katie Johnson, Donald Kreis, Carey Rosser, and Jonathan Voegele, Vermont Law School; Steve Weissman of UC Berkeley; and Megan A. Billingsley and Charles A. Goldman of Lawrence Berkeley National Laboratory, under contract to the U.S. Department of Energy. This work was supported by the National Electricity Delivery Division of the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability under Lawrence Berkeley National Laboratory Contract No. DE-AC02-05CH11231.

The authors received direction and comments from the CIB Working Group; members can be viewed at www.seeaction.energy.gov/members.html. In addition to direction and comment by the CIB Working Group, the following reviewers provided valuable input and review comments on a draft of this report:

- Tanya Brewer (National Institute of Standards and Technology)
- Tanya Burns (Energetics)
- Kathleen Hogan (U.S. Department of Energy)
- Larry Mansueti (U.S. Department of Energy)
- Amanda Stallings (Public Utilities Commission of Ohio)
- Brent Struthers (Neustar, Inc.)
- Marianne Swanson (National Institute of Standards and Technology)
- Chris Villarreal (California Public Utilities Commission)
- Johanna Zetterberg (U.S. Department of Energy).

Acronyms

AMI	Advanced metering infrastructure
CEUD	Consumer-specific energy usage data
CIMS	Confidential Information Management System
CPNI	Customer proprietary network information
DHS	United States Department of Homeland Security
DOE	United States Department of Energy
EESP	Energy efficiency service provider
EEU	Energy efficiency utility
EPA	United States Environmental Protection Agency
ESP	Electric service provider
ESPI	Energy Service Provider Interface Standard
FCC	Federal Communications Commission
FIPPs	Fair information practice principles
FTC	Federal Trade Commission
HHS	United States Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
NAESB	North American Energy Standards Board
NIST	National Institute of Standards and Technology
PIC	Program implementation contractor
PII	Personally identifiable information
PSB	Public service board
PSC	Public service commission
PUC	Public utilities commission
VEIC	Vermont Energy Investment Corporation

Table of Contents

Executive Summary

Energy efficiency has become a widely accepted public policy across the United States. Program administrators in more than 40 states are implementing energy efficiency programs funded by either electric or gas utility customers.

With the advent of smart meters, approximately one-third of U.S. homes now have devices that are capable of collecting and communicating more detailed data about individual customers' energy usage. Interval usage data from smart meters in conjunction with other enabling technologies (e.g., information/feedback tools, smart appliances) offer even greater opportunities for optimizing energy efficiency programs.

In addition to administrators of customer-funded efficiency programs, access to consumer data presents a significant opportunity for other actors in the energy efficiency services market. For example, many of these actors play a role in educating customers about energy usage monitoring and home energy upgrades, often providing services that go beyond those encouraged by customer-funded programs. The inability for energy efficiency service providers (EESPs) to gain access to the data because of legitimate privacy concerns creates a barrier to realizing many of the benefits from these services. Often, regulatory commissions confront and must resolve two competing policy imperatives: (1) the need to facilitate access to customer data for energy efficiency purposes while (2) safeguarding customer privacy and providing consumer protections in connection with unwanted uses of data. This report informs state regulators about issues and policy options related to providing access to customer information held by utilities that can be used to support and enhance provision of energy efficiency services and protect customer privacy.

The "customer information" and "data" referred to in this guide comprise two distinct categories:

- **Personally identifiable information (PII),** which consists of customer names, addresses, Social Security numbers, and other information that specifically identifies the person or entity to which it applies.
- **Customer-specific energy usage data (CEUD),** which, in most cases, does not identify an individual customer[1] but includes detailed information about the utility service provided to the customer.

It is also useful to distinguish among the three types of entities that are involved in the provision of energy efficiency services that may reasonably require or request access to customer data that are acquired by utilities in the course of providing service:

- **Program administrators** of energy efficiency programs funded by utility customers are typically under direct supervision by a state regulatory agency (e.g., public utilities commission [PUC]). Utilities administer energy efficiency programs in approximately 40 states, while state agencies or profit/nonprofit companies manage programs in eight states.
- **Program implementation contractors (PICs)** are entities that work on behalf of the program administrator and have a contractual relationship to provide various types of services needed in program design, implementation, or evaluation (e.g., energy audits, project design, inspection, verification of installations, evaluation of savings). Typically, a PIC has access to customer information necessary to perform only the services for which they have been contracted.
- **Energy efficiency service providers (EESPs)** [2] are third-party market participants that provide energy efficiency services or products to end users but do not have a direct contractual or legal relationship with the program administrator or state PUC. Some EESPs have expressed a strong interest in obtaining access to certain types of customer data in order to reduce their costs of acquiring and delivering services to new

[1] If a single individual or single company is the sole occupant of a building, this data could identify a specific customer's energy usage.

[2] Some common examples of EESPs include electrical or mechanical contractors, home performance contractors, auditing firms, product vendors, and local government or nonprofit entities that have either implemented or plan to implement local or regional energy efficiency programs.

and existing customers. Because many state regulators have an interest in leveraging spending by program administrators and/or are interested in transforming markets over the long term, this issue of access to energy efficiency-related customer data to support private sector business models is an important policy issue.

The data access and privacy policy landscape is changing quickly, as legislative activity continues and utility regulators conduct proceedings on their own initiative or at the request of stakeholders. Based on phone and email inquiries, as well as a literature search of legal databases and PUC websites, eight jurisdictions (as of this publication) were identified that have adopted statutes, regulations, and/or PUC orders that govern third-party access to customer data: California, Colorado, Oklahoma, Oregon, Texas, Vermont, Washington, and Wisconsin. Additionally, seven states were identified where commissions have opened dockets driven by increased attention to data privacy or security in the context of smart grid legislation or applications by utilities.

Based on a review of state experiences to date, regulators and policymakers are likely to address certain common issues in policymaking regarding data access, security and privacy in the context of energy efficiency programs and services. These include customer consent to data access (at the individual and/or aggregated levels); access by customers to their own utility data; data management, data security, and privacy; enforcement mechanisms and business practices; and cost recovery for utilities. This report's primary focus is on potential solutions to address customer privacy when the utility is providing the access to customer data. Privacy issues that arise when the utility is not involved, such as when a customer provides their energy usage data directly to a third party, is addressed in a more limited manner.[3]

Customer Consent

Figure ES-1 provides an overview of current state approaches to consent and identifies the types of non-utility entities that may want access to a customer's PII or energy usage data.

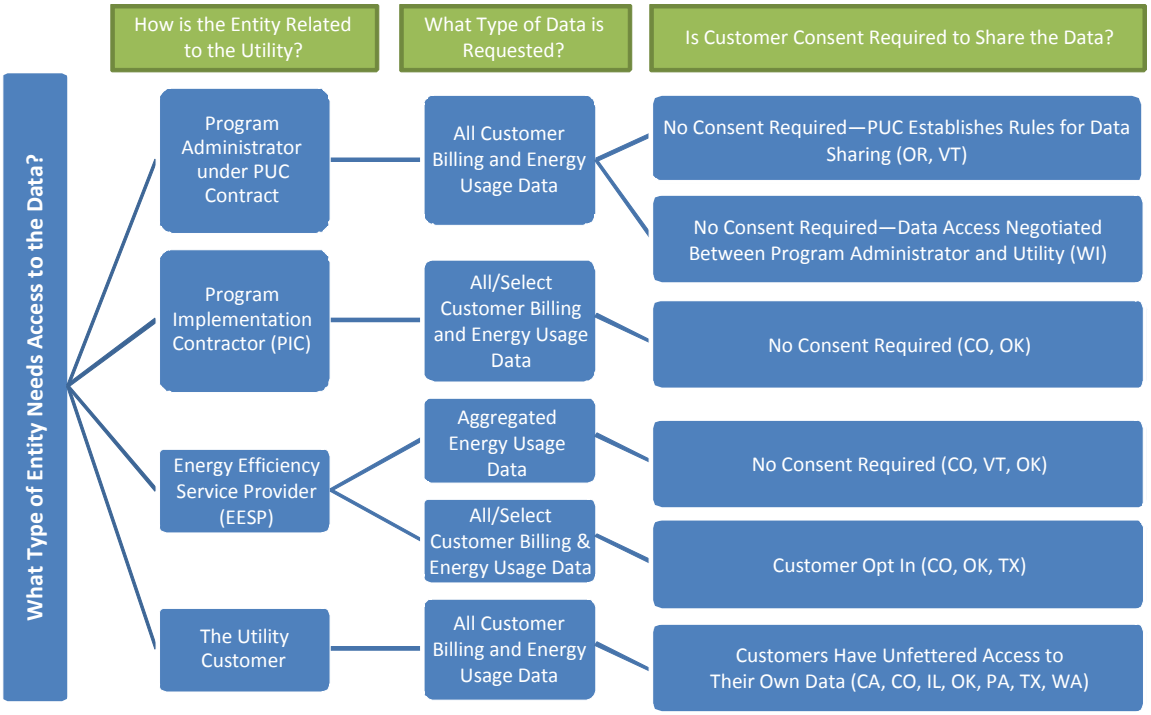


Figure ES-1. Overview of state approaches on accessing customer utility data

[3] See Section 4.1 for more information on privacy protection options for customers who provide third parties with their energy use data.

Customer Consent: Individuals

For states with a third-party energy efficiency program administrator, the general approach has been for the PUC or legislature to establish the rules for sharing customer data prior to program activities (e.g., VT) or to negotiate data access between the utilities and the third-party program administrator (e.g., WI).[4]

PICs working under contract to utilities typically have been able to access customer data to fulfill their scope of services because they are assumed to be subject to the same privacy standards as the utility itself.

In the case of unregulated EESPs that request access to customer data, several state PUCs have required customers to give affirmative consent (e.g., CO, TX, and WA).

Customer Consent: Aggregated Data

Insight from other industries as well as historic experience of electric and gas utilities administering energy efficiency programs suggests that disclosing aggregated data poses limited risk to the customer. Aggregated data—information about specific customers that is combined in a manner that leaves individual customers unidentifiable by the recipient—allows program administrators, PICs, or EESPs to determine trends and evaluate results so that they, for example, can identify specific geographic areas or demographic groups that may have a higher ability to benefit from energy efficiency programs or services. Aggregated information that may be valuable and useful to EESPs includes data on customer energy usage patterns, market assessments of efficiency opportunities in selected market segments or geographic regions, process and impact evaluations, and market potential studies. Additionally, providing aggregate energy usage of tenants can inform building owners so their investments can support greater energy savings for tenants and strengthen the market for energy efficiency.

However, given the availability of powerful analytic tools and multiple databases outside the records of utilities, there are concerns that an authorized third party, or others, might be able to 'reverse engineer' aggregated data and identify individual customers. To address this concern, the Colorado PUC has adopted a 15/15 rule that prohibits the release of aggregated data (without individual customer consent) unless there are at least 15 customers included in the data and no individual customer comprises more than 15 percent of the customer group.[5] In Vermont, the Public Service Board has only allowed disclosure of aggregated data that are characterized at the level of a municipality (e.g., town, city).[6] If state PUCs decide to support the provisioning of aggregated data, they should consider establishing guidelines or policies that set standards for when data are sufficiently aggregated.

Access by Customers to Their Utility Data

The general consensus among states that have established policies on customer data sharing appears to be that customers should have access to their own data (e.g**.,** California, Colorado, Illinois, Oklahoma, Pennsylvania, Texas, and Washington).[7] Application of this principle may require regulators and/or policymakers to consider whether and how to manage what customers do with the data they obtain.

[4] For more information about the types of program administrators, see Regulatory Assistance Project (RAP). (2011). *Who Should Deliver Ratepayer Funded Energy Efficiency? A 2011 Update.* Prepared by Richard Sedano. www.raponline.org/document/download/id/4707.

[5] 4 Colo. Code Regs. 723-3 Part 3 §3031(b)(c).

[6] Vermont Public Service Board. (2010). *Investigation into Petition Filed by Vermont Department of Public Service Re: Energy Efficiency Utility Structure.* Docket No. 7466.

[7] 4 Colo. Code Regs. 723-3 Part 3 §3026(d); Okla. Stat. tit. 17 §710.4; Cal. Pub. Util. Code §8380(a)(4); Ill. Admin. Code. tit. 83 §410.210; 66 Pa. Cons. Stat. § 2807; 2 Tex. Util. Code §39.107; Wash. Admin. Code §480-100-153.

The Green Button initiative,[8] in which several utilities facilitate web-based access for customers to access and download their own data in a standardized format, raises the question of what happens when customers, rather than utilities, give third parties access to their information. Although state regulators generally lack authority to intervene in such disclosures, they can promote independent industry standards. Third parties seeking data directly from customers could win the confidence of those customers by obtaining documentation certifying the company's ability to adhere to industry standards regarding privacy. Regulators can encourage third parties receiving customer data to publicly commit to personal data practices by adopting a privacy policy. In those circumstances, a company breaching its commitments can be subject to an enforcement action by the Federal Trade Commission.

Data Management, Data Security, and Privacy

Authorizing disclosures to PICs and EESPs is, in some sense, just the beginning. In other contexts—such as healthcare—and in at least two states (e.g., CO, WI) that have regulated access to customer information, PICs that are under the jurisdiction of the PUC are required to destroy the data once the purposes for disclosing the information are achieved. Likewise, policymakers have found it appropriate to limit data sharing to only that information which is necessary for the PIC or EESP to complete its tasks. PICs and EESPs can be required to not only maintain specified security measures, but also verify their compliance with generally accepted practices through an independent auditor.

Enforcement Mechanisms and Business Practices

Given the significance of privacy concerns, civil and criminal penalties may effectively deter breaches of state privacy law. Penalties could be more stringent for intentional, illegal data disclosures as opposed to accidental disclosures and disclosures of aggregated data. Violations, and sanctions for violations, could be defined by either the state legislature or state PUC and be applicable across a broad swath of third parties interested in accessing customer data. State PUCs, or the state attorney general, can then enforce rules or sanctions for any violation. The U.S. Department of Homeland Security Fair Information Practice Principles (FIPPs),[9] the telecommunications industry's Consumer Privacy Bill of Rights, and state policy related to third-party access to customer data in California, Colorado, Vermont, and Wisconsin all provide examples of how a PUC might choose to structure rules or legislation.[10]

To increase accountability for entities under the jurisdiction of a state PUC that possesses customer information, the following policy options may be useful practices for a state to consider:

- Require that each utility and contractor be covered by a privacy policy, obtain regulatory approval of the policy, follow the policy, and make the policy available to customers
- Require utilities to submit annual reports that include their written privacy policies, compliance statistics, and information about each complaint received, including its resolution
- Encourage periodic "privacy audits" for utilities and third parties to assure the public that these entities are faithfully maintaining the privacy of customer data and using it only for authorized purposes
- Encourage "for cause audits" where major changes (e.g., bankruptcy) occur to the corporate structure of an entity handling CEUD, or where a data breach has occurred.

[8] "Green Button Data Demonstration." (2012). www.greenbuttondata.org.

[9] U.S. Department of Homeland Security. (2008). *Privacy Policy Guidance Memorandum*. www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[10] Cal. Pub. Util. Code §8380(f); 4 Colo. Code Regs. 723-3 Part 3 §3976; Wisconsin Public Service Commission. (2009). *Provision of Energy Utility Customer Information to Focus on Energy*. Docket No. 9501-GF-101; Vermont Public Service Board. (2010). *Investigation into Petition Filed by Vermont Department of Public Service Re: Energy Efficiency Utility Structure.* Docket No. 7466.

For entities not under the jurisdiction of a state PUC, the options to address privacy issues are more limited, but can still help bring about more consistent privacy protections. For example, states can implement either of the following:

- Efforts to educate customers about the responsible use of their date
- A voluntary privacy code of conduct.

Cost Recovery

In some cases, providing third parties and customers with access to usage data may lead to additional costs for utilities. States vary in their approach as to whether and how a utility can recover these costs. There are five broad options that can address this issue:

- Allow utilities to include these costs in general operating expenses
- Allow utilities to recover the costs through customer charges
- Allow utilities to charge third parties for access to the data
- Prohibit utilities from recovering any additional costs for providing data to third parties
- Recover costs as part of other related utility projects, such as energy efficiency program portfolios, billing system upgrades, or smart grid deployments.

Federal Policy

As states consider the best ways to enact policies that govern access to customer data, there are several relevant federal privacy policies that can inform decision making at the state level. To date, neither Congress nor any federal agency has adopted any privacy standards that are specific to retail electric utilities or energy efficiency services; however, there are several federal initiatives that are relevant to electric utilities and EESPs including: FIPPs, the Consumer Privacy Bill of Rights, Federal Trade Commission (FTC) Codes of Conduct, non-binding industry standards, and a number of emerging "privacy seal" initiatives. Many of the federal privacy practices and industry standards share basic principles, including the following:

- Requiring customer consent to share data, and allowing customers to revoke consent
- Allowing customers to access their own data
- Disclosing privacy practices, collection practices, sharing practices, etc.
- Limiting the amount of data transferred to purposes specified
- Limiting the type, or granularity, of the data transferred
- Requiring precautions against data security threats
- Requiring a review to ensure compliance with the other principles
- Using public relations as a tool to encourage compliance.

Although none of these practices or standards were adopted with the electric industry or energy efficiency specifically in mind, they are useful to state regulators and legislators both as examples of policy principles they can adopt and as backdrops against which to make state policy.

Privacy Practices in other Industries

While governing access to utility customer data is an emerging challenge, the telecommunications, health care, retail grocery, and retail electric supply industries have all addressed privacy concerns in the context of managing, utilizing, and providing access to customer information. The experience in the telecommunications industry demonstrates the value of customer data to a wide range of third parties and that regulators should be prepared

to address attempts by disfavored third parties to access customer data. Imposing penalties, civil or criminal, on improperly obtaining customer data is one option to address this concern.

The healthcare industry demonstrates the importance of customer consent. Medical data—more than electricity usage data—is perceived as private, personal information. However, as electricity usage data also provides insight into a customer's behavior, the importance of consent should not be overlooked.

The retail grocery industry provides an example of how an industry can achieve its goals while simultaneously maintaining consumer confidence. By rewarding participation in a customer rewards program, while still making it voluntary, consumers retain the freedom of choice but predominantly choose to participate. Further, the existence and publication of a robust privacy policy is important.

The principles that stand out as being relevant from other industries are the following:

- Penalties for improper access
- Customer consent
- Voluntary participation
- Incentivized participation
- Robust privacy policies.

The Way Forward

The governance of third-party access to customer information held by utilities that may enhance or facilitate provision of energy efficiency services is primarily a matter of state jurisdiction. Ultimately, each state may wish to make its own decisions about access to customer information and energy usage data; however, federal privacy practices, lessons learned from other industries, and experiences of those states that have adopted policies on third-party access to customer data held by utilities provide important starting points and a template for consistency. If state policymakers and regulators take action on this issue, utilities will have a well-defined set of privacy and data access rules to implement. Utilities will then understand their responsibilities and the conditions under which they can share customer data.

This guide summarizes the range of approaches adopted by states on privacy and security issues related to third-party access to customer data for energy efficiency. The goal of this guide is to provide regulators, policymakers, and stakeholders options to overcome barriers to realizing the benefits of energy efficiency.

1. Intended Audience

Program administrators in more than 40 states are managing energy efficiency programs funded by either electric or gas utility customers, or both.[11] Access to consumer data by actors in the energy efficiency services market can improve the market in a number of ways. However, the inability for energy efficiency service providers (EESPs) to gain access to the data because of privacy concerns creates a barrier to realizing many of the benefits.

State legislatures and public utilities commissions (PUCs) are uniquely positioned to support energy efficiency and protect customer data because of their jurisdiction over retail electric utilities. Furthermore, PUCs have the ability to create policies for public utilities (and other entities under their jurisdiction) that balance customer privacy concerns with policies that support energy efficiency. State PUCs may not have direct jurisdiction over most third-party EESPs; however, they can work with utilities, consumer groups, and other stakeholders to formulate effective state policies that address third-party access to customer data.

The objective of this guide is to inform state regulators, policymakers, and other stakeholders about issues and policy options related to third-party access to customer energy usage data and other information held by utilities that can be used to support and enhance provision of energy efficiency services. This guide focuses primarily on data access issues in the residential and small commercial context.

[11] Barbose, G.; Billingsley; M.; Goldman, C.; Hoffman, I.; Schlegel, J. (August 2012). "On a Rising Tide: The Future of U.S. Utility Customer-Funded Energy Efficiency Programs." *2012 ACEEE Summer Study Proceedings*; August 12-17, 2012, Pacific Grove, California. Washington, D.C.: American Council for an Energy-Efficient Economy (ACEEE). LBNL-5755E. www.aceee.org/files/proceedings/2012/data/papers/0193-000173.pdf.

2. Introduction

2.1 Customer Data

Historically, electric utilities have used electro-mechanical meters that measure cumulative kilowatt-hour usage for residential customers and typically read the meters monthly.[12] The low granularity of the data limited the scope of the information services that could have been provided to customers. In part to encourage the efficient use of energy, utilities in many states are taking advantage of smart meter technology (i.e., advanced metering infrastructure, or AMI). Currently, over one-third of U.S. residences have AMI devices installed.[13] Smart meters have the capability to record data at frequent intervals. These highly granular data (e.g., near real-time, 15 minute, or hourly) provide additional opportunities to inform and educate customers about their energy usage patterns as well as opportunities to both modify usage patterns and increase efficiency. However, the availability and access to this type of data also raises potential privacy and security concerns.

Data about customers—which may provide insight on energy usage, adoption of energy efficiency measures, and the effects of those measures—is a powerful tool capable of increasing the success of energy efficiency programs. For example, with usage data, analysts can determine which buildings would benefit the most from energy efficiency improvements. If analysts have access to smart meter data, they can assess how building systems (e.g., HVAC), appliances, and devices consume energy. Using this information, analysts may be able to provide insights on the most efficient times of day to operate equipment or when equipment may not be operating properly.[14] If energy usage and other utility data are made available to third parties, energy efficiency service providers (EESPs) could offer additional information and technical services to customers at a reduced cost (e.g., energy audits, high efficiency products appropriate for the homeowner). This could help facilitate the development of a more robust competitive market where EESPs use individual or aggregated customer data to benefit businesses and customers.[15]

However, giving third parties access to customer data potentially raises security and privacy concerns. These concerns are less prevalent for conventional electro-mechanical meters because utility bills based on monthly meter reads of cumulative kilowatt-hours provide less information about a customer's activities. For example, traditional meter data can indicate whether a building has heat in the winter and air conditioning in the summer, but the data will not indicate the hours that the building is unoccupied. In contrast, interval energy usage data from smart meters can suggest patterns of household energy use. This information may allow EESPs to identify specific household activities and appliances that are energy inefficient—enabling them to engage in targeted energy efficiency marketing efforts. However, third parties with ulterior motives may find customer usage data valuable as well. For example, criminals can use the data to survey and target a residence. Law enforcement authorities could track the data to identify potentially illegal activities.[16] Some consumers express concerns about access to smart meter data when they learn that the data can reveal the following:

- Which hours of the day a building remains unoccupied
- Whether the building is a permanent or vacation residence
- When the HVAC system is in use.

[12] Many utilities also have installed meters with multiple registers that support time-of-use (TOU) rates for residential and small commercial customers.

[13] Edison Foundation. (2012). *Utility-Scale Smart Meter Deployments, Plans, & Proposals*. www.edisonfoundation.net/iee/Documents/IEE_SmartMeterRollouts_0512.pdf.

[14] U.S. Department of Energy (DOE). (2010). *Data Access and Privacy Issues Related to Smart Grid Technologies*. http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf.

[15] *Id*.

[16] Smart Grid Interoperability Panel Cyber Security Working Group. (2010). *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*. National Institute for Standards and Technology (NIST). www.nist.gov/smartgrid/upload/nistir-7628_total.pdf.

2.2 Addressing Utility Concerns

Historically, many utilities have been reluctant to share customer data and have raised concerns regarding the following:

- The potential for customer complaints or legal exposure for unauthorized sharing
- The cost, infrastructure, and transactional burden of sharing large quantities of data, especially with the advent of smart meters
- The surrendering of economically valuable data.

However, utilities often share customer information with entities that are under contract to provide a specific service (e.g., those providing billing services or outage repairs) and such sharing is routinely accepted as a function of performing essential utility services. Increasingly, regulators are facing the question of how to allow the sharing of customer data while protecting customer privacy.

2.3 Electricity Usage Data

For the purpose of defining customer data related to energy-efficiency, there are three types of relevant data: personally identifiable information (PII), customer-specific energy usage data (CEUD), and aggregated data.[17] PII typically consists of an individual's name and address.[18] However, depending on the state, it may include other information such as Social Security numbers, account number, rate class, contact information, credit information, tax identification numbers, and driver's license numbers. CEUD includes all data specific to an individual customer's energy use, such as total and time-differentiated energy use.[19] For the purposes of this report, the combination of PII and CEUD data are referred to as "customer data." Aggregated data are data that the utility assembles from multiple residences, tenants, or commercial buildings to provide information about energy consumption across a specified area.[20]

2.3.1 Traditional Meter Data

Many utilities store and retain monthly billing data for a specified time period, most for at least twelve to eighteen months and often upwards of 10 years, and make it available to their customers upon request. Historic billing data allow customers (and service providers) to assess seasonal energy consumption trends and evaluate energy efficiency upgrades. For example, an EESP can use monthly billing data, combined with additional analytics and diagnostic tools, to identify buildings that could benefit from energy efficiency upgrades or buildings that may have inefficient heating or air conditioning systems.

Several states (e.g., Vermont and Washington) contemplated the disclosure of this data to third parties as early as the late 1990s.[21] In Vermont, the electric utilities were required to disclose customer data to the third-party program administrator, the Energy Efficiency Utility (EEU), which was overseen by the Public Service Board.[22] Further, the utilities could not require customer consent prior to disclosing the data to the EEU (see Appendix A for more information). By contrast, Washington essentially required its utilities to obtain specific customer approval to disclose energy usage data.[23] In both cases, the states recognized the value of the data to third parties and

[17] U.S. Department of Energy (DOE). (2010). *Data Access and Privacy Issues Related to Smart Grid Technologies*. http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf.

[18] *Id*.

[19] *Id*.

[20] *Id*.

[21] See, for example, Wash. Admin. Code §480-100-153 (2001).

[22] See Vermont Public Service Board. (2000). *Investigation into Dispute Regarding the Provision of Customer Information to Efficiency Vermont by the Village of Hyde Park Electric Department, et al.* Docket No. 6379.

[23] Wash. Admin. Code §480-100-153 (2001)

addressed consumer privacy concerns by limiting—but not preventing—disclosure. However, the advent of smart meter technology has changed the context of this debate to some extent.

2.3.2 Smart Meter Data

Smart meters have interval recording capability (e.g., every 15 minutes, hourly) and integration with some type of communication system that allows the meter information to be remotely collected by the utility. This more granular data raises additional privacy concerns because the data can be used to identify specific customer activity. For example, in California, Pacific Gas & Electric's (PG&E) smart meters record consumers' electricity consumption on an hourly basis.[25] Utilities can (and some do) collect data at more frequent intervals, but at a cost. Data collection at more frequent intervals has the potential to provide the customer (or third party) with more comprehensive—and often more valuable—information.

Protocols for data transfer are important to realize the full potential of smart meters. Data transfer involves two key considerations: (1) the interface by which a customer (or third party) accesses the data; and (2) the machine-readable structure of the data. Green Button provides a standardized approach to both of these.

THE GREEN BUTTON

The energy industry developed the Green Button Initiative[24] in response to the Administration's challenge for industry to create easy access to energy usage data in a "consumer-friendly and computer-friendly format." Under the program, utility customers can access their own electricity usage data through online utility accounts. With the simple push of a (green) button, customers can view or download their data. The data are both tabulated and presented graphically to show hourly, daily, and/or monthly trends in use.

The downloadable data are available in a standardized XML-based electronic file type, (e.g., .xml or .xls) which customers can then export to other programs. Because the file types are standardized, third parties can more easily develop software to analyze the data and suggest various energy (and cost) saving options. By contrast, if utilities do not follow a uniform approach, EESPs would have to develop software specific to each utility's data set, which results in higher transaction costs.

2.3.3 Aggregated Data

Aggregated data are data that the utility assembles from multiple customers to provide information about energy consumption across a specified building or geographic area. Aggregated data can be used to inform energy efficiency program plans, landlords about a building's energy consumption when tenants are responsible for their own meters, load forecasting, and energy efficiency policy.

2.4 Energy Efficiency Service Providers and Other Entities Interested in Data Access

It is useful to distinguish among the three types of entities involved in the provision of energy efficiency services that are likely to be interested in access to customer data:

- **Program administrators** of energy efficiency programs funded by utility customers are typically under direct supervision by a state regulatory agency (e.g., PUC). Utilities are program administrators of energy efficiency programs in approximately 40 states, while state agencies or profit/nonprofit companies manage programs in eight states.
- **Program implementation contractors (PICs)** are entities that work on behalf of the program administrator (i.e., sub-contractors) and have a contractual relationship to provide various types of services needed in

[24] "Green Button Data Demonstration." (2012). www.greenbuttondata.org.

[25] "SmartMeter™ Network—How It Works." (2012). Pacific Gas and Electric Company (PG&E). www.pge.com/myhome/customerservice/smartmeter/howitworks/.

program design, implementation, or evaluation (e.g., energy audits, project design, inspection, verification of installations, monitoring of savings). Typically, a PIC has access to customer information necessary to perform the services for which they have been contracted through the utility. Most state PUCs require the electric utility to pass its privacy policy along to the sub-contractor in the service contract. As a result, the PUC has some authority over this type of entity's privacy policies.

- **Energy efficiency service providers (EESPs)** are third-party market participants that offer and provide energy efficiency services or products to end users but do not have a direct contractual or legal relationship with the program administrator or state PUC. EESPs include architectural and engineering firms providing energy efficiency design services, including lighting, HVAC, and motors. EESPs may also include contractors that sell and install high-efficiency products (e.g., insulation, windows) and/or firms that provide energy audit services. Some groups of EESPs have expressed a strong interest in obtaining access to certain types of customer data in order to provide energy information services or reduce their marketing costs. Providing the aggregated energy usage of tenants can inform building owners about potential investments in energy efficiency. In addition, many state regulators have an interest in leveraging spending by program administrators and/or are interested in transforming markets over the long-term so they may be interested in supporting EESPs.

A list of potentially interested entities is included in Table 1.

Table 1. Examples of Entities Interested in Customer Data to Support Energy Efficiency

Program Administrators (Direct PUC Oversight)	Program Implementation Contractors (PIC) (Indirect PUC Oversight)	Energy Efficiency Service Providers (EESP) (No PUC Oversight)
• Nonprofit or for-profit companies, or state energy agencies, that administer utility customer-funded programs • Competitive retail electric service providers	• Energy efficiency implementation contractors • Billing agents	• Architectural and engineering design firms • Home performance contractors (e.g., lighting, HVAC, insulation) • Appliance and equipment retailers • Energy audit and commissioning services contractors • Energy management service providers • Independent research organizations • Local government or nonprofit entities implementing energy efficiency programs • Building owners making efficiency investments that lower tenant energy usage

3. Existing State Policies Regarding Customer Usage Data

3.1 Approach

The primary objective of this guide is to identify policy options designed to manage access to customer data by third parties. The research team conducted a phone and email inquiry of all 50 states and the District of Columbia, and searched legal databases (e.g., Westlaw, Lexis Nexis, and Public Utilities Reports available through Westlaw) and public utilities commission (PUC) websites between January and April 2012 as part of the background research for this project.

Table 2 provides a summary by state of statutes, regulations, PUC orders, and proposed legislation identified through those research efforts. As of April 2012, the research team found at least eight jurisdictions that had statutes, regulations, and/or orders that governed access to customer data: California, Colorado, Oklahoma, Oregon, Texas, Vermont, Washington, and Wisconsin.[26]

Four other jurisdictions (DC, MD, NJ, OH) were identified that have adopted a "general data protection statute" which connotes a law that applies generally to the treatment of customer data by utilities (and in some instances, other business entities) as distinct from statutes and regulations that deal specifically with such data in the context of energy efficiency and/or smart grid applications. Examples of action were discovered in seven states where commissions have opened dockets on this issue, typically driven by increased attention to data privacy or security in the context of smart grid legislation and/or utility advanced metering infrastructure (AMI) deployment.

Approximately 30 states have "no ascertainable authority," as shown in Table 3. This does not necessarily mean there is no applicable law, regulation, or other regulatory guidance—only that the research efforts did not reveal any such authority as of April 2012.[27] Utilities routinely must address questions related to customer data privacy and typically apply privacy principles derived from general civil law in states that do not appear to have adopted explicit public policies on this issue.

3.2 Existing Policy Overview

This section summarizes approaches taken by various states and highlights several broad themes based on a review of the states that had adopted explicit policies regarding providing access to customer data.[28] Generally, state PUCs and/or legislatures have taken the following approaches: (1) no explicit policy in place, (2) adopted consent requirements that apply to third parties under contract to the utility, (3) customer consent required for certain uses, (4) policies for access to aggregated data. Appendix A includes more detailed case studies of four states. State approaches on several broader issues are also highlighted: (1) efforts to enact registration requirements for third parties (2) utility charges for and cost recovery associated with data disclosure, and (3) methods that states use to enforce policies (e.g., liability).

[26] Several jurisdictions (e.g., the District of Columbia, California, and Maryland) had confronted the question of third-party data access in the context of retail restructuring and the attendant need for non-utility energy suppliers to reach customers.

[27] Readers should keep in mind that in all jurisdictions, there are background rules, derived from judge-made common law, commercial law, or otherwise, that utilities will typically apply in the absence of specific guidance.

[28] In many states, statutes, regulations, and orders on third-party access to customer data are often quite detailed and complex; hence, this report provides only a higher level summary.

Table 2. State Statutes, Regulations, Orders, and Dockets Governing Third-Party Access to Energy Efficiency Data

State	Policy
Arkansas	**Docket:** In the Matter of the Consideration of Smart Grid, Advanced Metering Infrastructure, and Related Demand Response Technologies. Docket No 10-102-U, Arkansas Public Service Commission.
California	**Statute:** Cal. Pub. Util. Code §8380 & 8381. **Order:** Decision Adopting Rules to Protect the Privacy & Security of the Elec. Usage Data of the Customers of Pacific Gas and Elec. Company, Southern California Edison Company, & San Diego Gas & Electric Company. Decision 11-07-056. California Public Utilities Commission. (July 28, 2011).
Colorado	**Regulation:** 4 Colo. Code Regs. §3000 et seq.
Delaware	**Order:** Customer Information. Order No. 5469 **Docket:** In the Matter of the Application of Delmarva Power & Light Company d/b/a Connective Power Delivery for Approval. PSC DOCKET NO. 99-582.
District of Columbia	**General Data Protection Statute:** D.C. Code § 34-1507.
Maryland	**General Data Protection Statute**: Md. Pub. Utils. Code Ann. § 7-505(b)(6). **Regulation**: Code of Md. Regs. 20.53.07.02.
Michigan	**Docket:** In the Matter, on the Commission's Own Motion, Commencing a Proceeding to Implement Smart Grid. Docket No.U-15278, Michigan Public Service Commission.
Minnesota	**Docket:** Xcel Energy's proposed "privacy tariff." Docket No. E002/M-12-188.
Nevada	**Docket:** Application of Nevada Power Company d/b/a NV Energy for approval of its 2010-2029 IRP. Docket No. 10-02009, Public Utilities Commission of Nevada.
New Jersey	**General Data Protection Statute**: N.J. Stat. § 48:3-85(b). **Regulation**: N.J. Admin. Code 14:4-7.8
New York	**Docket**: Proceeding on Motion of the Commission to Consider Regulatory Policies Regarding Smart Grid Systems and the Modernization of the Electric Grid. Case 10–E–0285.
Ohio	**General Protection Statute:** Ohio Admin. Code 4901:1-10-24(E)(1)(2). **Docket:** Review of the Consumer Privacy Protection Customer Data Access, and Cyber Security Issues. Case No. 11-277-GE-UNC, Public Utilities Commission of Ohio.
Oklahoma	**Statute:** Electric Utility Data Protection Act. Okla. Stat. tit. 17 §710.
Oregon	**Regulation:** Or. Admin R. 860-038-0540.
Pennsylvania	**Statute:** 66 Pa. Cons. Stat. § 2807 **Regulation:** 52 Pa. Code § 54.8.
Texas	**Statute:** 2 Tex. Util. Code §39.107 **Substantive Rule:** 25.130(j)(1).
Vermont	**Order:** VEIC Order of Appointment Process & Administrative Document. Docket 7466. State of Vermont Public Service Board. **Docket:** Smart Metering & Alternative Rate Design. Docket 7307. State of Vermont Public Service Board.
Virginia	**Proposed Legislation:** House Bill 312 (the "Opower Bill").
Washington	**Regulation:** Wash. Admin. Code §480-100-153. **Docket:** Number UE-990473, Washington Utilities & Transportation Commission.
Wisconsin	**Regulation:** Wis. Admin. Code § PSC 113.0505(2); Wis. Admin. Code § PSC 113.01(2) **Order:** Docket 9501-GF-101, Wisconsin Public Service Commission.

Table 3. States with no Ascertainable Authority Governing Third-Party Access to Energy Efficiency Data

Alabama	Kansas	New Mexico
Alaska	Kentucky	North Carolina
Arizona	Louisiana	North Dakota
Connecticut	Maine	Rhode Island
Florida	Massachusetts	South Carolina
Georgia	Mississippi	South Dakota
Hawaii	Missouri	Tennessee
Idaho	Montana	Utah
Illinois	Nebraska	West Virginia
Indiana	New Hampshire	Wyoming
Iowa		

3.3 States without Specific Policies

The fact that a state does not have a statute, regulation, or rule that directly addresses whether or not a third party can access a customer's data does not mean that there are no policies in place that address this issue. In some states where a specific policy is not in place, utilities may have their own company policies that govern access to customer energy usage data. Several of these jurisdictions have general privacy statutes that require that a utility obtain the customer's consent in writing before disclosing the customer's data (e.g., District of Columbia).[29] Statutes and regulations in the District of Columbia, Ohio, and Illinois require an entity to transfer a customer's data upon the customer's request, or require a utility to provide generic customer information to retail electric providers.[30]

3.4 Access to Customer Data by Contracted Third Parties

Some jurisdictions have promulgated policies that cover program implementation contractors (PICs) who have ongoing contractual relationships with a utility or are themselves legally considered a utility subject to oversight by regulators.

3.4.1 Utility Contract

Some states (e.g., Colorado and Oklahoma) have adopted statutes or regulations that allow PICs to access a customer's data with additional protections if a utility has a contract with that entity to assist the utility in providing regulated services. For example, Colorado state law requires the PIC to implement and maintain reasonable security procedures that are equal to or greater than the security procedures maintained by utilities, use customer data solely for the purpose of the contract, destroy customer data that are no longer useful for the contract, and sign a non-disclosure agreement with the utility.[31] In Oklahoma, a PIC may have access to the customer's data, but the disclosure must be limited to the specific information necessary for the entity to carry out its responsibilities. Additionally, a representative of the PIC must agree in writing to maintain the security and

[29] D.C. Code §34-1507.

[30] See D.C. Code §34-1507; Ill. Admin. Code. tit. 83 §410.210; Ohio Admin. Code 4901:1-10-24(E)(1)(2).

[31] See 4 Colo. Code Regs. 723-3 Part 3 §3029(a); Okla. Stat. tit.17 §710.6(A).

confidentiality of customer information, and the third party must limit the use of customer information to the provision of services to the electric utility.[32]

For entities under contract to utilities in California, the California PUC regulates access to customer energy usage data based on the third party's purpose for using the data. For example, PICs may use data for purposes that California classifies as either a "primary purpose" or "secondary purpose."[33] A utility does not have to obtain a customer's consent to disclose information to a PIC when the entity is using that information for a primary purpose. A primary purpose includes energy efficiency, demand management, and energy management programs under utility administration.[34] Even though the customer does not have to consent to disclosure, the PIC must have reasonable security procedures and practices in place to prevent unauthorized access, destruction, use, or modification of the data, and prohibits the use of the data for a purpose other than the purpose stated in the contract.[35] Any other use of the data is a secondary purpose and its disclosure requires customer consent.[36]

3.4.2 PUC Contract

In other states, nonprofit or for-profit entities administer state energy efficiency programs and services. These companies have access to customer energy usage data but have strict confidentiality policies to prevent unauthorized entities from obtaining such data. For example, in Vermont, the energy efficiency utility and any energy efficiency utility contractor must agree to follow the guidelines in the Confidential Information Management System (CIMS) and cannot provide any confidential information to affiliates not directly involved with the energy efficiency utility.[37] In Wisconsin, Focus on Energy administers energy efficiency programs funded by utility customers. In order to receive customer information, Focus on Energy must enter into an agreement with the releasing utility that: (1) protects the confidentiality of customer information, (2) specifies how long Focus on Energy will retain the information, (3) specifies when Focus on

NEGOTIATING DATA ACCESS WITH THE LOCAL UTILITY

The Neighbor to Neighbor Energy Challenge (N2N) in Connecticut— administered by Earth Markets, an independent EESP program administrator—is working with the citizens of 14 Connecticut towns to complete comprehensive energy upgrades in ten percent of utility customer residences in those areas. To achieve their goals and measure their success, N2N needed 24 months of historical usage data, and access to ongoing data, for participating customers.

Lacking guidance from regulators, N2N entered into six months of ultimately successful negotiations with the local utility, Connecticut Light & Power. The result was a detailed contract and a meticulously crafted set of technical specifications for data exchange and security. The utility has already used the agreements as a template for similar arrangements with other programs.

Consistent standards adopted by either the legislature or utility regulators may have improved this process and allowed N2N to get a quicker start on deploying measures in its 14 communities.

[32] Okla. Stat. tit.17 §710.6(A).

[33] California Public Utilities Commission. (2011). *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.* Decision 11-07-056. These rules were recently extended to cover natural gas data generated by advanced meters, as well as community choice aggregators and electric service providers who serve small commercial and residential customers (see CPUC Decision 12-08-045).

[34] Utilities in California have also provided research institutions access to customer data where the research being conducted furthers a public goal. These agreements are negotiated between the research institution and include a non-disclosure agreement and strict data management and security requirements.

[35] Cal. Pub. Util. Code §8380(a)(2).

[36] California Public Utilities Commission. (2011). *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.* Decision 11-07-056.

[37] See Vermont Public Service Board. (2000). *Investigation into Dispute Regarding the Provision of Customer Information to Efficiency Vermont by the Village of Hyde Park Electric Department, et al.* Docket No. 6379.

Energy will destroy the information, and (4) pays a monetary penalty for any unauthorized release of data.[38]

3.5 Customer Consent

3.5.1 Affirmative Customer Consent

Some states (e.g., Washington and Colorado) require customer consent to grant access to the customer's data and specify the method that a customer must use to consent. For example, Washington requires consent in written or electronic format.[39] Colorado mandates that customers fill out a form that contains certain required information.[40] Additionally, Washington requires that customers know what entity is accessing their data and must consent to each instance of disclosure, and the utility must maintain a record of each instance of disclosure.[41]

Texas requires customer authorization for disclosure and also specifies that all generated meter data belong to the customer.[42] Specifying ownership of customer usage data can be effective because certain rights flow from the ownership. For example, often the ownership of data gives the owner the right to control the data and use of the data. However, conferring a right of ownership to the customer may complicate other aspects of the utility business. Therefore, to decrease disputes over who has the right to control the use of a customer's energy usage data, a utility regulator can specify whether the customer, utility, or a third-party entity owns and/or controls access to the data.[43]

THE CHALLENGE OF CHANGING CUSTOMER CONSENT FORMS MIDSTREAM

Under a $25 million grant from the U.S. Department of Energy's Better Buildings Neighborhood Program, the EnergySmart program in Boulder County, Colorado is improving the energy efficiency of at least 10,000 homes and 3,000 businesses by June 2013.

When they began the program, County officials were able to reach an agreement directly with a local utility, Xcel, to gain access to customer energy use data. The agreement included a one-page form that EnergySmart program participants would sign providing consent. In Spring 2012, the Colorado PUC adopted new rules on customer data privacy, including a mandatory, three-page disclosure form. This change created some uncertainty over whether the previous disclosure agreement was valid or if a new agreement would be necessary.

Regulators considering new customer data access and protection policies may need to review whether any existing policies are already in use by utilities and provide explicit guidance on whether such policies are acceptable under the new framework.

3.5.2 Consent for Secondary Commercial Purposes

California, Colorado, and Oklahoma all require customer consent before the utility may give any third party a customer's data for secondary commercial purposes (i.e., purposes unrelated to the provision of utility or energy efficiency services).[44]

3.6 Aggregated Data

In states that have adopted policies to regulate access to energy efficiency data, a utility's disclosure of aggregated data is typically treated differently than a utility's disclosure of a customer's individual energy usage data. The difference in regulation likely stems from the fact that individual customer privacy is more protected once

[38] Wisconsin Public Service Commission. (2009). *Provision of Energy Utility Customer Information to Focus on Energy*. Docket No. 9501-GF-101.

[39] Wash. Admin. Code §480-100-153.

[40] 4 Colo. Code Regs. 723-3 Part 3 §3028.

[41] Wash. Admin. Code §480-100-153.

[42] See 2 Tex. Util. Code §39.107(b).

[43] It is not within the scope of this paper to investigate which ownership path provides the greatest benefit to uses of data for energy efficiency.

[44] See Cal. Pub. Util. Code §8380(c); 4 Colo. Code Regs. 723-3 Part 3 §3029(a); Okla. Stat. tit.17 §710.6.

aggregated. Therefore, a utility is typically not precluded from sharing aggregated data. However, regulations often require that the utility undertake certain efforts to ensure that all information is removed from the aggregated data that would allow a PIC or EESP to identify a customer. For example, in Colorado, a particular aggregation must contain at least fifteen customers or premises. Further, no single customer's data may comprise more than 15 percent of the total aggregated data.[45] This is otherwise known as the "15/15 Rule."[46] In Oklahoma, aggregated data must contain a "sufficient number of similarly situated customers within a particular geographic area so that the daily usage routines or habits of an individual customer could not reasonably be deduced from the data."[47] Vermont allows utilities to aggregate data if the sample is no smaller than the "town level."[48]

State PUCs that want to facilitate development of energy efficiency services should also consider supporting public disclosure of other information collected by program administrators or evaluators that may have significant value to private sector market entities. For example, market assessments, impact evaluations, and other research conducted to ascertain either the potential or actual effects of ratepayer-funded energy efficiency initiatives are integral parts of these programs. The resulting written reports contain a wealth of aggregated customer data that could be used by third parties to target programs, products, and services. These studies are made available on public web sites in many jurisdictions.[49] It does not appear that any jurisdiction has explicitly considered the privacy implications, if any, of this aggregated data being publicly available.

3.7 Third-Party Registration Requirements

A number of states have addressed the contentious issue of how state PUCs can enforce data privacy policies in dealing with third parties that are not under the jurisdiction of the PUCs. For example, Colorado only allows utilities to provide customer data to PICs to perform regulated services, which allows the PUC to retain jurisdiction.[50] In California, the PUC has indicated that utility tariff changes should include processes through which a commission can oversee third parties that obtain data from the utility, such as a registration policy.[51] In Vermont, energy efficiency utilities are under the jurisdiction of the Public Service Board.[52] Therefore, those entities are subject to the board's orders and state regulations.[53] However, if a customer provides their information to a third party directly, rather than the utility providing the data, the PUC may not have jurisdiction over that third party. In such a situation, an entity other than a state PUC (e.g., attorney general or Department of Commerce) may need to monitor such transfers of information.

[45] 4 Colo. Code Regs. 723-3 Part 3 §3031(b)(c).

[46] Even with the 15/15 rule, the utility is not required to disclose data if the disclosure would compromise the customer's data.

[47] See Okla. Stat. tit.17 §710.7(B)(2).

[48] See Vermont Public Service Board. (2010). *Investigation into Petition Filed by Vermont Department of Public Service Re: Energy Efficiency Utility Structure.* Docket No. 7466.

[49] Such jurisdictions include California, see "California Measurement Advisory Council." (2012). www.calmac.org; New York, see New York State Energy Research and Development Authority (NYSERDA). (2012). *New York Energy $mart Evaluation Contractor Reports*. www.nyserda.ny.gov/en/Program-Evaluation/NYE$-Evaluation-Contractor-Reports/2012-Reports.aspx; the Pacific Northwest states, see Northwest Energy Efficiency Alliance. (2012). *Market Research and Evaluation Reports*. http://neea.org/resource-center/market-research-and-evaluation-reports; and Wisconsin, see Focus on Energy. (2012). *Evaluation Reports*. www.focusonenergy.com/evaluation-reports/default.aspx.

[50] See 4 Colo. Code Regs. 723-3 Part 3 §3029(a).

[51] See California Public Utilities Commission. (2011). *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.* Decision 11-07-056. Third parties that obtain data from the customer are not subject to the rules or PUC jurisdiction.

[52] Vermont Public Service Board. (2010). *Investigation into Petition Filed by Vermont Department of Public Service Re: Energy Efficiency Utility Structure.* Docket No. 7466.

[53] *Id*.

3.8 Cost Recovery

States vary as to whether a utility can charge an EESP for costs associated with providing or selling customer data to an EESP. There are three primary questions at issue:

- Can a utility sell customer data to an EESP?
- Can a utility charge an EESP for the costs that the utility incurs in providing the data?
- Can a utility recover its data-related costs through a general rate case or other proceeding to approve specific investments (e.g., energy efficiency program portfolios, billing system upgrades, or smart grid deployments)?

Regarding the first issue, California forbids a utility from selling customer data for any reason.[54] Regarding the second issue, Oklahoma allows an electric utility to charge a reasonable fee for providing nonstandard usage such as real-time data, which allows utilities to recover the actual costs incurred in providing the data.[55] In contrast, in Colorado, the utility must provide access to standard format data without charge.[56] Jurisdictions without special provisions addressing this question are likely to have these costs fall within a utility's general revenue requirement.

3.9 Liability and Penalties for Violating State Privacy Policies

A situation may arise where a utility, PIC, or EESP violates the state's privacy policy. In such instances, it is important to determine who is liable for that harm; the state privacy policy may help provide that clarification.[57] To determine what entity is liable for the harm to the customer, states typically look at: (1) which entity released the information, (2) whether that data were aggregated, and (3) whether the release of the information was accidental or intentional. In California, if a customer chooses to disclose his or her data to a third party that is unaffiliated with a utility, then the utility is not liable for the security of that data or its misuse.[58] In Colorado, a utility is not held liable for the release of aggregated data, but the intentional release of customer-specific data can lead to civil and criminal penalties.[59] In Vermont, if an energy efficiency utility intentionally or accidentally releases confidential information, the energy efficiency utility must indemnify the Public Service Board for any claims that result.[60] In Wisconsin, if Focus on Energy (the third-party program administrator for energy efficiency programs) releases any information, it may be liable for a monetary penalty.[61]

[54] See California Public Utilities Commission. (2011). *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*. Decision 11-07-056. See also Cal. Pub. Util. Code Section 8380(b)(2).

[55] See Okla. Stat. tit.17 §710.5.

[56] See 4 Colo. Code Regs. 723-3 Part 3 §3026(e).

[57] The lack of a customer privacy policy does not isolate the utility from liability from misuse.

[58] Cal. Pub. Util. Code §8380(f).

[59] 4 Colo. Code Regs. 723-3 Part 3 §3976.

[60] Vermont Public Service Board. (2010). Investigation into Petition Filed by Vermont Department of Public Service Re: Energy Efficiency Utility Structure. Docket No. 7466.

[61] Wisconsin Public Service Commission. (2009). *Provision of Energy Utility Customer Information to Focus on Energy*. Docket No. 9501-GF-101.

4. Legal and Policy Considerations Regarding Accessing Energy Usage Data

Neither Congress nor any federal agency has acted to restrict access to energy usage information.[62] However, there are a number of federal policy initiatives that could influence—directly or indirectly—customer data access and privacy concerns. Additionally, the U.S. Supreme Court recently indicated that there may be constitutional limits on whether state regulators may restrict third-party access to data.[63] Therefore, it is important for state policymakers to understand these considerations when drafting statutes, rules, regulations, and orders related to data access issues to lessen the possibility of legal challenges to these policies.

4.1 Relevant Federal Privacy Practices

As states consider the best ways to enact policies that govern access to customer data, there are several relevant federal privacy policies that can inform decision making at the state level. To date, neither Congress nor any federal agency has adopted any privacy standards that are specific to retail electric utilities or energy efficiency services; however, there are several federal initiatives that are relevant to electric utilities and energy efficiency service providers (EESPs) including Fair Information Practice Principles (FIPPs), the Consumer Privacy Bill of Rights, FTC Codes of Conduct, non-binding industry standards, and a number of emerging initiatives discussed below. This section discusses these initiatives and their relevance to the use of utility customer data for the promotion of energy efficiency services.

4.1.1 Fair Information Practice Principles and Consumer Privacy Bill of Rights

Many modern privacy protection laws are based on "fair information practice principles," otherwise known as FIPPs. At their inception in the 1970s and 1980s, FIPPs were broad, aspirational privacy principles.[64] Government agencies and legislatures have taken these principles and integrated them into various laws and policies. For example, in a 1998 report to Congress, the Federal Trade Commission distilled the FIPPs into five core principles of privacy-protective practices.[65]

In February 2012, the White House released the Consumer Privacy Bill of Rights, which updates FIPPs to reflect the more decentralized and pervasive collection of personal data that exists today, compared to when FIPPs were initially developed. As part of the Administration's Privacy Blueprint, the Consumer Privacy Bill of Rights could provide the basis for codes of conduct tailored to the specific types and amount of data that specific industries collect. The Privacy Blueprint also states that "it may be appropriate to allow states to enact laws that apply the Consumer Privacy Bill of Rights to personal data in sectors they closely regulate, such as electricity distribution."[66] Thus, even if there were federal legislation based on the Consumer Privacy Bill of Rights, Congress may defer to states to enact laws codifying the principles in the Consumer Privacy Bill of Rights that govern specific industries, like electricity distribution. In any event, any enacted Consumer Privacy Bill of Rights would likely apply to granular energy consumption data that smart meters collect and transmit. The White House noted that it would push for a Consumer Privacy Bill of Rights to apply to any "commercial uses of personal data…including aggregations of data" that may be linked to a specific individual.

---

[62] *See* Schira, A. (2011). "Protecting Progress and Privacy: The Challengers of Smart Grid Implementation." *A Journal of Law and Policy for the Information Society.* (evaluating possible application of the Privacy Act of 1974, the Electronic Communications Privacy Act, and Section 5 of the Federal Trade Commission Act, to metering data).

[63] On June 23, 2011, the U.S. Supreme Court, in *Sorrell v. IMS Health, Inc.*, held that a Vermont statute restricting the sale, disclosure, and use of pharmacy records containing the prescribing practices of doctors for marketing purposes by pharmaceutical companies violated the First Amendment's protection of commercial advertising speech.

[64] Cate, F.H. (2006). *The Failure of Fair Information Practice Principles: Consumer Protection in the Age of the Information Economy*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972.

[65] Federal Trade Commission. (1998). *Privacy Online: A Report to Congress*. www.ftc.gov/reports/privacy3/toc.shtm.

[66] White House. (2012). *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. www.whitehouse.gov/sites/default/files/privacy-final.pdf.

The Consumer Privacy Bill of Rights is based on seven core principles, which are compared to the Department of Homeland Security (DHS) FIPPs,[67] in Table 4 below. In each instance, the principle adopted in the Consumer Privacy Bill of Rights serves as an adaptation and refinement of the corresponding FIPP; the creators of the former document revised the title of each principle accordingly.

Table 4: Comparison of DHS FIPPs and Consumer Privacy Bill of Rights

DHS Fair Information Practice Principles (FIPPs)	Consumer Privacy Bill of Rights
Transparency Notify individuals about the dissemination, maintenance, collection, and use of their data	Transparency Easily understood mechanisms that reflect the scale, scope, and sensitivity of the personal data collected
Individual Participation Seek individual consent for the collection, use, dissemination, and maintenance of personally identifiable information	Individual Control Policy that makes it as easy for an individual to withdraw consent as it was to grant consent in the first instance
Purpose Specification and Data Minimization Collect data that are directly relevant and necessary to accomplish the specified task	Respect for Context Consumers should expect companies to handle data consistent with the context of the consumer's consent
Use Limitation Should only share data to accomplish the task specified	Focused Collection Consumers should have a right to set reasonable limits on data use and collection
Data Quality and Integrity Ensure that data are accurate, relevant, timely, and complete	Access and Accuracy Consumers should have the ability to both access and correct any incorrect data
Security Protect data against risks of loss, unauthorized access or use, destruction, modification, etc.	Security Consumers have a right to secure and responsible handling of personal data
Accountability and Auditing Audit actual use to demonstrate compliance	Accountability Companies must take appropriate measures to ensure compliance, even if transferring data to another party

4.1.2 FTC Codes of Conduct

In March 2012, the Federal Trade Commission (FTC) issued a final report outlining a set of voluntary "best practices" for businesses that collect, maintain, and use consumer data.[68] The FTC opted to exempt from the presumptive standards entities that collect only "non-sensitive data" from fewer than 5,000 customers per year and do not share this data with third parties.[69] Similarly, the FTC limited the applicability of the standards to data that can be "reasonably linked to a specific consumer, computer, or other device."[70]

[67] U.S. Department of Homeland Security. (2008). *Privacy Policy Guidance Memorandum*. www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[68] Federal Trade Commission. (March 2012). *Protecting Consumer Privacy in an Era of Rapid Change*. http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[69] *Id.*

[70] *Id.*

The FTC urged companies to "simplify" consumer choice in the privacy realm, concluding that these entities "do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law."[71] However, the FTC recommended that companies should obtain "affirmative express consent" before using consumer data "in a materially different manner than claimed when the data was collected" or when collecting "sensitive data."[72]

4.1.3 Enforceable Codes of Conduct

In July 2012, the National Telecommunications and Information Administration (part of the U.S. Department of Commerce) began the process of convening stakeholders for the purpose of developing industry-specific privacy codes of conduct.[73] The codes would not bind any company unless it chooses to adopt them. If a company did adopt one of these voluntary codes, the FTC could enforce future breaches as an unfair or deceptive practice.[74]

With regard to smart meter privacy, the FTC's jurisdiction varies depending on the nature of the utility. While the FTC has jurisdiction over investor-owned utilities and for-profit cooperatives, it does not have jurisdiction over federally owned utilities, such as the Tennessee Valley Authority (although federal entities are subject to the Federal Privacy Act). The FTC's jurisdiction over nonprofit utilities is less clear and may depend on the particular arrangements governing that utility. However, state attorneys general may have broader enforcement jurisdiction in their states.

4.1.4 Non-Binding Industry Standards

Non-binding industry standards or model business practices models have been successfully applied to efforts such as LEED®-certified buildings and ENERGY STAR®. In the context of utility customer data, if a third party can demonstrate that it satisfies various data security measures, that party could be certified under a non-binding industry standard and customers could feel more secure sharing their data.

One example of a standard developed for the distribution of smart meter data is the North American Energy Standards Board's (NAESB's) Energy Service Provider Interface (ESPI) standard, developed with the support of the National Institute of Standards and Technology (NIST).[75] This copyrighted standard was developed with consideration to the Green Button initiative, and provides the added benefit of compatibility with Green Button requirements. ESPI envisions a framework within which the utility's data are transferred to a "data custodian" that would have the responsibility of authorizing third-party access to the data. The ESPI standard primarily addresses the process by which the custodian authorizes a third party and then transfers the data.[76] Precautions include the following: limitations on the amount of data the third party can access, granularity of the data that the third party can access, a default restriction that prevents the third party from modifying the data, and very specific requirements regarding how the data are actually transferred.[77]

This type of standard is especially beneficial for state officials because they can direct concerned customers to a very detailed outline of the standards that third parties must meet in order to be authorized. Additionally,

[71] *Id*.

[72] *Id*. at viii and 46-48 (referencing, as examples of sensitive data, information about children, financial and health information, Social Security numbers, and certain geo-location data).

[73] See National Telecommunications and Information Administration. (2012). *Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct*. Publication Title 77 F.R. 13098. www.gpo.gov/fdsys/granule/FR-2012-03-05/2012-5220/content-detail.html.

[74] The FTC's authority to sanction unfair or deceptive trade practices is found at 5 U.S.C. § 45.

[75] North American Energy Standards Board (NAESB). (2010). *Req. 21—Energy Service Provider Interface* (short article). www.naesb.org/ESPI_Standards.asp.

[76] See, e.g. Req. 21.3.1.15–17.

[77] See, e.g. Req.21.3.1.6 & 21.6.1.1.

customers can either share their data through data custodians to authorized third parties, or transfer data directly to a third party. Thus, customers can be better assured that third parties are following very strict data security practices, making it unnecessary for state regulators to develop and implement the standards themselves.

4.1.5 Privacy Seal Initiatives

In an effort to improve the management and oversight of e-commerce, several "Privacy Seal" initiatives have been developed and promoted. Essentially, several large groups involved with e-commerce (e.g., the Better Business Bureau) have developed programs through which an online business can become accredited or certified as meeting certain privacy standards. Once the business is accredited or certified, the business may post an easily recognizable seal on its website to indicate its status. In addition to the privacy standards, the Better Business Bureau requires businesses to adhere to several basic conditions such as honesty, transparency, and disclosure.[78] Another example is the "TRUSTe" program, which examines an e-business' privacy policy and verifies that the business meets all federal and state regulations, including the standards established by the Consumer Privacy Bill of Rights.[79]

The private accrediting organization is responsible for ensuring that the businesses maintain their practices and that unaccredited organizations do not display the seal. The private organizations have an incentive to police the use of their seal, because the value of their accreditation depends on their ability to maintain these strict standards.

4.1.6 Summary of Federal Privacy Practices

Many of the federal privacy practices and industry standards share the following basic principles:

- Requiring customer consent to share data, and allowing customers to revoke consent
- Allowing customers to access data about them
- Disclosing privacy practices, collection practices, sharing practices, etc.
- Limiting the amount of data transferred to purposes specified
- Limiting the type, or granularity, of the data transferred
- Requiring precautions against data security threats
- Requiring a review to ensure compliance with the other principles
- Using public relations as a tool to encourage compliance.

Although none of these practices were adopted with the electric industry or energy efficiency specifically in mind, they are examples of policy principles that state regulators and legislators can use as backdrops against which to make state policy.

4.2 Fourth Amendment

The Fourth Amendment secures an individual "against unreasonable searches and seizures" by federal and state authorities.[80] The U.S. Supreme Court has not yet directly ruled on whether the Fourth Amendment protects

[78] "Better Business Bureau (BBB) Code of Business Practices (BBB Accreditation Standards)." (2009). Better Business Bureau. www.bbb.org/us/bbb-accreditation-standards.

[79] "Customers Choose to do Business with Companies They Trust." (2012). TRUSTe. www.truste.com/privacy_seals_and_services/enterprise_privacy/web_privacy_seal.

[80] Supreme Court of the United States. (1961). *Mapp v. Ohio*. 367 U.S. 643.

utilities records or energy usage data from government access.[81] Typically, however, the Fourth Amendment does not apply when government agents, like police officers, obtain information from third parties about a specific individual.[82] However, the U.S. Supreme Court has recognized that an individual's privacy in the home is "the very core" of the Fourth Amendment.[83] Depending on how detailed smart data may become or how much they may reveal about an individual, a court could reason that an individual's expectation of privacy in the home outweighs the benefit of providing government access to revealing data about one's daily activities. The Supreme Court's recent Fourth Amendment decision concerning GPS devices suggests heightened concern with the ability of new technologies to reveal personal information that was heretofore unavailable to law enforcement.[84]

Despite having no direct U.S. Supreme Court ruling on utility records, at least one Circuit Court of Appeals has applied the logic from cases involving information disclosed or recorded by third-party service providers. The Ninth Circuit—covering Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, and Oregon—has held that the police can obtain utility records without a warrant.[85] In summary, the question whether the government may access customer data that a utility compiles remains unresolved. Therefore, policymakers should take this into consideration when they formulate policies that may allow or restrict government access to customer information.

4.3 State Law Considerations

Some state constitutions afford greater protections for access to customer data than the U.S. Constitution or federal law. But even states that grant such protections have a mixed stance on whether an individual has a privacy right to data disclosed to a third party, willingly or not.[86] For example, the New Jersey Constitution grants greater rights than those under the Fourth Amendment or federal law.[87] New Jersey courts have held that internet subscribers have a reasonable expectation of privacy in any information an internet provider may give or sell.[88] That interest can be waived if a subscriber identifies himself by making a purchase, completing a survey, or by using a work computer in which the subscriber has no such expectation of privacy. This case is premised on the view that an Internet Protocol address does not reveal personal information.[89]

[81] For a more thorough discussion of how Fourth Amendment precedent may influence metering data, see Lerner, J.I.; Mulligan, D.K. (2008). "Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home." *Stanford Technology Law Review*. http://stlr.stanford.edu/2008/02/taking-the-long-view-on-the-fourth-amendment/.

[82] See, for example, Supreme Court of the United States. (1976). *United States v. Miller*. 425 U.S. 435.

[83] Supreme Court of the United States. (1961). *Silverman v. United States*. 365 U.S. 505.

[84] Supreme Court of the United States. (2012). *United States v. Jones*. 132 S.Ct. 945. The case is not directly applicable to smart meters because it concerns GPS tracking devices secretly placed on vehicles by police, in contrast to meters that are installed by utilities.

[85] U.S. Court of Appeals, Ninth Circuit. (1992). *United States v. Starkweather*. 972 F.2d 1347 at *2 ("We see no principled reason to accord electric utility records any different status under the Fourth Amendment than that accorded bank or telephone records."). The Supreme Court case on which the Ninth Circuit relied is United States v. Miller, 425 U.S. 435 (1972), which concerned bank records. The Court concluded that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Id*. at 443.

[86] See, for example, Missouri Supreme Court. (1997). *State v. Simmons*. 955 S.W.2d 752 (defendant relinquished any expectation of privacy in photographs or negatives by giving them to the developer); U.S. District Court, W.D. Virginia. (1999). *United States v. Hambrick*. 55 F. Supp. 2d 504, *aff'd*, U.S. Court of Appeals, Fourth Circuit. (2000). *United States v. Hambrick*. 225 F.3d 656, cert. denied by Supreme Court of the United States. (2001). *Hambrick v. United States*, 531 U.S. 1099 (no expectation of privacy in data given to Internet Service Provider; nothing prevented the provider from using or releasing the information even though the person giving the information used Internet under a pseudonym, that was linked to real information); *see* U.S. Court of Appeals, Ninth Circuit. (2006). *Freeman v. DirecTV, Inc.* 457 F.3d 1001 (ECPA provisions imposing civil liability on providers of electronic communication services that knowingly divulge the contents of communications being stored by that provider, did not create secondary liability for aiding and abetting or conspiracy to violate the ECPA; plain language of statute did not provide for secondary liability and unambiguously limited liability to an identified class of defendants; legislative history of the ECPA confirmed that Congress did not intend to allow secondary liability or any claims for aiding and abetting or conspiracy.).

[87] See, for example, Supreme Court of New Jersey. (2008). *State v. Reid*. 945 A.2d 26.

[88] *Id*.

[89] *Id*.

5. Privacy Practices in other Industries

While governing access to utility customer data is an emerging challenge, the telecommunications, health care, retail grocery, and retail electric supply industries have all addressed privacy concerns in the context of managing, utilizing, and providing access to customer information. The following sections discuss examples of some of the concerns raised through the course of their actions as well as the practical and legal constraints placed on their use of the data.

5.1 Telecommunications

The telecommunications sector has long been collecting and using highly granular data about customer usage; lessons from the telecommunications industry can be usefully applied to customer data used to provide energy efficiency services.

KEY OBSERVATION

The telecommunications example suggests that electricity regulators consider opt-in procedures, requiring explicit privacy policies and compliance disclosures by entities that gain access to customer data in the energy efficiency context.

Federal law protects certain customer-specific information (known as CPNI, or customer proprietary network information) from disclosure by federally regulated telephone companies without the consent of the consumer to whom the data apply. However, regulatory efforts to protect this data have not always been successful.

In the telecommunications realm, "pretexting" or "slamming" has occurred in which "data brokers" gained access to consumer telephone records by forging customer consent forms. In response, Congress passed the Telephone Records and Privacy Protection Act in 1996, which criminalized the making of false statements to telephone companies, providing fake documents to such companies, or accessing customer accounts via the internet without customer authorization. Various states—including Arizona, California, Connecticut, Florida, Maryland, Rhode Island, and Virginia—have prohibited "pretexting" as a matter of state law.

In 2007, the Federal Communications Commission (FCC) adopted privacy rules that require telephone carriers (including providers of voice-over-internet service) to:

> Obtain authorization from customers before sharing their CPNI with outside contractors or joint-venture partners, refuse to release call data over the phone unless the person requesting the information provides a password chosen by the customer, and file an annual report with the FCC that includes all consumer complaints about unauthorized CPNI disclosure and the actions taken on such complaints.

Telephone carriers may obtain authorization to release CPNI orally, in writing, or electronically. The FCC also requires telephone carriers to use an opt-in method to obtain such authorization.

5.2 Health Care

In 1996, Congress passed the Health Insurance Portability and Accountability Act, commonly referred to as HIPAA.[90] HIPAA contained "administrative simplification" provisions designed to streamline the electronic exchange of information for claims reimbursement.[91] Congress was concerned that sharing patient information

[90] U.S. Congress. (1996). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Pub. L. No. 104-191, §261–64, 110 Stat. 1936 (1996) (codified as amended at 42 U.S.C. § 300gg; 29 U.S.C § 1181 et seq.; 42 USC 1320d). For a comprehensive summary of HIPAA, see U.S. Department of Health and Human Services. (2003). *Summary of the HIPAA Privacy Rule*. www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

[91] 42 U.S.C. § 1320d. In addition to "administrative simplification," HIPAA also gives patients expanded rights to access their medical and billing records, request amendments to those records and obtain an accounting of disclosures of protected health information.

electronically would also increase the risk of unauthorized disclosures; thus, the legislation included a provision that required Congress to enact privacy legislation within three years or the Secretary of the Department of Health and Human Services (HHS) would be authorized to issue privacy regulations governing the electronic exchange, privacy, and security of health information. Congress did not enact privacy legislation, so HHS developed the HIPAA Privacy Rule in 2003 (herein referred to as The Privacy Rule).

The Privacy Rule prohibits the use or disclosure of any "individually identifiable" health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.[92] This includes common identifiers such as name, address, date of birth, and Social Security number, as well as treatment, physical condition, and payment information.[93] The rule applies to any use of this information by health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form in connection with claims-related transactions.[94]

KEY OBSERVATION

The HIPAA experience illustrates the desirability of a privacy regime that actively facilitates procedures for useful and appropriate data disclosure while simultaneously promulgating rigorous protections against disclosures that are not strictly necessary in light of the purpose for which the data were gathered and shared in the first instance.

The Privacy Rule permits four categories of uses and disclosures:

1. Patient information can be used or disclosed to: (1) treat the patient; (2) obtain payment for treating the patient; or (3) conduct health care operations if a patient has acknowledged receipt of a Notice of Privacy Practices (or good faith efforts have been made to obtain an acknowledgment).
2. Patient information can be given to caregivers, but only if the patient expressly or impliedly consents.
3. Certain disclosures can be made by a health care provider without patient authorization to accomplish public policy objectives (e.g., to report child or elder abuse).
4. Any other disclosure (e.g., for research, fundraising, or marketing) may be made only if the patient specifically authorizes the disclosure in writing.[95]

As a general rule, even if a use or disclosure is permitted under the Privacy Rule, no more than the "minimum necessary" amount of protected information may be used to accomplish a particular task.[96] However, there are no restrictions on the use or disclosure of de-identified health information[97] that neither identifies nor provides a reasonable basis to identify an individual. The Privacy Rule establishes two ways for entities to de-identify information. First, they may acquire a formal determination by a qualified statistician. Otherwise, they must remove specified identifiers of the individual and of the individual's relatives, household members, and employers.[98] Additionally, the entity must have no actual knowledge that the remaining information could be used to identify the individual.[99]

[92] See U.S. Congress. (2012). *Definitions*. Title 45 Code of Federal Regulations §160.103.

[93] *Id*.

[94] In addition to this federal standard, these covered entities must also comply with state laws that provide extra protection to patients, and includes civil and criminal penalties for non-compliance.

[95] This authorization must be a customized document that requests the patient's permission to use protected health information for specific purposes and for a specific time period.

[96] For example, while a physician may need to see all of a patient's health information for treatment purposes, a receptionist who simply checks patients in to the clinic should not need to see medical records.

[97] 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

[98] The Rule dictates the identifiers that must be removed, although individuals may be aggregated to the initial three digits of a zip code if doing so still includes more than 20,000 people). 45 C.F.R. § 164.514(b).

[99] 45 C.F.R. § 164.514(b).

5.3 Retail Grocery

The retail grocery industry has also utilized customer purchasing data very effectively to tailor marketing campaigns. Retail data mining can provide an analyst with geographic, demographic, seasonal, habitual, and gender correlations with purchasing decisions—valuable information for third parties (and the grocery store itself) seeking to maximize revenue and target marketing efforts.

The data are obtained when customers use their loyalty cards during a grocery store transaction. Customers initially register for the loyalty cards by providing information such as name, address, or telephone number. Thereafter, each transaction that is associated with that loyalty card is linked to that customer's demographic data.

KEY OBSERVATION

The retail grocery sector has relied upon voluntarily adopted industry standards and illustrates that, given appropriate disclosure policies, customers will understand the value they receive from disclosing their data in certain circumstances.

The loyalty cards are typically incentivized but voluntary. Essentially, the programs function as an opt-in data collection service. Most grocery chains have fairly extensive privacy policies that accompany their loyalty card programs, and in many cases, the policies prohibit the grocery store from selling individualized data to a third party. However, this is typically combined with an exception for aggregated data.[100] The voluntary nature of the programs and the fact that the stores only sell non-identifiable aggregated data has made grocery store loyalty cards quite successful since the 1980s.

5.4 Retail Electricity Supply

Approximately 20 states have opted to restructure their electric industries and allow customers to purchase electricity from retail energy services providers. In these states, electric utilities and their regulators have experience in dealing with issues related to third-party access to customer data in the context of retail electric supply.

Connecticut provides an example of an opt-out approach to dealing with the distribution utility providing customer information to potential competitive energy suppliers. Utilities must make available a form that customers can use to prevent specified basic customer data (e.g., name, address, telephone number, rate class) from being released to competitive suppliers.[101] Otherwise, the utility is required to make this contact information available to all electric suppliers.[102] With respect to all other customer information—including usage data—disclosure is prohibited without informed written or electronic consent or, alternatively, consent given by telephone but verified by an independent third party.[103]

In Pennsylvania, a utility must notify the customer of the company's intent to share the data with a third party. Additionally, it must provide a convenient method of notifying the entity of the customer's desire to restrict the release of the private information before providing customer information to a third party. Customers may restrict the information in three ways: by returning a signed form, orally, or electronically.[104]

[100] For example, Kroger's Privacy Policy states that: "We do not sell, trade, or rent our customers' personal information to outside companies or marketing firms." However, the policy also explains that "the company collects, stores, and uses aggregated data that do not contain personally identifiable information, such as demographic or statistical information. This aggregated data may be shared with and used by third parties to help us and our suppliers better serve and understand our customers." "The Kroger Co. Privacy Policy."(2012). The Kroger Co. www.kroger.com/company_information/Pages/privacy_policy.aspx.

[101] Conn. Gen. Stat. Ann. § 16-245o(a).

[102] *Id*.

[103] *Id*.

[104] 52 Pa. Code § 54.8.

5.5 Summary of Other Industries

The telecommunications, healthcare, and retail grocery industries have addressed the issue of access to customer data. The experience in the telecommunications industry demonstrates the value of customer data to a wide range of third parties and that regulators should be prepared to address attempts by disfavored third parties to access customer data. Imposing penalties, civil or criminal, on improperly obtaining customer data is one option to address this concern.

Additionally, the healthcare industry demonstrates the importance of customer consent. Medical data—more than electricity usage data—are perceived as private, personal information. However, as electricity usage data also provide insight into a customer's behavior, the importance of consent should not be overlooked.

The retail grocery industry provides an example of how an industry can achieve its goals while simultaneously maintaining consumer confidence. By rewarding participation in the program, while still making it voluntary, consumers retain the freedom of choice but predominantly choose to participate. Further, the existence and publication of a robust privacy policy is important.

In summary, the principles that stand out as being relevant are as follows:

- Penalties for improper access
- Customer consent
- Voluntary participation
- Incentivized participation
- Robust privacy policies.

6. Summary

State utility regulators can play a pivotal role in developing policies that both support energy efficiency and address privacy concerns regarding third-party access to customer data. Based upon this review of state experiences to date, regulators and policymakers are likely to address certain common issues: customer consent, data management, data access, enforcement, aggregated data, and cost recovery for utilities. Table 1 provides an overview of state approaches to date and lists the types of entities that may want access to utility customer data: (1) a non-utility energy efficiency program administrator that is under contract to a state public utilities commission (PUC) or the utility, (2) an entity that is under contract to a utility to provide energy efficiency services, (3) an unregulated third-party energy efficiency service provider (EESP), and (4) individual customers. Table 1 also summarizes state approaches to customer consent and options for addressing data management and security, as well as mitigating privacy concerns.

6.1 Customer Consent: Individuals

The fundamental issue regarding approaches to customer consent is how to resolve two competing policy imperatives: facilitating access to customer data for energy efficiency purposes while safeguarding customer privacy and providing consumer protections against unwanted uses of data. For states with a third-party energy efficiency program administrator, the general approach has been for the PUC or legislature to establish upfront the rules for sharing customer data (e.g., VT) or negotiate data access between utilities and the third-party program administrator (e.g., WI). Program implementation contractors (PICs) working under contract to a utility typically have been able to access customer data to fulfill their scope of services because they are assumed to be subject to same privacy standards as the utility itself through their contract. California follows this same track but requires customer consent if the PIC uses the data for a secondary purpose.

For unregulated EESPs that request access to customer data, several state PUCs have required customers to give affirmative consent (e.g., CO, TX, WA).

6.2 Customer Consent: Aggregated Data

Insight from other industries as well as historic experience of electric/gas utilities administering energy efficiency programs suggest that disclosing aggregated data poses limited risk to the customer. As a result, several states have adopted guidelines and rules that allow utilities or third-party program administrators to disclose aggregated data that can facilitate provision of energy efficiency services by the private sector (see Figure 1). Examples from states that have adopted policies on provision of aggregated data include the following:

- 15/15 Rule (e.g., CO)[105]
- Town-level (e.g., VT)
- 20,000 people (e.g., HIPAA)
- At an unspecified level that ensures customer-specific information cannot be determined (e.g., CA).[106]

Aggregated information that may be valuable and useful to EESPs includes aggregated data on customer energy usage patterns, market assessments of efficiency opportunities in selected market segments or geographic regions, process and impact evaluations, and market potential studies. Aggregated data are also useful for building benchmarking and whole building efficiency programs when each tenant is individually metered and the building owner does not have access to each meter in the building. If regulators decide to allow the provision of aggregated data, they will likely need to establish policies that determine when data are sufficiently aggregated.

[105] 4 Colo. Code Regs. 723-3 Part 3 §3031(b)(c); Okla. Stat. tit.17 §710.7(B)(2); Vermont Public Service Board. (2010). *Investigation into Petition Filed by Vermont Department of Public Service Re: Energy Efficiency Utility Structure.* Docket No. 7466.

[106] CPUC D.11-07-056, Attachment D at Sec. 6(g).

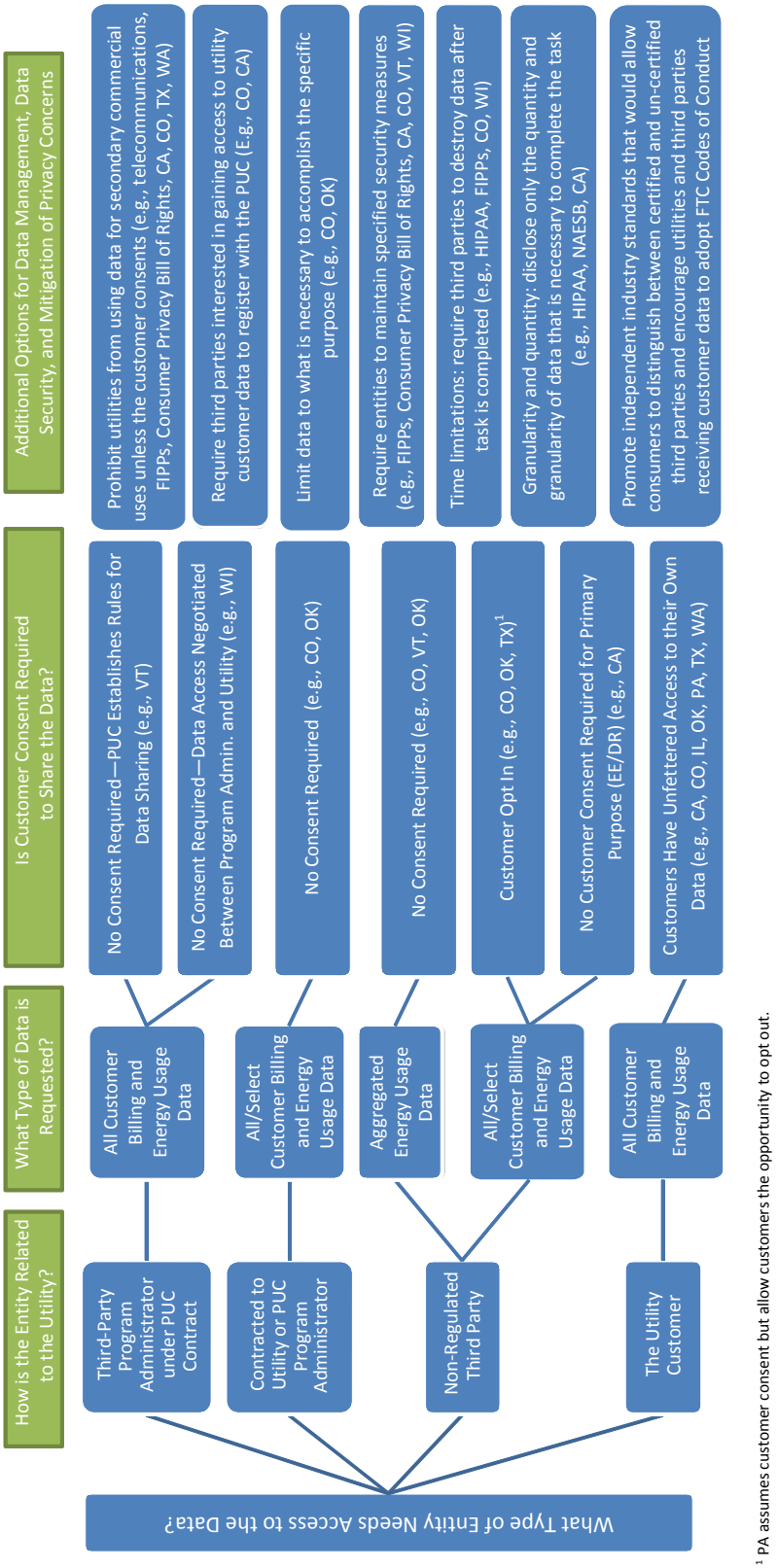


Figure 1. Overview of state approaches on accessing customer utility data

6.3 Access by Customers to Their Utility Data

The general consensus among states that have established policies on customer data appears to be that customers should have access to their own data (e.g., Consumer Privacy Bill of Rights; state law in California, Colorado, Illinois, Oklahoma, Pennsylvania, Texas, and Washington).[107]

6.4 Data Management, Data Security, and Privacy

The consensus view that has emerged among most states thus far is that safeguarding customer privacy does not end with regulating the extent to which a customer controls data disclosures. Rather, policymakers may wish to consider additional limitations on the disclosures themselves and on the use of the data post-disclosure. Four states prohibit utilities from using customer data for secondary commercial uses unless the customer consents to other uses.[108] This is also a component in telecommunications, Fair Information Practice Principles (FIPPs), and Consumer Privacy Bill of Rights documents. [109] In addition, four states, FIPPs, and the Consumer Privacy Bill of Rights also require third parties to maintain specified security measures. Options for data management, data security, and privacy mitigation are highlighted in Figure 1. Below are examples of other policies that have been put in place from other industries and selected states:

- **Time limitations:** require third parties to destroy data after the intended purpose is accomplished (e.g., HIPAA, FIPPs, CO, WI)[110]
- **Granularity and quantity:** disclose only the quantity and granularity of data necessary to complete the task (e.g., HIPAA, NAESB, CA)
- **Security verification:** require a third party's security measures to be certified by an independent entity (e.g., NAESB, Privacy Seal).

Utility regulators can encourage and promote certain practices that increase the chances that problems will not arise if/when third parties obtain access to customer information**.** These practices include the following:

- Promoting independent industry standards that would allow consumers to distinguish between certified and un-certified third parties
- Encouraging utilities and third parties receiving customer data to adopt Codes of Conduct; companies that breach the Codes of Conduct can be subject to Federal Trade Commission (FTC) enforcement.[111]

6.5 Enforcement Mechanisms and Business Practices

Given the significance of privacy concerns, civil and criminal penalties may effectively deter breaches of state privacy law. Penalties could be stricter for intentional, illegal data disclosures as opposed to accidental disclosures or disclosures of aggregated data. Sanctions for violations could be defined by state PUCs or state legislatures. State PUCs can enforce rules or impose sanctions for violations. Sources that reflect this principle include FIPPs, the telecommunications industry, and the Consumer Privacy Bill of Rights, as well as state policy related to third-party access to customer data in California, Colorado, Vermont, and Wisconsin.[112]

[107] 4 Colo. Code Regs. 723-3 Part 3 §3026(d); Okla. Stat. tit. 17 §710.4; Cal. Pub. Util. Code §8380(a)(4); Ill. Admin. Code. tit. 83 §410.210; 66 Pa. Cons. Stat. § 2807; 2 Tex. Util. Code §39.107; Wash. Admin. Code §480-100-153.

[108] Wash. Admin. Code §480-100-153; 4 Colo. Code Regs. 723-3 Part 3 §3028; Cal. Pub. Util. Code §8380; 2 Tex. Util. Code §39.107(b).

[109] Cal. Pub. Util. Code §8380; 4 Colo. Code Regs. §3029; Vermont Public Service Board. (2010). Docket No. 7466.

[110] 4 Colo. Code Regs. 723-3 Part 3 §3029(a)(III); Wisconsin Public Service Commission. (2009). Docket No. 9501-GF-101.

[111] Federal Trade Commission. (March 2012). *Protecting Consumer Privacy in an Era of Rapid Change*. http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[112] Cal. Pub. Util. Code §8380(f); 4 Colo. Code Regs. 723-3 Part 3 §3976; Wisconsin Public Service Commission. (2009). Docket No. 9501-GF-101; Vermont Public Service Board. (2010). Docket No. 7466.

To increase accountability for entities that possess customer information, the following may be useful practices for a state to consider:

- Require that each utility and contractor be covered by a privacy policy, obtain regulatory approval of the policy, follow the policy, and make the policy available to customers
- Require utilities to submit annual reports that include their written privacy policies, compliance statistics, and information about each complaint received, including its resolution
- Conduct periodic "privacy audits" for utilities and third parties to assure the public that these entities are faithfully maintaining the privacy of customer data and using it only for authorized purposes
- Initiate efforts to educate customers about the responsible use of their data.[113]

6.6 Cost Recovery

Utilities are often reluctant to undertake major initiatives involving disclosure of customer data to third parties because of uncertainties regarding recovery of costs. State regulatory agencies may consider setting guidelines or addressing potential cost recovery issues. As part of their provision of basic customer services, utilities will typically recover costs to provide periodic billing and metering information. Some states have established policies that allow utilities to recover costs incurred in connection with the acquisition, maintenance, and provision of customer smart meter data beyond what is provided as part of routine billing processes, such as access to near real-time data (e.g., CO, OK).[114]

Based on existing state policies, there is no consensus on whether utilities should charge third parties for fees to acquire customer data. Oklahoma allows utilities to recover costs by charging third parties a reasonable fee to acquire customer data while Colorado does not allow utilities to charge third parties to access customer data. Charging individual third parties for data access may pose an additional burden that hinders innovation. If PUCs encourage utilities to provide various types of aggregated data which involve additional costs, PUCs may wish to be more proactive in establishing guidelines on cost recovery for these types of services. There are five broad options that can address this issue:

- Allow the utility to include these costs in general operating expenses
- Allow utilities to recover the costs through customer charges
- Allow utilities to charge third parties for access to the data
- Prohibit utilities from recovering any additional costs for providing data to third parties
- Recover costs as part of other related utility projects, such as energy efficiency program portfolios, billing system upgrades, or smart grid deployments.

6.7 Conclusion

Customer data has the potential to be the fuel for innovation which unlocks vast unrealized opportunities for greater energy efficiency. As innovators experiment with new uses of data to help meet energy efficiency goals, stakeholders must be mindful of customer expectations regarding privacy. There is a delicate balance between the two; but, as demonstrated, states have navigated this balance with success.

[113] Pennsylvania law requires companies to institute education programs for customers.

[114] Okla. Stat. tit.17 §710.5; 4 Colo. Code Regs. 723-3 Part 3 §3026(e). Note that Colorado's policy states that a utility may not charge for providing standard format data while Oklahoma's policy allows companies to recover costs for providing higher granularity data than the customer's bill (e.g., near-real time data). It may be desirable to include these costs in general operating expenses, as opposed to requiring utilities to recover them via individual customer charges and/or charges to contractors.

References

Barbose, G.; Billingsley; M.; Goldman, C.; Hoffman, I.; Schlegel, J. (August 2012). "On a Rising Tide: The Future of U.S. Utility Customer-Funded Energy Efficiency Programs." *2012 ACEEE Summer Study Proceedings*; August 12-17, 2012, Pacific Grove, California. Washington, D.C.: American Council for an Energy-Efficient Economy (ACEEE). LBNL-5755E. www.aceee.org/files/proceedings/2012/data/papers/0193-000173.pdf.

"Better Business Bureau (BBB) Code of Business Practices (BBB Accreditation Standards)." (2009). Better Business Bureau. www.bbb.org/us/bbb-accreditation-standards.

California Legislature. (2012). *Telecommunications: master-metering: data security*. SB 674. California Public Utilities Code §8380. http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201120120SB674.

"California Measurement Advisory Council." (2012). www.calmac.org.

California Public Utilities Commission. (2012). *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*. Decision 11-07-056. http://docs.cpuc.ca.gov/PublishedDocs/WORD_PDF/FINAL_DECISION/140369.PDF.

_____. (2012). *Decision Extending Privacy Protections to Customers of Gas Corporations and Community Choice Aggregators, and to Residential and Small Commercial Customers of Electric Service Providers*. Decision 12-08-045. http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M026/K531/26531585.PDF.

Cate, F.H. (2006). *The Failure of Fair Information Practice Principles: Consumer Protection in the Age of the Information Economy*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972.

Chopra, A. (2012). "Green Button: Providing Consumers with Access to Their Energy Data." *Office of Science and Technology* blog. www.whitehouse.gov/blog/2012/01/18/green-button-providing-consumers-access-their-energy-data.

Colorado Legislature. (2012). *Contracted Agent Access to Customer Data from a Utility*. Title 700 Subtitle 723-3 Regulation §3029. www.dora.state.co.us/puc/rules/723-3.pdf, page 28.

_____. (2012b). *Customer Consent Form for the Disclosure of Customer Data to Third-Party Recipients by a Utility*. Title 700 Subtitle 723-3 Regulation §3028. www.dora.state.co.us/puc/rules/723-3.pdf, page 26.

_____. (2012c). *Disclosure of Customer Data by a Utility*. Title 700 Subtitle 723-3 Regulation §3026. www.dora.state.co.us/puc/rules/723-3.pdf, page 24.

_____. (2012d). *Regulated Electric Utility Rule Violations, Civil Enforcement, and Civil Penalties*. Title 700 Subtitle 723-3 Regulation §3976. www.dora.state.co.us/puc/rules/723-3.pdf, page 203.

_____. (2012e). *Requests for Aggregated Data Reports from a Utility*. Title 700 Subtitle 723-3 Regulation §3031. www.dora.state.co.us/puc/rules/723-3.pdf, page 29.

_____. (2012f). *Scope and Applicability*. Title 700 Subtitle 723-3 Regulation §3000. www.dora.state.co.us/puc/rules/723-3.pdf, page 9.

Colorado Public Utilities Commission. (2011). *In the Matter of the Proposed Rules Relating to Smart Grid Data Privacy for Electric Utilities*. Docket No. 10R-799E.

Connecticut Legislature. (2012). *Restrictions on Use of Customer Information for Marketing. Promotional Inserts in Electric Bills Prohibited. Procedures for Entering and Terminating Service Contracts. Penalties*. Title 16 Code §245o. www.cga.ct.gov/2012/sup/chap283.htm#Sec16-245o.htm.

"Customers Choose to do Business with Companies They Trust." (2012). TRUSTe. www.truste.com/privacy_seals_and_services/enterprise_privacy/web_privacy_seal.

District of Columbia Legislature. (2012). *Public Utilities, Electricity, Consumer Protections*. Title 34 Code §34-1507. http://government.westlaw.com/linkedslice/default.asp?SP=DCC-1000.

Edison Foundation. (2012). *Utility-Scale Smart Meter Deployments, Plans, & Proposals*. www.edisonfoundation.net/iee/Documents/IEE_SmartMeterRollouts_0512.pdf.

"Energy Efficiency Resource Standards (EERS)." (2012). American Council for an Energy-Efficient Economy (ACEEE). www.aceee.org/topics/eers.

Federal Trade Commission. (1998). *Privacy Online: A Report to Congress*. www.ftc.gov/reports/privacy3/toc.shtm.

Federal Trade Commission. (March 2012). *Protecting Consumer Privacy in an Era of Rapid Change*. http://ftc.gov/os/2012/03/120326privacyreport.pdf.

Fehrenbacher, K. (2009). "Google Jumps Into Organizing Smart Meter Energy Data." *Gigaom*. http://gigaom.com/cleantech/google-jumps-into-organizing-smart-meter-energy-data/.

Focus on Energy. (2012). *Evaluation Reports*. www.focusonenergy.com/evaluation-reports/default.aspx.

"Frequently Asked Questions." (2012). Smart Meter Texas. https://www.smartmetertexas.com/CAP/public/home/home_faq.html.

"Green Button Data Demonstration." (2012). www.greenbuttondata.org.

Illinois Legislature. (2012). *Public Utilities, Electric Utilities, Information to Customers*. Title 83 Code §410.210. www.ilga.gov/commission/jcar/admincode/083/083004100C02100R.html.

"The Kroger Co. Privacy Policy."(2012). The Kroger Co. www.kroger.com/company_information/Pages/privacy_policy.aspx.

Kushler, M.; Nowak, S.; Witte, P. (February 2012). *A National Survey of State Policies and Practices for the Evaluation of Ratepayer-Funded Energy Efficiency Programs.* American Council for an Energy-Efficient Economy (ACEEE). Report Number U122. www.aceee.org/research-report/u122.

Lerner, J.I.; Mulligan, D.K. (2008). "Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home." *Stanford Technology Law Review*. http://stlr.stanford.edu/2008/02/taking-the-long-view-on-the-fourth-amendment/.

Missouri Supreme Court. (1997). *State v. Simmons*. 955 S.W.2d 752. http://scholar.google.com/scholar_case?case=11244113451652898258&q=State+v.+Simmons,+955+S.W.2d+752&hl=en&as_sdt=2,46&as_vis=1.

National Telecommunications and Information Administration. (2012). *Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct*. Publication Title 77 F.R. 13098. www.gpo.gov/fdsys/granule/FR-2012-03-05/2012-5220/content-detail.html.

New York State Energy Research and Development Authority (NYSERDA). (2012). *New York Energy $mart Evaluation Contractor Reports*. www.nyserda.ny.gov/en/Program-Evaluation/NYE$-Evaluation-Contractor-Reports/2012-Reports.aspx.

North American Energy Standards Board (NAESB). (2010). *Req. 21—Energy Service Provider Interface* (short article). www.naesb.org/ESPI_Standards.asp.

North American Energy Standards Board (NAESB). (2011). *Req. 21—Energy Service Provider Interface* (draft recommendation). www.naesb.org/pdf4/espi_task_force_052411w1.docx.

Northwest Energy Efficiency Alliance. (2012). *Market Research and Evaluation Reports*. http://neea.org/resource-center/market-research-and-evaluation-reports.

Ohio Legislature. (2012). *Customer Safeguards and Information*. Ohio Administrative Code §4901:1-10-24. http://codes.ohio.gov/oac/4901%3A1-10-24.

Oklahoma Legislature. (2011). *Aggregate Customer Usage Information*. Title 17 Code §710.7. www.oklegislature.gov/osstatuestitle.html (click on Title 17).

_____. (2011b). *Customer Information–Affiliates*. Title 17 Code §710.6. www.oklegislature.gov/osstatuestitle.html (click on Title 17).

_____. (2011c). *Electric Utilities–Usage Data*. Title 17 Code §710.5. www.oklegislature.gov/osstatuestitle.html (click on Title 17).

_____. (2011d). *Electric Utilities–Customer Information*. Title 17 Code §710.4. www.oklegislature.gov/osstatuestitle.html (click on Title 17).

Pennsylvania Legislature. (2007). *Duties of Electric Distribution Companies*. Title 66 Code §2807. www.legis.state.pa.us/WU01/LI/LI/US/PDF/2007/0/0036.PDF.

Pennsylvania Legislature. (1998). *Privacy of Consumer Information*. Title 52 Code §54.8. www.pacode.com/secure/data/052/chapter54/chap54toc.html#54.8.

Public Utility Commission of Texas. (2007). *Order Adopting New §25.130 and Amendments to §§25.121, 25.123, 25.311, and 25.346 as Approved at the May 10, 2007 Open Meeting*. Project No. 31418. http://puc.texas.gov/agency/rulesnlaws/subrules/electric/25.121/31418adt.pdf.

Schira, A. (2011). "Protecting Progress and Privacy: The Challengers of Smart Grid Implementation." *A Journal of Law and Policy for the Information Society*. https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=6+ISJLP+629&srctype=smi&srcid=3B15&key=cab8ad65498d1644d19b174e2a8a7086.

Smart Grid Interoperability Panel Cyber Security Working Group. (2010). *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*. National Institute for Standards and Technology (NIST). www.nist.gov/smartgrid/upload/nistir-7628_total.pdf.

"Smart Meter Texas." www.smartmetertexas.com/CAP/public/.

"SmartMeter™ Network—How It Works." (2012). Pacific Gas and Electric Company (PG&E). www.pge.com/myhome/customerservice/smartmeter/howitworks/.

Supreme Court of New Jersey. (2008). *State v. Reid*. 945 A.2d 26. http://www.leagle.com/xmlResult.aspx?xmldoc=2008971945A2d26_1971.xml.

Supreme Court of the United States. (1961). *Mapp v. Ohio*. 367 U.S. 643. http://supreme.justia.com/cases/federal/us/367/643/case.html.

Supreme Court of the United States. (1961). *Silverman v. United States*. 365 U.S. 505. http://supreme.justia.com/cases/federal/us/365/505/case.html.

Supreme Court of the United States. (1976). *United States v. Miller*. 425 U.S. 435. http://supreme.justia.com/cases/federal/us/425/435/case.html.

Supreme Court of the United States. (2001). *Hambrick v. United States*, 531 U.S. 1099.

Supreme Court of the United States. (2011). *Sorrell v. IMS Health, Inc.* 131 S. Ct. 2653. www.supremecourt.gov/opinions/10pdf/10-779.pdf.

Supreme Court of the United States. (2012). *United States v. Jones*. 132 S.Ct. 945. www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

Texas Legislature. (2009). *Metering and Billing Services*. Utilities Code Title 2 Chapter 39 Code §39.107. www.lawserver.com/law/state/texas/tx-codes/texas_utilities_code_39-107.

U.S. Congress. (1996). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Pub. L. No. 104-191, §261–64, 110 Stat. 1936 (1996) (codified as amended at 42 U.S.C. § 300gg; 29 U.S.C § 1181 et seq.; 42 USC 1320d). Original text at http://attorneygeneral.utah.gov/cmsdocuments/HealthInsurancePortabilityandAccountabilityAct1996.pdf.

U.S. Congress. (2006). *Unfair Methods of Competition Unlawful; Prevention by Commission*. Title 15 United States Code §45. www.gpo.gov/fdsys/pkg/USCODE-2011-title15/pdf/USCODE-2011-title15-chap2-subchapI-sec45.pdf.

U.S. Congress. (2010). *Definitions*. Title 42 United States Code Annotated §1320d. www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap7-subchapXI-partC-sec1320d.pdf.

U.S. Congress. (2012). *Definitions*. Title 45 Code of Federal Regulations §160.103. www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec160-103.pdf.

_____. (2012b). *Other Requirements Relating to Uses and Disclosures of Protected Health Information*. Title 45 Code of Federal Regulations §164.514. www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-514.pdf.

_____. (2012c). *Uses and Disclosures of Protected Health Information: General Rules*. Title 45 Code of Federal Regulations §164.502. www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-502.pdf.

U.S. Court of Appeals, Fourth Circuit. (2000). *United States v. Hambrick*. 225 F.3d 656.

U.S. Court of Appeals, Ninth Circuit. (1992). *United States v. Starkweather*. 972 F.2d 1347. http://ftp.resource.org/courts.gov/c/F2/972/972.F2d.1347.91-30354.html.

U.S. Court of Appeals, Ninth Circuit. (2006). *Freeman v. DirecTV, Inc.* 457 F.3d 1001. http://classactiondefense.jmbm.com/freemanclassactiondefense_opn.pdf.

U.S. Department of Commerce. (2010). *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*. The Internet Policy Task Force. www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.

U.S. Department of Energy (DOE). (2010). *Data Access and Privacy Issues Related to Smart Grid Technologies*. http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf.

U.S. Department of Health and Human Services. (2003). *Summary of the HIPAA Privacy Rule*. www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

U.S. Department of Homeland Security. (2008). *Privacy Policy Guidance Memorandum*. www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

U.S. District Court, W.D. Virginia. (1999). *United States v. Hambrick*. 55 F. Supp. 2d 504. http://scholar.google.com/scholar_case?case=10987987507072980066&q=U.S.+v.+Hambrick,+55+F.+Supp.+2d&hl=en&as_sdt=2,46&as_vis=1.

Vermont Public Service Board. (2000). Investigation into Dispute Regarding the Provision of Customer Information to Efficiency Vermont by the Village of Hyde Park Electric Department, et al. Docket Number 6379. www.state.vt.us/psb/orders/document/6379fnl.pdf.

Vermont Public Service Board. (2010). *Investigation into Petition Filed by Vermont Department of Public Service Re: Energy Efficiency Utility Structure.* Docket Number 7466. http://psb.vermont.gov/sites/psb/files/docket/7466EEUStructure/7466_PFD_Order_of_Appt.pdf.

Vermont Public Service Board. (2011). *Investigation into Vermont Electric Utilities' Use of Smart Meter and Time-Based Rates*. Docket No. 7307. http://psb.vermont.gov/sites/psb/files/orders/2011/2011-2/7307%20OrderReIntervention.pdf.

Vermont Public Service Board. (2012). *Joint Petition of Central Vermont Public Service Corporation, Green Mountain Power Corporation, et al.* Docket No. 7770. http://psb.vermont.gov/sites/psb/files/orders/2012/2012-4/Reply%20Brief%20of%20VPPSA%20050412.pdf.

Wagnon, W. (2012). "Green Button Has a New Site to Connect." *Jetson Green*. www.jetsongreen.com/2012/02/green-button-connect-energy-efficiency-app-gallery.html.

Washington State Legislature. (2001). *Disclosure of Private Information*. Title 480 Code §480-100-153. http://apps.leg.wa.gov/wac/default.aspx?cite=480-100-153.

White House. (2012). *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Wickenden, M. (2011). *Letter to Susan Hudson, Clerk at the Vermont Public Service Board*. http://psb.vermont.gov/sites/psb/files/orders/2011/2011-2/VEIC%20Combined.pdf.

Wisconsin Public Service Commission. (2009). *Provision of Energy Utility Customer Information to Focus on Energy*. Docket No. 9501-GF-101. http://psc.wi.gov/apps35/ERF_view/viewdoc.aspx?docid=115210.

Appendix A: Case Studies

California

On September 29, 2010, Senate Bill 1476 was signed into law in California. The bill addresses privacy issues related to customer data generated by advanced meters and adds two important provisions, Sections 8380 and 8381, to California's Public Utility Code. The statute requires electric and natural gas companies to employ reasonable security practices to protect customer information, prohibits them from allowing unauthorized access to customer data or from destroying or modifying the customer's data, and prohibits an electric or natural gas company from selling customer consumption data or any other personally identifiable information for any purpose.

Applying these specific statutory mandates, the California Public Utilities Commission (CPUC) issued a detailed order on July 29, 2011 to further clarify California's policy for third-party access to data. The rules—consistent with Senate Bill 1476 and the U.S. Department of Homeland Security's Fair Information Practice Principles (FIPPs)—apply to the state's three major electric utilities (Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas and Electric Company). A supplemental CPUC decision extends these protections to cover natural gas data generated by advanced meters from the three major natural gas utilities (Pacific Gas and Electric Company, San Diego Gas and Electric Company, and Southern California Gas Company), as well as to Community Choice Aggregators and small commercial and residential customers of electric service providers.[115]

The CPUC order distinguishes between data used for a "primary purpose" and data used for a "secondary purpose" when determining whether a utility may disclose individual consumers' electricity usage data to a program implementation contractor (PIC). Primary purpose data include data used for utility energy efficiency and demand response programs, as well as utility energy management. All other uses are defined as a secondary purpose under the rule. An electric utility may disclose information that could indicate the identity of a customer to a PIC for a primary purpose without customer consent. To disclose customer data to a PIC for a secondary purpose, the utility must have the customer's consent. However, even if customer consent is not required, the PIC must meet certain basic privacy and security requirements in order to obtain customer usage information.

California's regulation of access to customer data based on the intended use is a unique way to apply the FIPPs principle of forming data protections based on the purpose the data are used for.

Colorado

Colorado has completed a rulemaking docket that addresses issues of customer data privacy. Utilities, third-party energy efficiency services providers (EESPs), municipalities, and telecommunications service providers, among others, provided comments. Rules were drafted and redrafted over the course of approximately two years to come to a compromise among various stakeholders.[116]

In Colorado, a utility must provide customer data to a third party if the customer has authorized disclosure. The disclosure must be in standard-formatted, electronic machine-readable form. Access must be provided without additional charges to the customer or third party if the disclosure is in standard format. However, if the third party or customer requests high-granularity data, such as real-time data, the utility may be able to charge a reasonable fee to cover costs for providing the data. Nothing can prevent a customer from disclosing his or her own data. However, if the customer discloses information to a third party that does not contract with the utility, the third party is not subject to these privacy regulations. Additionally, a utility may disclose customer data to a contracted agent provided that the contracted agent: (1) maintains reasonable data security procedures that are greater than

[115] California Public Utilities Commission. (2012). *Decision Extending Privacy Protections to Customers of Gas Corporations and Community Choice Aggregators, and to Residential and Small Commercial Customers of Electric Service Providers*. Decision 12-08-045.

[116] Colorado Public Utilities Commission. (2012). *In the Matter of the Proposed Rules Relating to Smart Grid Data Privacy for Electric Utilities*. Docket No. 10R-799E.

or equal to the data privacy and security policies that the utility uses internally to protect customer data; (2) uses customer data solely for the purposes of the contract; (3) destroys any customer data that are no longer necessary; and (4) executes a non-disclosure agreement with the utility. Otherwise, a utility may not disclose customer data to any third party unless the customer (or third party acting for the customer) submits paper- or electronic-signed consent to disclose customer data.

Utilities must provide notice to customers annually. This notice will do the following:

- Inform customers that third parties can use customer data to obtain insight into their activities
- Include a description of customer data
- Include an explanation of how this information is collected
- Inform customers that a utility will protect a customer's data
- Explain that the customer can request his or her own data without charge
- Explain that customer's may have an expectation of privacy
- Explain that the utility may aggregate the customer's data and provide that aggregated data to third parties.

A utility may disclose aggregated data, thought it must take steps to ensure that an individual customer's data cannot be identified. A particular aggregation must contain at least 15 customers or premises and, within any customer class, no single customer's data or customer premise may comprise more than 15 percent of the total aggregated data. This is otherwise known as the "15/15 Rule." However, despite this rule, the utility does not have to disclose the individual customer's information if that information would compromise the individual's privacy. A utility—including its directors, officers, and employees—who discloses aggregated data may not be held liable for any claims of harm or loss related to the disclosure of aggregated data.

The intentional violation of any of the privacy rules may result in a penalty that the commission will assess. A list of the possible violations and their corresponding penalty amounts are provided in a table in the rule itself.[117]

Texas

On May 30, 2007, the Public Utility Commission of Texas adopted Substantive Rule 25.130, which established state privacy standards for access to advanced meter data. The rule implemented Texas House Bill 2129, relating to advanced metering.[118] The rule requires an electric utility to provide a customer's advanced meter data to the customer, the customer's retail electric provider, and other customer-authorized entities that have read-only access. This includes data that the utility uses to calculate charges, historical load data, and any other customer information. Utilities must provide access to the data in a way that is convenient and secure and the utility must make the data available no later than the day after it was created.[119] Additionally, Texas data privacy law is unique in that it specifies that all meter data belong to the customer.[120] This designation is important because it establishes, as a basic principle of state law, that the customer is the entity that controls his or her data.

To allow individuals to conveniently access and monitor their electricity usage, Texas implemented Smart Meter Texas.[121] Smart Meter Texas is a website sponsored by a coalition of transmission and distribution service providers. It is a shared web portal that allows customers to access their consumer-specific energy usage data

[117] 4 Colo. Code Regs. 723-3 Part 3 §3000 et seq.

[118] Public Utility Commission of Texas. (2007). Order Adopting New §25.130 and Amendments to §§25.121, 25.123, 25.311, and 25.346 as Approved at the May 10, 2007 Open Meeting. Project No. 31418.

[119] Public Utility Commission of Texas Substantive Rule: 25.130(j)(1).

[120] 2 Tex. Util. Code §39.107

[121] "Smart Meter Texas." www.smartmetertexas.com/CAP/public/.

(CEUD). The Smart Meter Texas interface allows customers to see their data in 15-minute intervals and provides graphs and tables for customers to easily see when they have spikes in electricity usage. Any customer can register for Smart Meter Texas access via the website.

To ensure customer privacy, Smart Meter Texas limits the entities that may access customers' data. Only a retail electric provider, Smart Meter Texas website administrators, and those that customers authorize to access their account may access customer data. Customers with a residential account may grant up to five "friends" access to their usage information. The Smart Grid Texas terms and conditions allow only Smart Grid Texas to share customer information with its own employees and corporate service affiliates; the customer or customer's agent; any vendor, contractor, consultant, licensor, or supplier that agrees to keep the information confidential; any person the customer has authorized to have access to the data; and any entity authorized by law to have the data.[122] Smart Meter Texas ensures that it will not sell a customer's information to any third party for any reason. Additionally, no customer can hold Smart Meter Texas liable for any harm that results from the use of information on the website, unless Smart Meter Texas caused the harm through gross negligence or intentional misconduct.

Vermont

Vermont's Public Service Board weighed the energy efficiency value of utility data against customer privacy concerns in the early 2000s. At that point, the board considered whether an electric utility was obligated to share customer usage data with Vermont's Energy Efficiency Utility (EEU). Vermont's structure is somewhat unique in that it is one of the few states that have EEUs (Efficiency Vermont and Burlington Electric Department). The EEUs were under contract with the state (and are now under designated franchises) to provide electric utility customers with energy efficiency services.

The board recognized that energy efficiency was one of the state's priorities. The board also found that the lack of customer information had a negative repercussion on the EEU's ability to utilize cost-effective energy efficiency resources. Specifically, the board stated that "without customer information, Vermont Energy Investment Corporation (VEIC), the state's third-party program administrator, will be unable to provide the same level of customer service to all customers who have paid for that service through the energy efficiency charge."[123] Notably, the EEUs are under contract with the board and are obligated to follow specified confidentiality procedures. Ultimately, the board concluded that the privacy concerns were sufficiently addressed and that the electric utilities would be required to disclose their customer information to the EEU.

More than 10 years later, Vermont is preparing for broad implementation of smart meters. Currently, the state has a policy in place for utility data, but has no official legislation specifically related to smart meter data. However, the board has an open docket regarding the issue of smart meter data security.[124]

Presently, utilities may only release usage data to the following:

- Public Service Board (PSB)
- Department of Public Service (DPS)
- Vermont utilities
- Members of the Vermont General Assembly (or legislative staff)
- Independent firms under contract with the PSB or DPS.

[122] The Smart Grid Texas Terms and Conditions are available at: "Frequently Asked Questions." (2012). Smart Meter Texas. https://www.smartmetertexas.com/CAP/public/home/home_faq.html.

[123] Vermont Public Service Board. (2000). *Investigation into Dispute Regarding the Provision of Customer Information to Efficiency Vermont by the Village of Hyde Park Electric Department, et al.* Docket No. 6379.

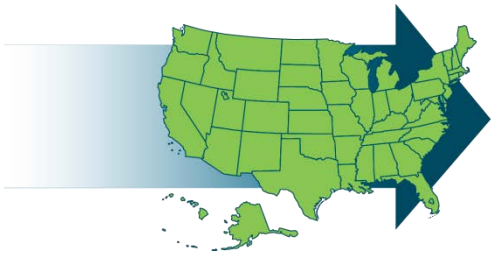
[124] Vermont Public Service Board. (2011). *Investigation into Vermont Electric Utilities' Use of Smart Meter and Time-Based Rates*. Docket No. 7307.

Because the EEUs provide almost all of the energy efficiency services to Vermont citizens, the above-listed restrictions on data release do not significantly impede the energy efficiency value of smart meter data. In states without energy efficiency utilities, these limitations might prove more restrictive.

Vermont distinguishes between third parties and utilities in its data access requirements; however, Vermont's EEUs do not anticipate any significant change in their access to customer data.[125] EEUs are subject to the Confidential Information Management System, which significantly restricts their handling of the data.

Under the existing system and the smart-meter proposed system, independent firms may access data that are aggregated to the town level.

[125] Wickenden, M. (2011). *Letter to Susan Hudson, Clerk at the Vermont Public Service Board*. http://psb.vermont.gov/sites/psb/files/orders/2011/2011-2/VEIC%20Combined.pdf.



SEE Action

STATE & LOCAL ENERGY EFFICIENCY ACTION NETWORK