BALANCING SMART GRID DATA AND CONSUMER PRIVACY

By Constance Douris

June 2017

Lexington Institute

FUTURE OF THE POWER GRID SERIES

BALANCING SMART GRID DATA AND CONSUMER PRIVACY

By Constance Douris
June 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Technologies on the electric grid allow for two-way communication and the transfer of data between utilities and customers. Information from the grid enables customers to decrease electricity costs and boosts the reliability of the grid infrastructure. Such information also equips third-party providers with data to create new energy-saving products and services. When electricity infrastructure is damaged as a result of a physical attack or natural disaster, data allows for quicker response times, boosting the overall security of the grid.

The two types of data collected by smart grid technologies are personally identifiable information and consumer-specific energy usage data. Personally identifiable information includes an individual's name, address and telephone number. An example of consumer-specific energy usage data is the total electricity used at various times in a day. This kind of information, fused with unique load signatures generated by electrical appliances, could be used for legal and illegal real-time surveillance.

Methods to remove personal information from electricity usage data already exist. Solutions include aggregation, encryption and steganography. However, anonymizing data requires computational time and effort. There are also additional costs to store, process and transfer large amounts of information. How these extra expenses will be paid for must be determined.

— continued

Utilities are hesitant to share usage data even though it provides many benefits to customers, businesses and operators of the electric grid. This reluctance is due to the costs required to process and transfer such data. In addition, utilities may be at legal risk if information is improperly disclosed or if a customer's privacy is violated. Due to these obstacles, electricity data is underutilized.

Consumer usage data is so valuable that some predict it eventually may be worth more than the distribution of electricity.[1] Even so, over half of states in the U.S. lack policy for electricity data access. Without guidelines, customers, businesses and grid operators lack the information they need to make better decisions on the grid. In addition, personal information potentially may be shared in a manner not desired by customers.

The grid must encourage innovation and make electricity usage available to customers and businesses all while respecting consumers' personal privacy and security. States that have implemented such policies include California, Texas, Illinois and Vermont. These actions will be analyzed and compared to inform other states of elements they could incorporate into future policies to allow customers, businesses and grid operators access to critical data.

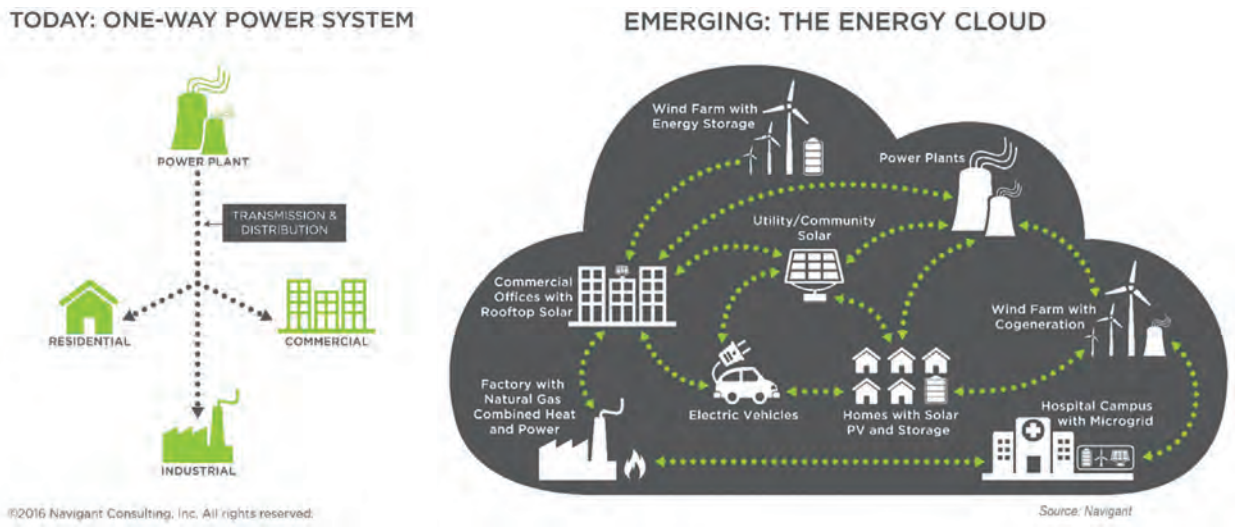
INTRODUCTION

The electric grid is becoming "smarter" with the deployment of technologies that allow for two-way communication and the transfer of data between utilities and consumers. Information provided by the grid enables customers to decrease electricity costs and boosts the reliability of electrical infrastructure. Electricity data also equips third parties with information to create new energy-saving products and services. However, measures must be taken to protect customers' privacy.

Information from the grid enables customers to decrease costs and increases the reliability of the electricity infrastructure.

To maintain consumer privacy, electricity consumption data and customers' personal information must be protected. Personal information linked with consumer-specific energy usage data could be used to identify and monitor behavior patterns inside homes or businesses. This is possible because electrical appliances such as refrigerators and air conditioners can be identified by their unique load signatures -- distinct energy consumption patterns specific to each source. Thus, personal information linked with load signatures may be used to perform real-time surveillance.

Some states have implemented policies related to data access. These actions will be analyzed and compared to provide insight as to how data access is possible while respecting customer privacy. This analysis may motivate more states to adopt policies for data access.



This image illustrates how the traditional one-way power system is moving towards two-way communication. Bidirectional exchanges allow for data transferring. (Published with permission from Navigant)

ELECTRICITY USAGE DATA IS BENEFICIAL

Smart grid technologies utilize electrical metering and monitoring equipment. These tools allow for two-way communication between utility companies and customers and enable data transference. In addition, information accumulated from bidirectional interactions on the grid enhances its design by improving reliability, flexibility and power quality. When electricity infrastructure is damaged as a result of a physical attack or other event, usage data will provide quicker response times, boosting the grid's resilience.

Currently, various tools are available that translate data into meaning, such as phone applications and home energy management systems. These allow customers to understand their usage patterns, enabling them to be proactive with their electricity consumption and decrease costs. The smart meter also measures, records and transmits granular information to communicate with utilities, monitor usage and bill customers. Smart meters permit customers to view usage online and manage billing charges, eliminating the expenses for a meter reader to visit homes or businesses.

There are more than seven million smart meters in homes today.[2] Data is collected and transmitted by smart meters, which benefits customers and the grid. Since smart meters report electricity consumption in time intervals, utilities have the opportunity to set pricing that varies by season and time of day. This can be used to reward customers for shifting electricity usage to off-peak periods.

Various tools are available that translate data into meaning, such as phone applications and home energy management systems. This is a picture of Comverge's IntelliSOURCE-Customer product, which allows consumers to manage thermostats and other appliances and helps reduce household energy consumption. (Published with permission from Comverge)

Off-peak electricity usage helps prevent brownouts, a reduction of electricity available in a particular area, and blackouts, a failure of electric power supply. In addition, expensive electricity generation methods are not needed for the grid as often. Furthermore, smart meters provide fast power notifications to utilities in the event of an incident and monitor the quality of power to prevent malfunction.

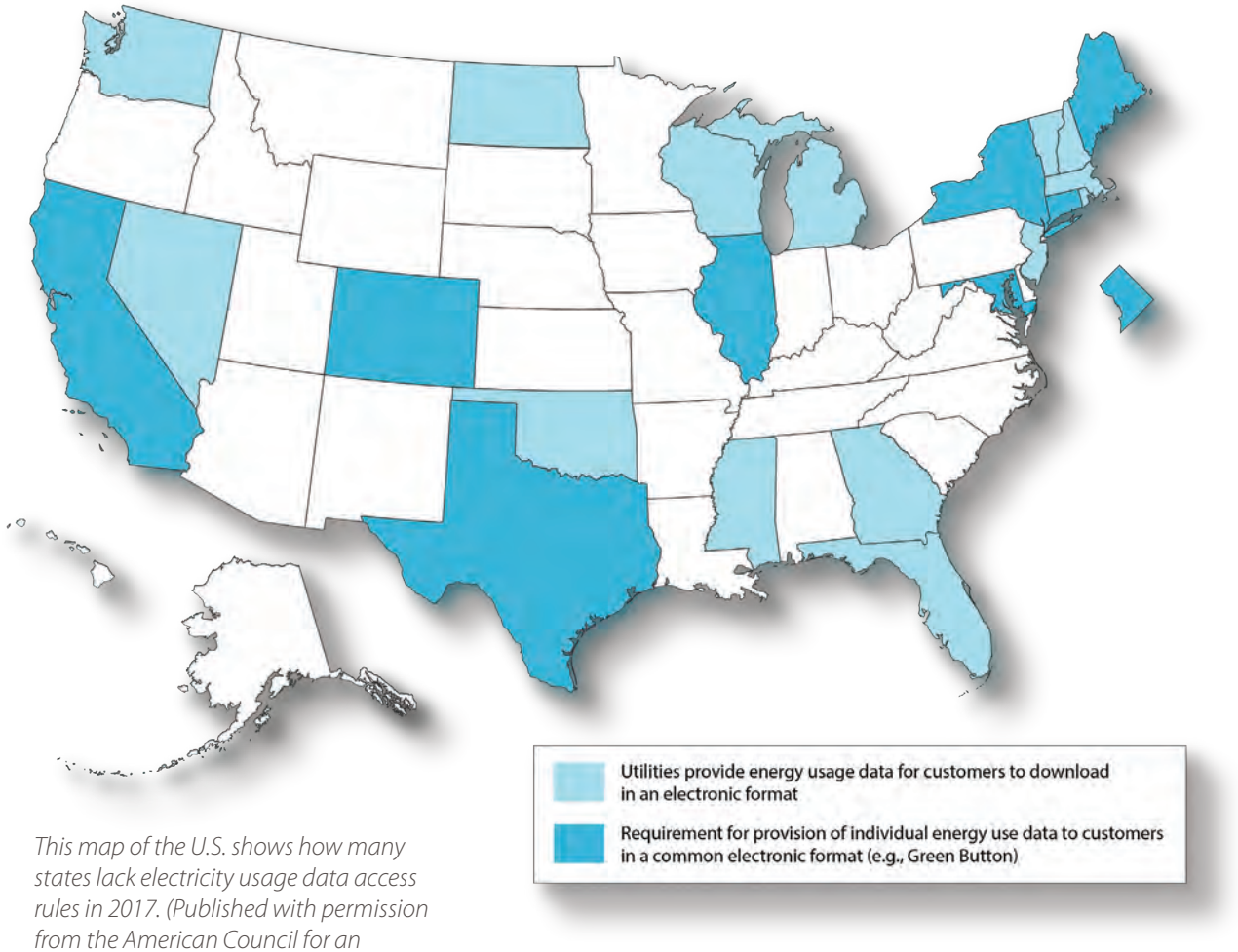
Electricity usage data is helpful for businesses to create new energy-saving products and services. Comverge has created the IntelliSOURCE-Customer product, which allows consumers to manage thermostats and other appliances and helps reduce household energy consumption. Oracle provides software services for consumers to reduce electricity consumption. FirstFuel offers energy analytics to reduce service costs.[3] Companies like these are dependent on electricity data to run algorithms and evaluate energy use. In turn, new products and services are made available to customers and high-quality and technological leadership jobs are created, stimulating economic growth.

The grid is incorporating more distributed resources. These include energy efficiency, storage, electric vehicles, demand response technologies and renewable sources. Usage data helps integrate distributed resources into the electricity transmission and generation system. California is a state that is focusing on incorporating more distributed resources on the grid to meet its policy goals, help the grid resist failure and allow for a quick recovery in the event of a power outage.[4]

Today, utilities collect and store energy consumption data to bill customers, manage networks, coordinate with grid operators and report energy usage data. However, utilities are hesitant to distribute this information because of extra costs involved with processing and transferring such data. Additionally, utilities could suffer legal consequences from improper disclosures and privacy violations.[5]

To date, more than half of U.S. states lack clear legal rules for data access.

The federal 2012 Green Button program aims to allow consumers to download their electricity usage data.[6] While some utilities and industry partners have supported this program, others have questioned the utility of the data made available. The data is accessible for download only in CSV and XML formats that are widely used, but include technical standards that may not be easy for average consumers to understand. To date, more than half of U.S. states lack clear legal rules for data access. Because many customers and businesses do not have access to usage information, electricity data is underutilized.[7]



This map of the U.S. shows how many states lack electricity usage data access rules in 2017. (Published with permission from the American Council for an Energy-Efficient Economy)

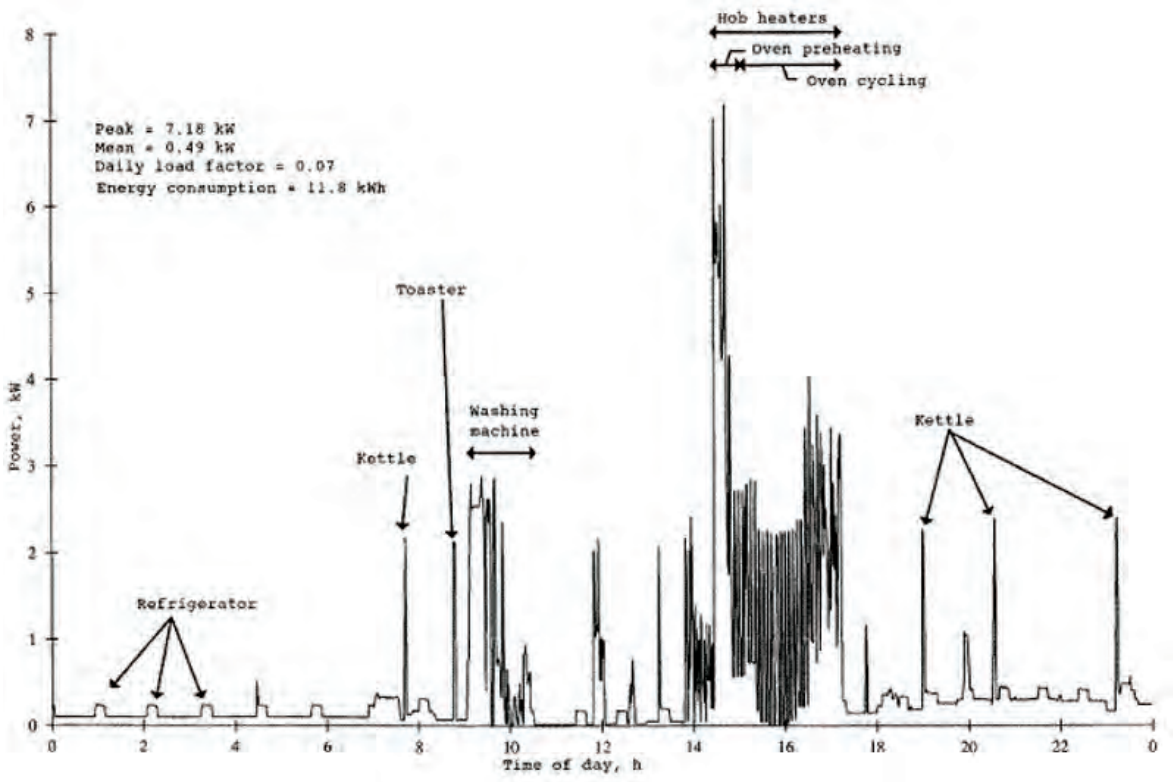
CONSUMER CONSUMPTION DETAILS COULD BE REVEALING

Electricity usage data provides many benefits to the operation of the grid and its customers. However, privacy concerns could result if usage information is linked with personal details of consumers and households or businesses.[8] This is because two types of data are collected by smart grid technologies: personally identifiable information and consumer-specific energy usage data.

Electrical appliances, such as refrigerators, air conditioners and electrical vehicles, generate unique load signatures. These signatures could potentially be linked with personal information, such as a person's name, address, telephone number and payment history, and customer usage data, such as total electricity use at various times in a day, to perform real-time surveillance.

Linking personal information with utility usage data is not just a hypothetical example. Electricity data has already been used by police detectives and law enforcement officials in Texas and California to identify marijuana growing operations in a home and to obtain a search warrant to access another home for the same reason. Moreover, electricity data that is hacked online could enable crimes like identity theft, burglary, vandalism, stalking and domestic abuse.

Just as detailed energy-usage data could be used to generate intelligence about household activities that many consumers might consider personal or sensitive, data could also be utilized to distinguish information about commercial or organizational activities. Hence, this could cause proprietary or competitive harm. Regulations of smart grid technologies should consider the implications for commercial and organizational utility customers.



Electrical appliances can be identified by their unique load signatures -- distinct energy consumption patterns specific to each source. Personal information linked with load signatures may be used to perform real-time surveillance. (Published with permission from the National Institute of Standards and Technology)

LEGAL ISSUES RELATED TO SMART GRID DATA

Utilities have long accessed customer energy usage data for billing purposes. However, privacy concerns were not previously raised because traditional meters needed to be physically accessed and they recorded electricity usage over longer time periods. In other words, traditional meters were not capable of collecting the type of granular, appliance-specific data that is possible with smart meters today. Furthermore, utilities did not have the means or economic incentive in the past to share usage data with other parties.

Traditional meters were not capable of collecting the type of granular, appliance-specific data that is possible with smart meters today.

The U.S. Supreme Court has historically provided a person's home with the highest legal privacy protections.[9] Since smart grid data is generated in the home, some argue that electricity data should only be accessible with a warrant and should not be seized without notice.

The Third Party Doctrine adds complexity to smart grid data and privacy debates. According to this principle, people who voluntarily give information to third parties, such as banks, phone companies and internet service providers, have "no reasonable expectation of privacy." This means that the Fourth Amendment, which prohibits search and seizure without probable cause, does not apply to information that is knowingly revealed to a third party. In *United States v. Miller* in 1976, the Supreme Court determined:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

In addition, the Supreme Court found in *Smith v. Maryland* in 1979 that "a person has no legitimate expectation of privacy for information he voluntarily turns over to third parties." U.S. Supreme Court Justice Sonia Sotomayor has argued that this doctrine needs to be revisited to reflect modern changes in society.[10] [11] This is especially illustrated by the fact that the emerging industry consensus is that customers are to provide consent for utilities to share smart grid data with third parties.[12] Thus, the Third Party Doctrine and the industry consensus appear at odds.

THE DEPARTMENT OF ENERGY'S PRIVACY PROGRAM

Studies conducted by utilities and consumer advocates have consistently shown that privacy issues are of tremendous importance to electricity customers. The U.S. Department of Energy views privacy and data access as complementary values, not competing goals. This is why its Office of Electricity Delivery and Energy Reliability created a voluntary code of conduct, the DataGuard Energy Data Privacy Program, with the Federal Smart Grid Task Force in 2015.[13]

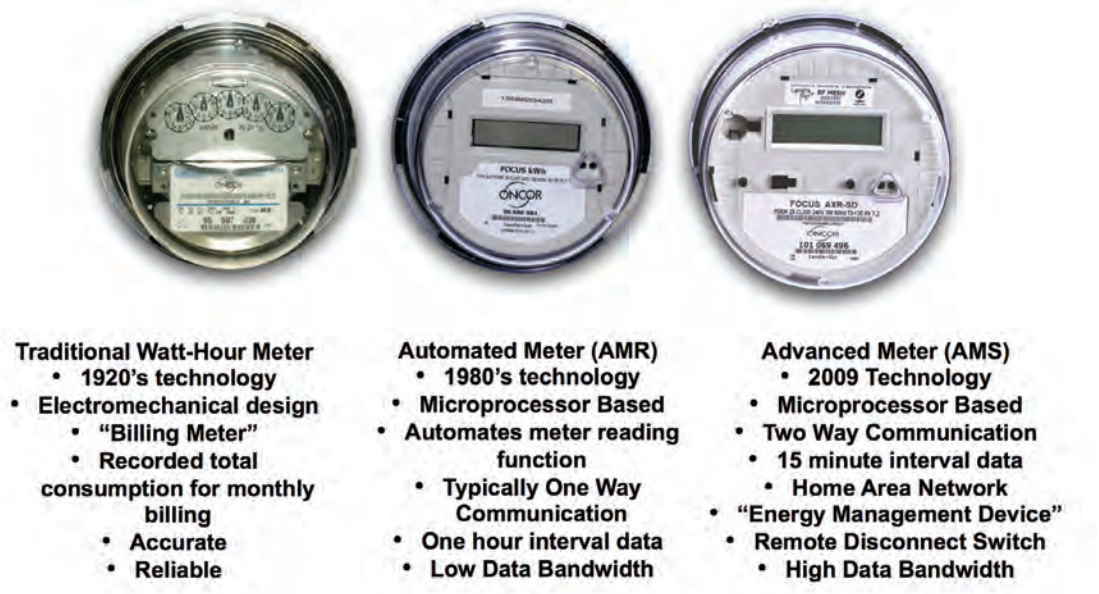
The DataGuard Energy Data Privacy Program supports usage data for customers. It promotes the existence of a customer consent process to share usage data with parties for purposes other than providing electricity. Customers also need an easy way to identify inaccuracies and request corrections and should be allowed to withdraw consent at any time.

A consent process should include the purpose and types of data that will be shared, along with the total duration. In addition, customers should receive notices of privacy policies and practices at the start of a service, on a regular basis and upon the customer's request. Customers should be notified of significant changes in procedure or ownership.

Data must be preserved to ensure its accuracy and protect against loss, unauthorized use, access or distribution. However, customer consent should not be required if third parties need access to electricity data to respond to life or property threats or if the information is needed by authorized law enforcement or other legal officials. In addition, providers ought to retain and dispose of data in accordance to local, state and federal rules and regulations.

Consumers should have a clear understanding how usage data is secured. This is necessary to prevent fraudulent disclosure. Service providers should not share a customer's sensitive personal information, such as a name in combination with a birth date, a mother's maiden name or other electronic signature. If such information is required, it should be provided directly by the customer.

Consumer electricity data should only be made available to authorized parties and users. Thus, access to this information ought to be retrieved via secure online connections.



Traditional meters were not capable of collecting the type of granular, appliance-specific data that is possible with smart meters today. This image explains the evolution of meter technology over time. (Published with permission from Oncor)

Usage information should be protected with a risk management program to identify, analyze and mitigate cybersecurity risks. A response program should be in place to identify, mitigate and resolve a breach that may put customer data at risk. Notices should be sent to customers if their data may have been compromised along with how the breach was corrected.

Utilities and third-party providers should incorporate these principles to create a friendlier environment to share and access data. Companies that have adopted this program include WattzOn, Open Energy Efficiency, Chai, Wexus Technologies, Inc., Energy Sense Finance, Utility API, Home Energy Analytics, Inc., Solar Verified, LLC and Solar Price Discovery Inc. More companies should include the DataGuard Energy Data Privacy Program norms to share electricity usage data and protect customers' privacy.

HOW SOME STATES SHARE ELECTRICITY DATA

State utility commissions regulate the retail side of electricity. This includes the distribution and selling of electricity. While more than half of U.S. states have no policy in place for electricity data access, some do. Exploring and comparing these diverse courses of action may provide some guidance for more states to develop data access strategies.

California

California Senate Bill 1476 allows customers to access their usage data. This law was signed on September 29, 2010 and went into effect on January 1, 2011. The bill requires utilities to obtain customer consent before sharing usage information with a third party. It also prohibits an electrical corporation from sharing or disclosing consumption data.

Today, California allows the sharing of energy data through Customer Data Access or Green Button Connect.[14] California also has a Data Request and Release Process that allows university researchers, state and federal agencies and local governments to request aggregated usage data from investor owned utilities.

When it comes to protecting customers' usage data, California Senate Bill 1476 requires utilities to use "reasonable security procedures and practices." This is to ensure the information is not available to unauthorized individuals and that the data is not modified or destroyed. The sale of electricity consumption information or any personally identifiable information is prohibited.

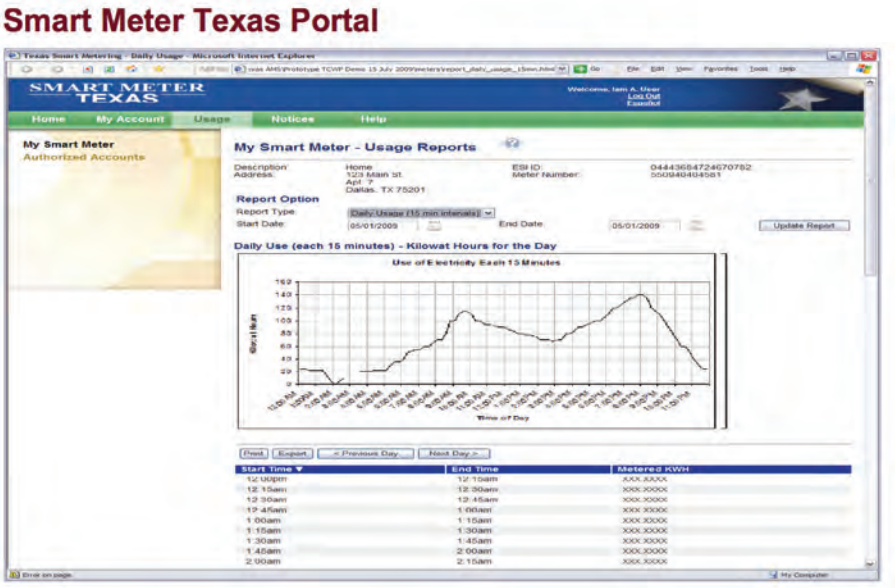
The California Public Utilities Commission was the first to establish rules to protect the privacy and security of customer usage data generated by smart meters.[15] The policies, aligned with the privacy and security principles adopted by the Department of Homeland Security, aimed to balance protecting consumer privacy and creating a new market for third-party participants.

Texas

According to Texas Utilities Code § 39.107(b), all data belongs to the customer. Consumers in Texas can access their energy usage data on the Smart Meter Texas portal. Usage information must be made available no later than the day after it was created and access must be convenient and secure. With customer consent, an electric utility is able to provide a customer's usage information to other entities.

The Smart Texas website reassures customers that their personal information will remain confidential and that it will not be sold or shared with third parties under any circumstances. Privacy terms and conditions are also easily accessible on the site.[16]

The Smart Texas website is endorsed by the Public Utility Commission of Texas and is a collaborative effort among the following utilities: AEP Texas Central Company, AEP Texas North Company, CenterPoint Energy, Houston Electric, LLC, Oncor Electric Delivery Company LLC and Texas-New Mexico Power Company. These utilities provide electricity to almost half of customers in the state.



Consumers in Texas can access their energy usage data on the Smart Meter Texas portal. (Published with Permission from Oncor)

Illinois

Electric utilities in Illinois are able to provide customer billing and usage data upon the request of the customer. Electric utilities are also able to provide anonymous information to alternative electric suppliers after they pay a "reasonable fee."[17]

The Illinois Commerce Commission recently approved Commonwealth Edison's new data sharing program, Anonymous Data Service. This allows companies and researchers

access to anonymous usage information for all zip codes where Commonwealth Edison has deployed smart meters.[18] The aggregated information must abide by the 15/15 rule. Meaning, the information from at least 15 customers must be included and no single customer's load can account for more than 15% of the total.[19]

Numerous stakeholders are allowed access to the Anonymous Data Service. Alternative retail suppliers in Illinois are interested in the service to develop new products. Academics and researchers are able to use the data to study how energy consumption varies from one zip code to the next. Companies that build new energy technologies for homes and businesses are likely to find the information helpful when creating the latest gadgets, and various levels of government are able to request the anonymized data.[20]

Vermont

In Vermont, customer energy usage information is confidential. This is supported by energy providers, energy efficiency utilities, the Public Service Department and the Public Service Board. As a result, electric utilities generally release usage data with the customer's written permission.

Intertwined products, software and networks on the grid have increased the number of potential entry points for cyberattacks.

However, the Vermont Public Service Board's Docket 7307 does require electric utilities to share aggregated data monthly, no more specific than the town level, with Vermont Energy Investment Corporation. This is a non-profit that manages a statewide energy efficiency program that utilized the aggregated information to develop a state map of electricity usage. The map identifies where new efficiency measures are needed in specific communities.[21]

Some utilities in Vermont have implemented Green Button. However, all utilities express some interest and are willing to investigate the costs and benefits of providing consumers with a mechanism to access their usage data.

PROTECTING CONSUMER USAGE INFORMATION

Intertwined products, software and networks on the grid have increased the number of potential entry points for cyberattacks. If communication disruptions and denial of services were to occur, the integrity of software, systems and data confidentiality would be compromised. Thus, cyber threats place confidentiality of consumer usage data at risk along with the safety and reliability of providing electricity.

Parties that handle consumer electricity usage data should be required to protect the privacy and security of that information. Useful methods that exist to remove personal information include aggregation, encryption and steganography.

Aggregation combines data that belongs to two or more individuals into groups over specific periods of time and removes personally identifiable information. For instance,

energy usage of 100 homes in a specific neighborhood could be grouped together to provide the necessary data for analysis per home while protecting customer identities and behavioral patterns. Another benefit of aggregated data is that it could reduce network delays. This is because large amounts of information could be delivered in packages instead of transmitted individually.[22]

Encryption scrambles data and encodes a message only known to authorized users. Thus, data can only be read by the recipient who has the key to open the information. While this is an effective way of implementing a layered security approach, it can be costly.[23] This is because the data must be stored with high capacity and frequent upgrades are required. Without capable systems, the security of the data can be compromised.[24] Finally, steganography hides a file or message with another file or message. Since the concealing image is unsuspicious, it is not suspected that valuable information may be underneath.

San Diego Gas & Electric (SDG&E) is an example of a utility that shares usage data while protecting customer privacy. After an electricity consumer authorizes SDG&E to share data, a unique identifier is assigned to transfer the consumer's usage data. This means the third party has the information associated with the unique identifier while protecting the customer's personal information.

Third parties could also develop efficient privacy control settings that allow consumers to control their data privacy. For instance, Tendril, a company that works with energy providers throughout the world, suggested that consumers use interactive controls such as those on Facebook to manage privacy settings.[25] This would allow customers to easily access their privacy settings and adjust them at any time.

These approaches protect customers' personal information while still enabling data to be valuable and shared. It must not be forgotten that aggregating and anonymizing data requires computational costs, time and effort. Additional resources are needed to modify, store, process and transfer large amounts of information.[26]

SECURING ELECTRICITY INFRASTRUCTURE FROM CYBER THREATS

There are at least 27 programs in the Department of Energy, Department of Homeland Security and the Federal Energy Regulatory Commission (FERC) to protect the grid from cyber breaches.[27] Currently, federal legislation exists for cybersecurity standards of the bulk power system, but is lacking for the distribution system.

GridEx III, a mock cyberattack exercise in November 2015 hosted by the North American Electric Reliability Corporation, found improvements need to be made to the cybersecurity of the distribution system.[28] Cybersecurity threats and attacks on the distribution system could have implications for the bulk power system and for broader national security and economic interests.

The distribution system delivers electricity to pipelines, water systems, telecommunications and other critical infrastructure, including critical government and military facilities. This means cyberattacks on this system could disrupt electricity service to such facilities, resulting in devastating economic and security consequences. Suggested enhancements include better communication and information sharing within organizations and agencies and clear plans to reestablish power after a major outage. Securing the electrical infrastructure is critical to protecting consumer personal information and usage data.

One solution to protect electrical infrastructure from cyber threats is to create a repository that stores cyber threat information, such as malicious internet protocol addresses.[29] The Department of Homeland Security is currently conducting a pilot to explore this option.[30] A storage bank allows cyber threat information to be shared anonymously by the federal government, industry and utilities. In addition, data would be stored, aggregated and analyzed to increase shared awareness about current and historical cyber conditions.

The private sector must also work together to protect their products from cyber threats. One example is how Check Point, Cisco, Fortinet, Intel Security, Palo Alto Networks and Symantec collaborate to protect their customers through threat intelligence sharing as members of the Cyber Threat Alliance.[31] More industry partners should follow their example and join forces to protect their products, services and customers from cyber threats.

Cybersecurity threats and attacks on the distribution system could have implications for the bulk power system and for broader national security and economic interests.

Public utility commissions ought to request utilities pursue efforts to protect against cyber threats. According to Richard Mroz, President, New Jersey Board of Public Utilities, security and data issues are intertwined.[32] Utilities in New Jersey are required to develop programs and procedures to identify and mitigate cyber risks, report incidents and suspicious activity, create incident response and recovery plans and provide training programs. In Pennsylvania, utilities are required to maintain physical and cybersecurity, emergency response, and business continuity plans and report cyber and physical attacks that cause more than $50,000 in damages. In Texas, an independent meter data-management organization specifies cybersecurity standards and the public utilities commission conducts annual security audits. More states should call for their utilities to implement protective measures against cyber threats.

Lawmakers must require standard performance criteria to ensure utilities are protected from cyber threats.[33] Detailed cybersecurity evaluations of individual facilities need to be conducted to identify strengths and weaknesses. Distribution employees also ought to be trained and accredited to enhance their cybersecurity skills.

Since cyberattacks on the distribution system could affect the bulk power system, it may be best to eliminate the jurisdictional divide and expand FERC's role. Currently, FERC regulates the transmission and wholesale of electricity in interstate commerce. In addition,

an agreement must be reached as to which parties will be responsible for paying for these activities. Provisions to encourage information sharing amongst federal agencies and industry should continue to develop.

DEVELOPING STATE POLICIES ON SHARING ELECTRICITY DATA

Customers with access to their electricity usage data can be proactive with their energy consumption and decrease costs. Since many states in the U.S. lack policies related to electricity data access, it is worth mentioning some issues that should be addressed as other states develop courses of action.

Consumer Consent Process

The emerging industry consensus is for customers to provide consent for utilities to share usage information. This means states must develop a process that allows consumers to do so. Customers could provide consent in written form, as required in Connecticut and Texas, or utilize an internet portal, such as the online authorization process on San Diego Gas & Electric's webpage.

The emerging industry consensus is for customers to provide consent for utilities to share usage information with other parties.

An opt-in authorization process should record the customer's approval, specify the type of data to be released and state how that information will be used. It is important to allow consumers to have a flexible opt-in or opt-out system because individuals have different thresholds when sharing such potentially sensitive information. Customers should also have the option to withdraw consent at any time.

In some cases it may be best for utilities to share usage details with a third party. States may want to transition towards standardized, machine-readable formats to transfer customer usage data efficiently. However, there may be instances where this information is best provided by the consumer to streamline the process. Customers could provide data to third parties with basic and sophisticated in-home displays through a home energy management system.

Authorization of Third Parties

Some states may find it necessary for third parties to undergo authorization to meet basic requirements prior to obtaining customer usage data. This could safeguard the privacy and usage information of electricity consumers and ensure third parties have the capabilities they claim. States and localities could provide these assurances via registration, licensing or approval from a third-party certifying body.

If certification requirements are deemed necessary, states, localities, utilities and third parties need to coordinate and create an efficient process. There should be

little paperwork and minimal regulatory burdens to prevent confusion from different requirements. While authorization may be viewed as helpful in some states, customers elsewhere may want the freedom to select from other available services. Thus, they could view an authorization process as an unnecessary barrier to entry and competition.

Funding Electricity Data Access

Electricity data access is costly because it requires time, effort and equipment. Processing third-party authorizations and storing, managing and securing data imposes more costs on utilities than those to provide electric power. Expenses could skyrocket if a utility is required to collect or retain data that exceeds what is necessary to provide electricity. Hence, who will pay for these extra costs needs to be determined.

One low cost solution for utilities to collect and retain large amounts of data is the cloud.

With regulatory oversight, the utility could charge all customers to pay for additional costs related to storing and transferring data. The downside to this is that it may distort the price of electricity. A second option is to only charge an additional fee to customers who utilize third-party resources. This ensures that customers who only use their data are charged, protecting customers not utilizing their data from extra costs.

A third option is to charge third parties that are causing the additional expenses. If utilities were allowed to charge businesses for access to customer data, they would have an additional source of revenue. This could help utilities since some state environmental goals and new technologies result in customers purchasing less electricity. Those against this idea argue that there should not be a fee for data access because third parties are acting on behalf of customers.

One low-cost solution for utilities to collect and retain large amounts of data is the cloud. Cloud computing is storing and accessing data over the Internet instead of using a computer's hard drive. The Central Intelligence Agency is one organization that utilizes Amazon's cloud to secure data. A 2016 study, conducted by Oracle and Zpryme, surveyed 100 utility executives and found that 45% currently use the cloud in some way. Another 52% are planning to use the cloud in the future.[34]

Utilizing Data for Other Purposes

Another topic that must be explored is whether third parties should obtain additional consent before sharing usage data for other purposes, such as marketing. Third parties may be interested in disclosing or reselling customer energy usage data to target their advertising and reduce the costs of their products and services.

If customer usage data were to be sold to businesses, advertisers could better tailor ads to specific behaviors. In addition, landlords could use the information to support claims that a tenant is in violation of a lease, and appliance and car manufacturers could determine validation of warranties. Finally, health insurance companies could use data to determine if an insured person has an unhealthy lifestyle, and divorce attorneys could use the

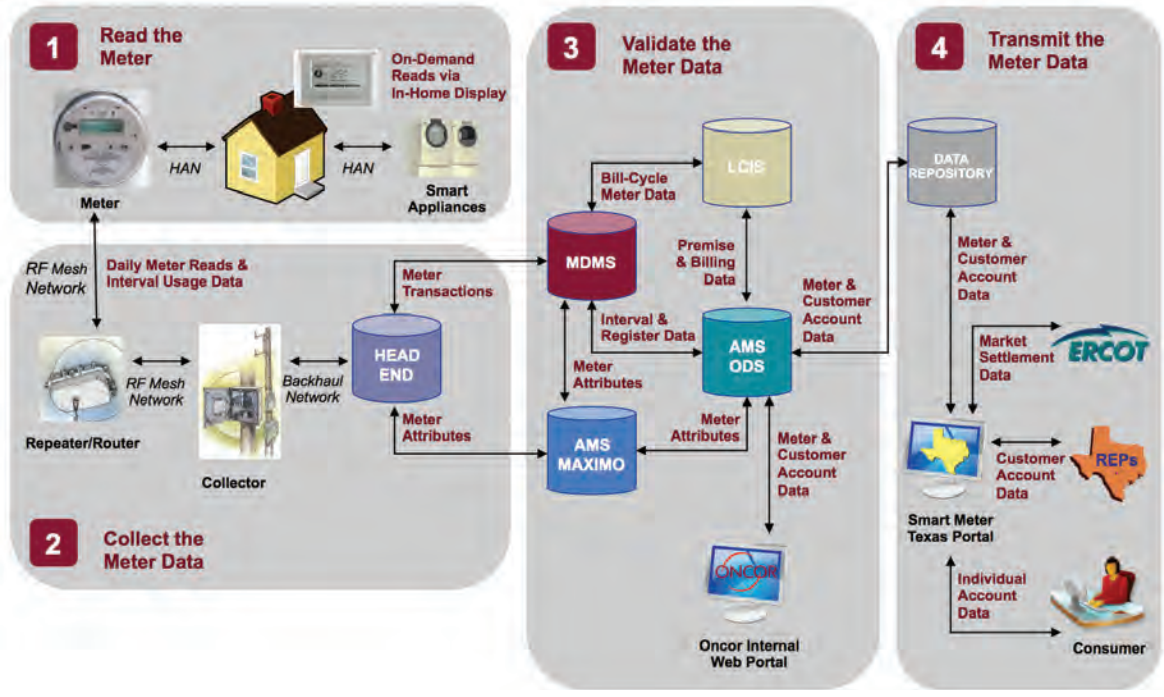
information as evidence to discredit the opposing party.

Several states do not allow utilities to share or sell customer-identifying data to third parties. For instance, Washington state law prohibits a utility from disclosing or selling private consumer information for marketing or other products that customers are not subscribed to without obtaining written consent. If the third party intends to use customer energy usage data for other purposes, then full and clear disclosure should be provided to the customer at a minimum.

Liability of Data Protection

When electricity data is transferred to a third party, utilities can no longer reasonably protect that information. Therefore, utilities should not be liable for transferred smart grid data. In September 2010, California passed a bill that shifted liability to the recipient of smart grid data.[35] This allows utilities to feel more comfortable transmitting the information.

Third parties should be required to comply with all legal requirements of usage data. This includes privacy, security, integrity and confidentiality of usage data. If information is utilized for purposes other than those stated in an agreement, the third party should be held accountable.



Electricity data access is costly because time, effort and equipment are required. This image shows the various steps involved for an individual to gain access to electricity usage data. (Published with permission from Oncor)

CONCLUSION

Smart grid technologies enable data transferring by utilizing equipment that allows for two-way communication. Electricity usage information is valuable because it allows customers to decrease costs and increases the reliability, flexibility and power quality of the grid. Usage data also provides third parties with information to create innovative energy products and services.

While electricity data provides many benefits, usage information linked with personal information, such as an individual's name or address, and households or businesses could potentially cause privacy concerns. This is because electrical appliances generate unique load signatures that could be linked with personal information and customer energy usage data to perform real-time surveillance.

Though some U.S. states have made clear legal regulations for electricity data access, over half of them lack policies. The policies analyzed and compared in this report along with the federal DataGuard Energy Data Privacy Program principles could be used as a guide for more states to allow for data access. Electricity consumers unable to retrieve usage data cannot use this information to decrease electricity costs, and they will have limited products and services available to them.

REFERENCES

1 David Perera, "Smart grid powers up privacy worries," *Politico*, Jan. 1, 2015 (http://www.politico.com/story/2015/01/energy-electricity-data-use-113901)

2 Phil Moeller, "Securing Smart Grid Data," *Lexington Institute*, https://www.youtube.com/watch?v=_82Il4xlS2U

3 Justin Worland, "Your Utility Company Wants to Sell You More than Just Electricity," *Time*, June 3, 2016 (http://time.com/4312285/utility-company-electricity-solar-power/)

4 Constance Douris, "California Aims To Incentivize Utilities To Adopt Third-Party Energy Resources," *Lexington Institute*, (March 2017).

5 Abrams Environmental Law Clinic, "Freeing Energy Data: A guide for regulators to reduce one barrier to residential energy efficiency," *University of Chicago Law School,* (June 2016).

6 Department of Energy, "Green Button," last accessed May 2017, https://energy.gov/data/green-button

7 Hannah Polikov, "Securing Smart Grid Data," *Lexington Institute*, https://www.youtube.com/watch?v=ZEngHLPYZi8

8 U.S. Department of Energy, *Data Access and Privacy Issues Related to Smart Grid Technologies*, https://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf (October 5, 2010).

9 Jay Stanley, "Securing Smart Grid Data," *Lexington Institute*, https://www.youtube.com/watch?v=xQnzlXYb4A4

10 Dr. Deborah Hurley, "Securing Smart Grid Data," *Lexington Institute*, https://www.youtube.com/watch?v=77QlwDQEn3Q

11 Parker Higgins, "The Troubling Truth of Why It's Still So Hard to Share Files Directly," *Wired*, June 24, 2014 (https://www.wired.com/2014/06/the-troubling-truth-of-why-its-still-so-hard-to-share-files-directly/)

12 American Public Power Association, *Smart Grid Data Privacy Concerns: An Overview of Recommended Guidelines*, http://www.publicpower.org/files/images/BookStore/APPA_Privacy_Concerns_guidelines.pdf.pdf (August 2014).

13 U.S. Department of Energy, *Data Privacy and the Smart Grid: Voluntary Code of Conduct*, https://www.smartgrid.gov/files/DataGuard_VCC_Concepts_and_Principles_2015_01_08_FINAL.pdf (January 8, 2015).

14 California Public Utilities Commission, *Decision Authorizing Provision of Customer Energy Data to Third Parties Upon Customer Request*, http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M077/K191/77191980.PDF (September 19, 2013).

15 California Public Utilities Commission, *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*, http://docs.cpuc.ca.gov/published/FINAL_DECISION/140369.htm#P95_5541 (July 28, 2011).

16 Smart Meter Texas, "Frequently Asked Questions," last accessed May 2017, https://www.smartmetertexas.com/CAP/public/home/home_faq.html#a1

17 Illinois Commerce Commission, *Investigation of Applicability of Sections 16-122 and 16-108.6 of the Public Utilities Act*, https://www.icc.illinois.gov/docket/files.aspx?no=13-0506&docId=208612 (January 28, 2014).

18 Robert Walton, "Illinois regulators approve ComEd's smart meter data sharing program," *Utility Dive*, Feb. 16, 2017 (http://www.utilitydive.com/news/illinois-regulators-approve-comeds-smart-meter-data-sharing-program/436338/)

19 Colorado Department of Regulatory Agencies - Public Utilities Commission, *Rules Regulating Electric Utilities*, https://www.sos.state.co.us/CCR/GenerateRulePdf.do?ruleVersionId=5595 (February 14, 2014).

20 David Unger, "Illinois regulators approve utility plan to share anonymous energy usage data," *Midwest Energy News*, Feb. 21, 2017 (http://midwestenergynews.com/2017/02/21/illinois-regulators-approve-utility-plan-to-share-anonymous-energy-usage-data/)

21 Dr. Audrey Lee and Maria Zafar, "Energy Data Center," *California Public Utilities Commission*, (September 2012).

22 Muhammad Daniel Hafiz Abdullah, Zurina Mohd Hanapi, Zuriati Ahmad Zukarnain and Mohamad Afendee Mohamed, "Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks," *KSII Transactions on Internet and Information Systems*, 9:4 (April 30, 2015): 1493-1515.

23 Scott Allen, "Enabling the industrial IoT with cyber security in mind," *ITProPortal*, May 4, 2017 (http://www.itproportal.com/features/enabling-the-industrial-iot-with-cyber-security-in-mind/)

24 Haripriya Rout & Brojo Kishore Mishra, "Pros and Cons of Cryptography, Steganography and Perturbation techniques," *IOSR Journal of Electronics and Communication Engineering*, (December 2014): 76-81.

25 U.S. Department of Energy, Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy, *Comments Of Tendril Networks, Inc.*, https://energy.gov/sites/prod/files/gcprod/documents/TendrilNetworks_Comments_DataAccess.pdf (July 12, 2010).

26 Audra E. Ryan-Jones, "Securing Smart Grid Data," *Lexington Institute*, https://www.youtube.com/watch?v=U2m7KlmGuDU

27 Mohana Ravindrath, "27 Separate Federal Programs Protect the Power Grid," *Nextgov*, Feb. 27, 2017 (http://cdn.nextgov.com/b/nextgov/interstitial.html?v=2.1.1&rf=http%3A%2F%2Fwww.nextgov.com%2Fcio-briefing%2F2017%2F02%2F27-separate-federal-programs-protect-power-grid%2F135740%2F)

28 North American Electric Reliability Corporation, *Grid Security Exercise: GridEx III Report*, http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf (March 2016).

29 U.S. Department of Homeland Security, *Enhancing Resilience Through Cyber Incident Data Sharing And Analysis*, https://www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015_v2.pdf (June 2015).

30 Matt Leonard, "DHS Preps Cyber Incident Data Repository," *GCN*, Apr. 24, 2017 (https://gcn.com/articles/2017/04/24/cyber-incident-data-repository.aspx)

31 Cyber Threat Alliance, *Cyber Threat Alliance Expands Mission through Appointment of President, Formal Incorporation as Not-for-Profit and New Founding Members*, https://www.cyberthreatalliance.org/pr/pr-021317.html (February 24, 2017).

32 Richard Mroz, "Securing Smart Grid Data," *Lexington Institute*, https://www.youtube.com/watch?v=vzY2gNQdwkY

33 Co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative, "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat," *Bipartisan Policy Center*, (February 2014).

34 Oracle Utilities and ZPryme, "On Cloud Now: Cloud Technologies are Here for Utilities" *Oracle Utilities,* (February 2016).

35 H. Russell Frisby Jr. & Jonathan P. Trotta, "The Smart Grid: The Complexities and Importance of Data Privacy and Security", *CommLaw Conspectus,* 19 (2011): 297-341.

Future of the Power Grid Series

Supported by the Severns Family Foundation

1. *Keeping the Lights On: How Electricity Policy Must Keep Pace with Technology*, Don Soifer and Daniel Goure, July 2014

2. *Challenges and Requirements for Tomorrow's Electrical Power Grid*, J. Michael Barrett, June 2016

3. *Connecting Microgrids With Public-Private Partnerships To Meet Critical Needs,* J. Michael Barrett, September 2016

4. *California Aims To Incentivize Utilities To Adopt Third-Party Energy Resources,* Constance Douris, March 2017

5. *Balancing Smart Grid Data and Consumer Privacy,* Constance Douris, June 2017

ABOUT THE AUTHOR

Constance Douris is Vice President of the Lexington Institute. Her current research interests include the electric grid and cyber security. Douris has been interviewed, published or quoted by various news outlets including the Associated Press, *New York Times*, *Washington Post*, and *The National Interest*. Douris has a Master and Bachelor of Arts in political science from California State University, Fullerton.

June 2017

Lexington Institute

1600 Wilson Boulevard, #203
Arlington, VA 22209

Telephone: 703-522-5828
Web: www.lexingtoninstitute.org
mail@lexingtoninstitute.org