REGULATORY GUIDE

Freeing Energy Data

A guide for regulators to reduce one barrier to residential energy efficiency

Abrams Environmental Law Clinic

University of Chicago Law School

June 2016

THE UNIVERSITY OF CHICAGO
THE LAW SCHOOL

Acknowledgments

The contributors to this report are Evan Feinauer ’15, Sean Fernandes ’16, Cole Francis ’17, Alex Gross ’16, Molly Jardine ’17, Nick Oliver ’16, Anna Sims ’16, and Associate Clinical Professor of Law and Abrams Environmental Law Clinic Director Mark Templeton.

The contributors wish to express deep gratitude to those people who spoke with us about this project and those who reviewed drafts of this manuscript. We thank Andy Frank, Matt Gee, Sean Helle, Kristin Munsch, Bob Sloan, Allen Stayman, Lior Strahilevitz, and colleagues at the works-in-progress workshop of the Energy Policy Institute at Chicago for their invaluable input at various stages of our research and writing. We appreciate production support from Molly Blondell and Natalia Ginsburg, outreach assistance from Trudy Vincent and Matt Greenwald, and publicity help from Eric Hernandez, Vicki Ekstrom High, and Sam Ori.

We are grateful for financial support for this effort from the Joyce Foundation, the 1896 Fund at the University of Chicago, and the Jonathan Mills Fund at the University of Chicago Law School.

All errors, omissions, and misstatements are the sole responsibility of the contributors to this report.

The Abrams Environmental Law Clinic would appreciate any comments or questions that you have about this work. We welcome in particular the opportunity to speak with legislators and regulators about measures that they can adopt from our recommendations. You can contact the clinic via Director Templeton’s e-mail (templeton “at” uchicago.edu) or 773-702-9611.

Table of Contents

Executive Summary

Increasing energy efficiency in residences can help to reduce the amount of energy consumed per home, to decrease greenhouse gas emissions, and to combat global warming. Entrepreneurs are actively developing sophisticated models for reducing energy intensity in residences and in targeting the homes with the greatest savings potential. However, for these entrepreneurs and others to realize the maximum amount of savings, legislators and regulators need to remove legal barriers that significantly limit access to energy-use information necessary for these models. This report shows how this can be done in a way that balances the concerns of utilities, energy-efficiency entrepreneurs, privacy advocates, and the public.

Third-party energy-efficiency service providers (EESPs) improve the energy efficiency of homes in a variety of ways. EESPs identify opportunities for reducing energy intensity by comparing current energy-usage practices to those achievable by using energy-efficient technology. For example, by accessing data held by utilities, EESPs can identify which houses consume more power than others when adjusted for certain factors such as number of square feet; the EESPs can then target those houses for energy-efficiency upgrades. With good projections about the amount of energy that can be saved at a given home, EESPs can offer innovative financial arrangements, such as capped bills in which the customer pays the EESP a fixed amount each month for energy services, and the EESP pays the utility for the actual energy used, which covers the costs of the upgrades it installed and provides it with a profit.

Utility companies already have access to large quantities of residential energy-use data. In order for EESPs to operate effectively and to have maximum impact, EESPs need better access to this data.

Unfortunately, legal ambiguities—along with concerns of consumer privacy advocates and utilities—appear to have discouraged utilities from releasing the data to EESPs. There is very little existing law allocating liability for the disclosure of energy-use data; those interested in this issue must refer to a patchwork of utility laws, privacy statutes and the common law to assess the legal risks. Further, some consumers may have privacy concerns about their utility releasing data about how much energy the consumer uses in his or her home. Utility companies may be hesitant to disclose the data they have for fear of legal

liability for any harm that may occur as a result of sharing this data for violating data-privacy laws. Therefore, it may presently be safest for those who have the data not to release any of it. Additionally, releasing this data to EESPs might threaten the ability of the utility to monetize the value of this data and would likely create implementation costs.

This report urges creation of a legal regime that permits energy-use data disclosure to certain third parties while addressing consumer and utility concerns. This report provides a slate of solutions—each of which has its own advantages and disadvantages—from which policymakers can select when designing the best laws and regulations for their constituents. The solutions include removing individually identifiable data so that consumers are more likely to be safe from privacy violations, implementing procedures for sharing data securely, allocating liability among the parties, and determining which parties can be allowed to receive consumer energy-use data, among other important tools.

For example, regulators can address privacy concerns by requiring that the utilities or another third party aggregate the data—by combining it across groups or time or both—or anonymize the data—by altering it to remove the users' personal identifying information—before the EESPs gain access to the information. The more the data is aggregated and anonymized, the more consumers will be protected from unwanted invasions of privacy. However, the less the data is aggregated and anonymized, the more valuable the data is to EESPs. Finding the right balance is difficult but critical.

As another example, regulators can assign liabilities for mishaps or data breaches so that the relevant parties are aware of what steps they must take to protect themselves from their respective potential liabilities. Setting clear rules eliminates regulatory ambiguities and encourages private parties to find their own contractual solutions (e.g., indemnification, insurance); the government could also require parties to undertake some of these solutions (e.g., posting a bond or purchasing data-breach insurance).

In addition to exploring possible solutions, this report provides model rules as examples of language that legislators or regulators can use to implement the various options. Whether a jurisdiction prefers rules that favor utilities, EESPs, or consumers on balance, we believe that all three groups will be better off by implementing these rules and facilitating the release of energy data, rather than maintaining the status quo.

Although this report is designed to serve as a guide to regulators and policymakers seeking to regulate energy-use data disclosure, it may also be useful to anyone who is interested in consumer privacy or improving energy efficiency. If designed correctly, proper regulation in this area will lead to lower energy bills, wealthier consumers, adequate

protection of consumer privacy, clear-cut allocation of liability for all parties involved, fewer greenhouse gas emissions from residences, and a reduction in the rate of global warming.

Introduction

This report advocates for improving entrepreneurs' access to residential energy-use data, thereby increasing the deployment of cost-effective energy-efficiency measures, generating savings and improving the environment. While this report does discuss policy, its focus is on informing policymakers on how to address liability, consumer privacy, and administrative concerns that could arise when third parties receive energy-use data from utilities. What makes this report novel compared to other efforts is that it provides model language for laws or rules that lawmakers or regulators can use as building blocks to open up access to energy data.

The Opportunity

Energy-efficient technologies and practices allow for similar levels of output—e.g., heating, cooling, lighting, mechanical work, etc.—with lower levels of energy inputs than those currently implemented. As a result, consumers use less energy, fewer fossil fuels are burned, fewer greenhouse gases are emitted, and less global warming occurs.[1] If the technologies and practices are cost-effective, then consumers pay less as well.

---

1. Many of points made in this report also apply to demand-response programs. Demand response involves shifting when energy is consumed, not necessarily how much energy is consumed. "Demand response is an electricity tariff or program established to motivate changes in electric use by end-use customers, designed to induce lower electricity use typically at times of high market prices or when grid reliability is jeopardized. In regions with centrally organized wholesale electricity markets, demand response can help stabilize volatile electricity prices and help mitigate generator market power. Demand response can include consumer actions that can change any part of the load profile of a utility or region. Common methods of engaging customers in demand response efforts include offering a retail electricity rate that reflects the time-varying nature of electricity costs or programs that provide incentives to reduce load at critical times. Radio or internet-controlled switches on residential air conditioners or electric water heaters is but one of many methods used." *See Demand Response – Policy*, U.S. DEP'T OF ENERGY, http://energy.gov/oe/services/electricity-policy-coordination-and-implementation/state-and-regional-policy-assistanc-4 (last visited June 20, 2016). Entrepreneurs who have access to residential energy data can make effective use of tools to shift when energy is consumed in households, thereby reducing peak demand and saving consumers money.

Fossil fuels are the primary fuel source for the generation of electric energy,[2] and burning them produces greenhouse gases that are warming the Earth. The Intergovernmental Panel on Climate Change (IPCC) has estimated that, without significant changes to how energy is produced and consumed, the world could experience mean surface temperatures 6.7 to 8.6 degrees Fahrenheit above those measured between 1850 and 1900 by 2100.[3] Economist Michael Greenstone recently asserted that burning through all currently extractable fossil fuels would raise temperatures 16.2 degrees Fahrenheit.[4]

Implementing energy-efficiency measures reduces greenhouse gas emissions.[5] A McKinsey & Company study estimated that implementing cost-effective energy-efficient technologies in the United States broadly could potentially abate up to 1.1 gigatons of greenhouse gas emissions annually.[6] Reducing energy consumption through energy efficiency reduces the need for fossil-fuel energy generation, which reduces the greenhouse gas

---

2. *See World Energy Outlook 2015*, INT'L ENERGY AGENCY (Nov. 10, 2015) at 310 (table 8.2) (showing fossil-fuel share of electricity generation worldwide at 67% in 2013); *Annual Energy Outlook 2015*, U.S. ENERGY INFO. ADMIN. (Apr. 2015) at 24, http://www.eia.gov/forecasts/aeo/pdf/0383(2015).pdf (showing fossil-fuel share of electricity generation in the U.S. at 67% in 2013). Fossil fuels are also the most commonly used forms of energy for transportation. *See How We Use Energy: Transportation*, NAT'L ACAD. OF SCI., ENG'G, MED., http://needtoknow.nas.edu/energy/energy-use/transportation/ (last visited May 6, 2016) (stating that 86% of all the energy used in the transportation sector in America comes from gasoline and diesel fuels).

3. *Climate Change 2014 Synthesis Report Summary for Policymakers*, INTERGOVERNMENTAL PANEL ON CLIMATE CHANGE (2014) at 20, https://www.ipcc.ch/pdf/assessment-report/ar5/syr/AR5_SYR_FINAL_SPM.pdf. The study listed the temperatures in Celsius instead of Fahrenheit so the range was recorded as 3.7°C to 4.8°C. When the IPCC took into account climate uncertainty, it found with a high degree of confidence that temperatures could range from 2.5°C to 7.8°C. *Id.*

4. Michael Greenstone, *If We Dig Out All Our Fossil Fuels, Here's How Hot We Can Expect It to Get*, N.Y. TIMES (Apr. 8, 2015), http://www.nytimes.com/2015/04/09/upshot/if-we-dig-out-all-our-fossil-fuels-heres-how-hot-we-can-expect-it-to-get.html?_r=0.

5. *Climate and Energy Resources for State, Local, and Tribal Governments*, U.S. ENVTL. PROT. AGENCY, http://www3.epa.gov/statelocalclimate/state/topics/energy-efficiency.html (last visited Apr. 18, 2016).

6. Hannah Choi Granade et al., *Unlocking Energy Efficiency in the U.S. Economy*, MCKINSEY & CO. (July 2009) at iii, 91, https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/Sustainability/PDFs/US_energy_efficiency_full_report.ashx; see also Jon Creyts et al., *Reducing U.S. Greenhouse Gas Emissions: How Much at What Cost?*, MCKINSEY & CO. (December 2007), http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Sustainability%20and%20Resource%20Productivity/Our%20Insights/Reducing%20US%20greenhouse%20gas%20emissions%20How%20much%20at%20what%20cost/Reducing%20US%20greenhouse%20gas%20emissions%20How%20much%20at%20what%20cost%20Final%20Report.ashx.

emissions that contribute to global warming; therefore, reducing energy use through improving energy efficiency should help slow the rate at which warming will occur.[7]

Implementing energy-efficiency measures provides a number of economic benefits. First, deploying energy-efficient technology can save consumers money. McKinsey has estimated that combining energy-efficient technologies with behavior adjustments could lead to savings of as high as 20% of total U.S residential-energy consumption.[8] Second, in addition to the savings realized directly by those who implement the energy-efficiency measures for themselves, lower demand for electricity in general—especially at peak times—reduces the need for high-cost power to meet marginal demand. It also reduces the need to construct additional generation and transmission infrastructure, which spares all consumers from paying for those investments.[9] Third, energy efficiency supports job creation.[10] According to a report by the American Council for an Energy-Efficient Economy, "a $1 million investment in building efficiency improvement will initially support approximately 20 jobs throughout the economy."[11] Fourth, energy efficiency mitigates financial risks associated with fuel markets. According to the U.S. Environmental Protection Agency (U.S. EPA), "energy efficiency also diversifies utility resource portfolios and can be a hedge against uncertainty associated with fluctuating fuel prices and other risk factors."[12]

---

7. *See generally Sources of Greenhouse Gas Emissions*, U.S. ENVTL. PROT. AGENCY, http://www3.epa.gov/climatechange/ghgemissions/sources/commercialresidential.html (last visited Apr. 18, 2016).

8. David Frankel et al., *Sizing the Potential Behavior of Energy Efficiency Initiatives in the Residential Market*, MCKINSEY & CO. (Nov. 2013) at 4, http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/epng/pdfs/savings_from_behavioral_energy_efficiency.ashx.

9. *See Assessing the Multiple Benefits of Clean Energy*, U.S. ENVTL. PROT. AGENCY (Sept. 2011) at 4 & n. 2, https://www.epa.gov/sites/production/files/2015-08/documents/epa_assessing_benefits.pdf . *See* generally Christopher Russell et al., *Recognizing the Value of Energy Efficiency's Multiple Benefits*, AM. COUNCIL FOR AN ENERGY-EFFICIENT ECON. (Dec. 2015), http://kms.energyefficiencycentre.org/sites/default/files/ie1502.pdf; Paul Chernick & John J. Plunkett, *Price Effects as a Benefit of Energy-Efficiency Programs*, AM. COUNCIL FOR AN ENERGY-EFFICIENT ECON. (2014), http://aceee.org/files/proceedings/2014/data/papers/5-1047.pdf; Brandon Davito et al., *The Smart Grid and the Promise of Demand-Side Management*, MCKINSEY & CO. (2010), https://www.smartgrid.gov/files/The_Smart_Grid_Promise_DemandSide_Management_201003.pdf.

10. *See* Granade et al., *supra* note 6, at 99.

11. *Energy Efficiency and Economic Opportunity Fact Sheet*, AM. COUNCIL FOR AN ENERGY-EFFICIENT ECON. (2012) at 1, http://aceee.org/files/pdf/fact-sheet/ee-economic-opportunity.pdf. ("By comparison, the same $1 million investment in the economy as a whole supports 17 jobs.").

12. *State Energy Efficiency*, U.S. ENVTL. PROT. AGENCY, https://www.epa.gov/statelocalclimate/state-energy-efficiency (last visited Apr. 18, 2016).

Policymakers have taken laudable steps to improve energy efficiency. They have developed and implemented energy-efficiency resource standards, required utilities to invest in energy-efficiency programs, provided direct financial support for investments in energy-efficient technologies, and created mechanisms by which utilities can rate recover for their investments in energy-efficiency measures.[13] For example, as of August 2014, twenty-four states had established specific "energy savings targets" for customer energy-efficiency programs.[14] Moreover, some areas have developed "direct install" initiatives, in which "energy-saving retrofits are performed in primarily low-income households."[15]

This report addresses the opportunity for growth in residential energy-efficiency services that comes from "open data." The idea of open data, defined as "the release of information by governments and private institutions and the sharing of private data to enable insights across industries,"[16] has garnered widespread support as a means to fuel innovation and investment by lowering currently existing barriers to information.[17] A 2013 McKinsey & Company study estimated the electricity sector's open-data potential at $340–580 billion in unexplored annual economic value worldwide.[18] Supplied with the knowledge that inadequate information is a major source of market failure in the energy-efficiency sector, the U.S. federal government,[19] states,[20] and cities[21] have gradually begun adopting energy-oriented open-data

13. *See generally* N.C. Clean Energy Tech. Center, *Find Policies and Incentives by State*, DATABASE OF STATE INCENTIVES FOR RENEWABLES & EFFICIENCY, http://www.dsireusa.org/ (last visited Apr. 18, 2016).

14. *Energy Efficiency Resource Standards (EERS)*, AM. COUNCIL FOR AN ENERGY-EFFICIENT ECON., http://aceee.org/topics/energy-efficiency-resource-standard-eers (last visited June 21, 2016).

15. *Local Residential Energy Efficiency*, U.S. ENVTL. PROT. AGENCY, https://www.epa.gov/statelocalclimate/local-residential-energy-efficiency (last visited Apr. 18, 2016). *See, e.g.*, *Low-Income Multi Family Energy Retrofit Grant Program Preliminary Program Description & Application Process*, MASSACHUSETTS (2010), http://www.mass.gov/hed/docs/dhcd/ph/publicnotices/10-01b.pdf; *Residential Retrofit Energy Efficiency Program*, ILLINOIS DEP'T OF COMM. AND ECON. OPP. (2012), http://www.illinois.gov/dceo/whyillinois/KeyIndustries/Energy/EEIAG/Pages/LowIncomeEnergyEfficiencyAssistance.aspx.

16. James Manyika et al., *Open Data: Unlocking Innovation and Performance with Liquid Information*, MCKINSEY & CO. GLOBAL INST. (Oct. 2013), http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Business%20Technology/Our%20Insights/Open%20data%20Unlocking%20innovation%20and%20performance%20with%20liquid%20information/MGI_Open_data_Executive_summary_Oct_2013.ashx .

17. Barbara Grady, *Open Data Movement Grows, Pushing Cities Toward Resilience*, GREENBIZ (Sep. 23, 2013), http://www.greenbiz.com/article/open-data-movement-grows-pushing-cities-resiliency.

18. Manyika et al., *supra* note 16, at Exhibit E3.

19. *See, e.g., Open Data*, U.S. ENERGY INFO. ADMIN., http://www.eia.gov/opendata/ (last visited Apr. 18, 2016).

policies over the past two to three years. Last year, Senator Edward Markey and Representative Peter Welch introduced companion bills in the Senate[22] and the House[23]—the Access to Consumer Energy Information Act or the E-Access Act—which direct the Department of Energy to encourage states to allow customers to access their energy data.

The U.S. EPA, in its technical support guidance on reducing greenhouse gas emissions under the Clean Power Plan, has also described the lack of access to energy information as a key barrier inhibiting investment in energy efficiency.[24] Although U.S. EPA dropped energy efficiency as a "building block" when it finalized the Clean Power Plan, the agency still thinks that energy efficiency will be a significant way in which states meet their goals for reducing carbon emissions from the energy sector.[25] Better access to data can only help achieve these goals.

We believe a data-driven approach to the deployment of greater energy-efficiency services is the way of the future. By resolving information asymmetries that have currently inhibited growth in this sector, companies will be able to create, disperse, and improve their energy-efficiency products and services—and market forces will select which products and services can bring about cost-effective energy savings. Furthermore, as this report shows, policymakers have many tools available to ensure that "open data" does not have to come at the expense of consumer privacy. We believe—and we show—that goals of openness and data security are reconcilable.

Addressing a Significant Challenge

In order to capture the optimal benefits of energy efficiency, policymakers should take steps to increase energy-use data availability. They should therefore consider giving responsible energy-efficiency service providers ("EESPs") access to consumer energy-use data. EESPs are third-party companies, which are not directly involved in the utility-consumer

---

20. *See, e.g., California Energy Efficiency Statistics*, CAL. PUB. UTILS. COMM'N, http://eestats.cpuc.ca.gov/Views/EEDataPortal.aspx (last visited Apr. 18, 2016).

21. *See, e.g., City of Chicago Data Portal*, CITY OF CHICAGO, https://data.cityofchicago.org/ (last visited Apr. 18, 2016); *Chicago Energy Data Map*, CITY OF CHICAGO, http://energymap.cityofchicago.org/ (last visited Apr. 18, 2016).

22. Access to Consumer Energy Information Act or the E-Access Act, S. 1044, 1114th Cong. (2015).

23. Access to Consumer Energy Information Act or the E-Access Act, H. 1980, 1114th Cong. (2015).

24. *GHG Abatement Measures*, U.S. ENVTL. PROT. AGENCY, OFFICE OF AIR & RADIATION (June 10, 2014) at 5-5, http://www.epa.gov/sites/production/files/2014-06/documents/20140602tsd-ghg-abatement-measures.pdf.

25. *See* Carbon Pollution Emission Guidelines for Existing Stationary Sources: Electricity Utility Generating Units 80 Fed. Reg. 64666, 64670, 64673 (Oct. 23, 2015) (to be codified at 40 C.F.R. pt. 60).

relationship, that provide services to both consumers and utilities to reduce energy consumption. Different EESPs may have different business models.

Many EESPs focus on installing energy-efficient products, including pipe and wall insulation, new water heaters, and LED lighting, for example. With residential energy-use data, EESPs can make better recommendations to their clients about which products are cost-effective.

Some EESPs attempt to use innovative targeting techniques. They compile and assess data to determine which households are most likely to benefit from their assistance. They may also use leverage the predictive capacity of energy usage data to forecast cost-effective ways to reduce or shift energy demand, rather than or in addition to traditional energy audits.[26]

Other EESPs are trying to finance the installation of energy-efficient products for customers. For example, companies like Sealed depend on the availability of energy data to assess and to guarantee customer savings.[27] Sealed helps finance the installation of energy-efficient products for customers, bearing the risk of loss if energy savings fall short of expectations.[28] Sealed's ability to recover its investment depends on its ability to predict correctly and to share in future energy savings with its customers. Without good data, Sealed's savings models may be incorrect, leading to poor returns on investment, which would undermine its business model and its ability to provide energy-efficiency savings.

---

26. *See* Michael Murray & Jim Hawley, *Got Data? The Value of Energy Data Access to Customers*, MISSION DATA (Jan. 2016) at 4, http://www.missiondata.org/s/Got-Data-value-of-energy-data-access-to-consumers.pdf.

27. *See How It Works*, SEALED, http://sealed.com/how-it-works/overview (last visited Apr. 18, 2016); Katherine Tweed, *New York Green Bank Funds a Startup Making Pay-As-You-Save Efficiency Upgrades*, GREENTECH MEDIA (May 18, 2016), https://www.greentechmedia.com/articles/read/New-York-Green-Bank-Funds-a-Startup-Making-Pay-As-You-Save-Efficiency-Upgra ("New York startup Sealed just received a $5 million credit facility from the New York Green Bank. It's not the biggest winner in terms of financing dollars from the New York Green Bank, but the financing will be used for one of the more novel applications in the Green Bank's portfolio, rather than as a boost to the maturing solar loan and power purchase market. Sealed offers no- and low-cost efficiency retrofits that are paid back through a Sealed bill instead of through the utility bill—similar to a residential solar lease. Homeowners are guaranteed a lower bill than they would have paid through their utility.... The New York City-based startup is working with National Grid on a REV demonstration pilot that is still awaiting final approval and is in talks with two other New York utilities. Sealed has done about 150 projects so far, mostly through word of mouth and direct sales efforts. [Founder and President Andy] Frank said that volume is growing at about 40 percent per month. The company has mostly signed customers on Long Island but will use the $5 million from the Green Bank to continue to scale up in other counties in New York. Most of the upgrades are for renovations such as air sealing and HVAC work. The average project is about $10,000 to $15,000 after rebates and has a seven- to eight-year payback.").

28. *See How It Works*, SEALED, http://sealed.com/how-it-works/overview (last visited Apr. 18, 2016).

Other as-yet-unknown innovations and business models may arise. With reduced barriers to data access, new EESPs develop optimized targeting profiles, improved baseline usage and savings models, and alternative service offerings.

EESPs should have access to at least two types of data in order to be most effective. First, EESPs should have access to the results of the energy-efficiency programs that the utilities have deployed. The California Energy Efficiency Statistics portal is an example of a state initiative to distribute datasets on the efficacy of utility-implemented energy efficiency.[29] Having this information will help the EESPs understand which devices and behaviors saved what level of energy at what cost. Second, EESPs should have access to meter data. Recent technological innovations such as smart meters and other technologies can provide significantly more data about consumers' energy consumption than traditional meters concerning the quantity, time, and purpose for which energy is being used. If EESPs were able to analyze this data, they could isolate regions of particularly high-energy usage and target those regions with energy-efficient products and programming that would not only reduce energy consumption but also save consumers money on their energy bills.

Some states have given limited third-party access to such data already. At least nine states, namely California, Colorado, Illinois, Oklahoma, Oregon, Texas, Vermont, Washington, and Wisconsin, have adopted legal authority governing third-party access to customer data.[30] The majority of state efforts to date have focused on consent-based approaches, in which each individual consumer gives permission for an EESP to access to his or her data;[31] fewer have adopted the non-consent, anonymized-and-aggregated-data approach advocated for in this report. Moreover, these states are in the minority. In general—and even in the states that do have friendlier energy-data access laws—EESPs

---

29. *See* California Energy Efficiency Statistics, http://eestats.cpuc.ca.gov/; *see also* CAL. PUB. UTILS. COMM'N, *supra* note 20.

30. *See A Regulator's Privacy Guide to Third-Party Data Access for Energy Efficiency*, STATE AND LOCAL ENERGY EFFICIENCY ACTION NETWORK (Dec. 2012) at vii, http://web.mit.edu/cron/project/EESP-Cambridge/Articles/SEEA%20-%202013%20-%20cib_regulator_privacy_guide.pdf [hereinafter *A Regulator's Privacy Guide*]; Kari Lydersen, *Illinois Looks to Data Access for Energy Savings*, MIDWEST ENERGY NEWS (June 22, 2016), http://midwestenergynews.com/2016/06/22/illinois-looks-to-data-access-for-energy-savings/.

31. *See, e.g.,* Pub. Utils. Comm'n of the State of Cal., *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, 150-51 (July 29, 2011) ("Within six months of the mailing of this decision, PG&E, SCE and SDG&E must each file an application that includes tariff changes which will provide third parties access to a customer's usage data via the utility's backhaul when authorized by the customer.") [hereinafter *California PUC Privacy and Security of the Electricity Usage Data Decision*]; Lydersen, *supra* note 30.

believe that they could do more if they had more access to data to analyze energy-consumption patterns and develop tailored energy-efficiency programs.[32]

Utilities collect and retain data but are reluctant to distribute or sell it.[33] They appear not to have used the data significantly.[34] As a result, this invaluable data has been vastly under-utilized.

Utility companies are uniquely positioned to share this information. Historically utilities have been subject to special forms of regulation and public control to ensure that they operate in the public's interest.[35] The Federal Energy Regulatory Commission and state public utility commissions[36] have regulated many aspects of the utility sector, including rates, rates of return, investments, terms of service, and transmission rates. While this has changed to some extent with deregulation—first regarding generators, now regarding retail service

32. One EESP suggested that less aggregation will enable more innovation, because opening up the data will provide opportunities to promote energy efficiency in ways people cannot even imagine today. *See* Email from Andy Frank, Founder & President, Sealed, Inc., to Nick Oliver (Feb. 3, 2016, 11:21 CST) (on file with author).

33. *See generally* Gary Radloff, *Where's the Data? Numbers & Transparency Critical to Energy Planning*, WISCONSIN ENERGY INST. (Oct. 22, 2015), https://energy.wisc.edu/news/power-points/wheres-data-numbers-transparency-critical-energy-planning ("A quiet crisis in the energy sector is building around the quality of and access to energy data in the United States. Two distinct but related energy data issues are currently in play. The first is growing concern with the lack of up-to-date renewable energy and energy efficiency data from the Energy Information Administration (EIA), the federal agency responsible for forecasting energy trends. *And the second is reluctance on the part of regulated electric utilities to share energy data with others*.") (emphasis added); Edward Vine, *Confidential Data in a Competitive Environment: Setting a Regulatory Agenda*, ELECTRICITY J. (Apr. 1997), http://web.mit.edu/cron/project/EESP-Cambridge/Articles/Energy%20Data/Vine%201996%20-%20confidentiality%20of%20utility%20info.pdf ("Utilities will be reluctant to share data that gives them a competitive advantage over competitors."); Alissa Burger, *HUD Supports Utility Data Access*, INST. FOR MARKET TRANS. (Nov. 17, 2014), http://www.imt.org/news/the-current/hud-supports-utility-data-access ("One specific challenge is that building owners with separately-metered units have trouble obtaining whole-building data, especially in jurisdictions without benchmarking and transparency laws and where utility providers are reluctant to share tenant data with the owner.").

34. *See* Murray & Hawley, *supra* note 26, at 3. ("The absence of web and mobile tools offered by utilities is remarkable when one observes that many states have approved advanced metering infrastructure (AMI) or automated meter reading (AMR) systems, measuring the consumption of homes and businesses at 15-minute or hourly intervals. Rich datasets for understanding and optimizing both financial and environmental costs in homes and buildings exist—if only one could access them. Sadly, monthly bills remain the norm."); *but see* Kari Lydersen, *In Illinois, Real-Time Pricing Saving Utility Customers Millions*, MIDWEST ENERGY NEWS (May 4, 2016), http://midwestenergynews.com/2016/05/04/in-illinois-real-time-pricing-saving-utility-customers-millions/.

35. *See generally* Ari Peskoe, *A Challenge for Federalism Achieving National Goals in the Electricity Industry*, 18 MO. ENVTL. L. & POL'Y REV. 209 (2011) (detailing the history and purpose of public utilities).

36. State public utility commissions can also be known as state public service commissions or state commerce commissions. In this report, we will use the term public utility commission to refer to these kinds of entities.

providers in some states—it remains true that most consumers in most states have limited options to switch to other providers.[37] Furthermore, many of the public service requirements for the utilities remain in place in the states, even if consumers have the right to select among potential electricity providers.

These solutions should address some of the critiques made against energy- efficiency efforts to date. Some economists have questioned the economic returns of such initiatives. Hunt Allcott and Michael Greenstone have argued that the evidence on cost savings from energy efficiency "comes from engineering analyses or observational studies that can suffer from a set of well-known biases. Furthermore, even if the energy cost savings were known, energy-efficiency investments often have other unobserved costs and benefits, making it difficult to assess welfare effects."[38] However, this report rests on the idea that better access to data will help guide entrepreneurs and others to invest in cost-effective technologies and practices, and those entrepreneurs who do not are likely to find themselves marginalized or out of business. In other words, by utilities making data available, the market will sort out what investments truly are cost-effective and which are not.

---

37. Additionally, in theory, utilities do not necessarily need to be as concerned about releasing this information as other companies. Other companies that have a wealth of personal information about their customers do not share it even though it might provide benefits to society because they operate in competitive markets, have concerns about customer retention, and seek to monetize the value of this information for themselves. Utilities operate somewhat differently and may not operate in fully-competitive markets. It is not clear that consumers would or could switch to a different utility if their utility disclosed their energy-usage data, especially if it was aggregated and anonymized as described below. Furthermore, if a state public utilities commission were to require such releases by all electricity service providers, then no single company would benefit or could be penalized in the market for such releases to authorized parties. Additionally, utilities generally have not sought to monetize the value of this data significantly as discussed in Section I.E. *infra*.

38. Hunt Allcott & Michael Greenstone, *Is There an Energy Efficiency Gap?*, MIT CENTER FOR ENERGY AND ENVTL. POLICY RES. (2012) at 5, http://web.mit.edu/ceepr/www/publications/reprints/Reprint_239_WC.pdf. To quantify the economic benefit of energy-efficiency technology for consumers, Greenstone and other economists recently ran a randomized controlled trial of more than 30,000 households in Michigan. The study found that while on average the upgrades reduced energy consumption by 10 to 20 percent and in turn reduced energy bills, the cost of implementing the efficiency upgrades was nearly twice the energy savings. Meredith Fowlie et al., *Do Energy Efficiency Investments Deliver? Evidence from the Weatherization Assistance Program*, BECKER FRIEDMAN INSTITUTE FOR RESEARCH IN ECON. WORKING PAPER (June 23, 2015) at 4, https://econresearch.uchicago.edu/sites/econresearch.uchicago.edu/files/paper_draft_06_15_clean.pdf; Greenstone told the Associated Press after publication of the study that he is finding similar results in a second study in Wisconsin. *See* Jonathan Fahey, *Home Efficiency Upgrades Fall Short, Don't Pay: Study*, ASSOCIATED PRESS (June 23, 2015), http://bigstory.ap.org/article/7e461ff92e684cf5be0f783af7c9fd21/home-efficiency-upgrades-fall-short-dont-pay-study.

While this report does discuss policy issues, its focus is informing policymakers how to address the liability, consumer privacy, and administrative concerns that could arise when EESPs receive energy data from utilities. While many resources already document the value of energy efficiency, there is no thorough legal analysis of those concerns and how to address them. This report aims to fill that void. In particular, this report provides model language for laws or rules that lawmakers or regulators can use as building blocks to open up access to energy data.[39]

How to Use This Report

Section I gives an overview of the liability, privacy, and administrative concerns stakeholders have about EESPs receiving access to consumer energy data. This section aims to describe the concerns rather than to assess the validity of each concern.

Section II provides an overview of the different policy options available for creating a program that allows EESPs to gain access to energy-use data. These options include aggregating and anonymizing data; implementing procedures to control the transfer, receipt, and safekeeping of data; tailoring liability rules to protect the interests of various stakeholders; and creating eligibility requirements for EESPs to gain access to the data.

Section III then highlights different model rules for policymakers to consider. Some of these rules benefit all consumers, utilities, and EESPs, while others benefit one stakeholder group more than another. Because such an energy-data program can lower energy costs and improve energy efficiency, the authors of this report are confident that a statutory or regulatory approach can be negotiated that is to the benefit of every stakeholder category to some extent. This section neither will recommend a specific combination of rules nor will hypothesize as to which combination would lead to the greatest savings for consumers, generate the most profits for EESPs, or be the least burdensome for utilities. Rather, we believe that each state's determinations are shaped by the structure of the utility sector in the state, the opportunities for energy-efficiency savings in the state, and the norms and values of citizens of the state and therefore are best left to those participating in the legislative or rulemaking process in the state to assess and to debate.

---

39. For discussions of these policy issues, see Center for Law, Energy, and the Environment & The Emmett Institute, *Knowledge is Power*, BERKELEY LAW AND UCLA SCHOOL OF LAW (Jan. 2015), http://law.ucla.edu/~/media/Files/UCLA/Law/Pages/Publications/CENN_EMM_PUBknowledge-is-power.ashx; Anne McKibbin, Unleashing the Power of Big Data on Efficiency? Not So Fast, ELEVATE ENERGY (2014), http://www.elevateenergy.org/wp/wp-content/uploads/Big_Data_on_Efficiency.pdf. What distinguishes this report is its focus on model language that policymakers can use as a basis for legislation or rules for their own states.

Finally, while the body of this report focuses on and promotes a non-consent based data-disclosure program, an appendix reviews consent-based contractual opportunities for improving access to data so that policymakers are aware of all of the available policy options.

I. The Problem of Insufficient Access to Energy Data

Currently, EESPs do not have access to enough data to analyze comprehensively the effectiveness of various energy-efficiency practices. While EESPs can and do seek consent from each consumer to acquire his or her usage information, doing so is cumbersome and requires significant expenditures; overall, such an approach leads to incomplete and therefore potentially biased data sets. Customers and EESPs have not benefited as much as they could have from consent-based energy data programs due to cumbersome and unnecessarily complex procedures for granting access.[40] A more effective approach would recognize that utility companies already possess comprehensive energy usage datasets and ensure that, within carefully circumscribed limits, EESPs can directly access this data.

Those who seek to increase cost-effective access to consumer energy data need to address at least five sets of concerns. First, utilities may be extremely reluctant to provide their customers' energy use data due to concerns about liability for improper disclosures and potential privacy violations. Second, utilities may be concerned about negative impacts on their reputation should information be shared more widely than intended, regardless of whether the utility faces legal liability. Third, some consumers may have concerns about utilities giving their individual energy-use data to EESPs because the data may reveal information that consumers would rather keep private. Fourth, utilities may be concerned about the administrative costs associated with processing and transferring the data. Fifth, utilities may be concerned about losing the exclusive opportunity to profit from this data.

In this part of the report, we review these concerns in more detail. To address them, we offer policy approaches in Section II and model language for laws and regulations in Section III.

---

40. *See, e.g.,* Murray & Hawley, *supra* note 26, at 18 ("For example, the consent process at Smart Meter Texas by which a customer grants access to a third party has been criticized by market participants as clumsy and an unnecessary friction point, leading to disappointing customer usage statistics as shown in a recent report.").

A. Legal Liability Concerns

Utilities may be concerned about releasing consumer energy-use data to EESPs because of potential liability. By liability, we mean the legal responsibility for the damaging effects that result from energy-use data disclosures.

Because most states have not yet promulgated liability rules regarding energy-use data, utilities in these jurisdictions are left guessing as to the appropriate amount of data to release and how to release it.[41] Therefore, the safest course of action from the utilities' perspective is not to release data to third parties at all.[42] Until those states promulgate a procedure for releasing energy-use data to third parties, or an industry standard to which they can adhere surfaces, it is unlikely that utilities will release data to any third parties, no matter the potential energy-efficiency benefits that may be gained from such a disclosure.[43]

Even in states where liability rules are clear, utilities may still have some concerns about their potential liabilities. First, liability for disclosing information that may violate consumer privacy interests may rests solely or primarily on the utilities. In such a case, utilities are likely to avoid disclosing data unless there is a clear legal duty for them to do so and a specified mechanism for disclosure. Second, liability rules may not be fully specified. For example, because Colorado's statutory regime does not explicitly shield utilities from liability for actions taken by third parties after the utilities have provided the data to them, utilities may fear that consumers will take action against the utilities for third-party misuse of the data.[44] If utilities are not protected against liability for the disclosure of private customer information in cases in which the utility took all reasonable steps to guard against improper disclosures and theft, it is likely the utilities will try to avoid disclosing any data.

---

41. As discussed above, only eight states have adopted at least limited laws and regulations governing third-party access to customer energy data. *See A Regulator's Privacy Guide*, *supra* note 30, at vii.

42. Furthermore, without a statutory regime dictating what behavior is liability-worthy, consumers have no guidance as to what appropriate utility conduct looks like. Therefore, until a liability regime is established, any data release may also have negative reputational effects, as releasing any data at all may appear reckless or like a breach of the consumers' trust. See discussion in Section I.B. *infra*.

43. Utilities may release some data to those energy-efficiency service providers who assist the utilities in implementing state energy-efficiency requirements. We understand, however, that more third-party EESPs would be able to provide more energy-efficiency savings if the utilities provided them with access to more data.

44. Although current legislation governing the release of customer data to third parties provides precautions that must be taken by the utilities before disclosure, the liability protection afforded to utilities after this stage is complete is unclear. *See generally* COLO. CODE REGS. § 723-3026-3031 (2016).

B. Reputational Concerns

In addition to concerns about legal liability and the financial consequences, utilities may be concerned about potential negative ramifications of a data breach on their reputations. This is regardless of whether the utility has legal liability for the misappropriation or misuse of consumer data.

A negative reputation could have several tangible effects on a utility. In competitive markets, consumers may turn to other suppliers. In non-competitive markets, regulators may look less favorably upon requests from the utility to increase its rates. Regulators and legislators in either kind of jurisdiction may scrutinize more closely the utility's operations and attempt to exert more control over the utility. The public may be less forgiving of the utility when it makes other missteps, such as not responding quickly to power outages. Utility management may need to spend time and money addressing the concerns of the public and public officials—valuable resources which might have otherwise gone to improving operations at the company.

C. Consumer Privacy Concerns

Although the authors of this report are unaware of any harms that have occurred from the disclosure of residential energy-use data, data breaches have happened in other industries,[45] and consumers may have concerns about similar releases of their energy data. Inappropriate access to energy-use data could lead to disclosures about activities inside a home, which could enable some to intrude upon consumers, their residences, and their expectations of privacy.

---

45. In recent years, there have been a series of inadvertent disclosures of non-energy consumer data. *See, e.g., Illinois Department of Insurance Reports 'Inadvertent Data Release'*, INS. J. (Nov. 15, 2015) http://www.insurancejournal.com/news/midwest/2015/11/15/388996.htm (stating that the Illinois Department of Insurance inadvertently released health care providers' social security numbers.); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 41-42 (2011) (documenting a series of damaging health data related "data spills"). Additionally, there have been multiple successful hacking attempts that revealed sensitive personal information. *See, e.g.,* Jane McCallion, *Hard Rock Hotel Loses Customer Data in Seven-Month Hack*, IT PRO (May 5, 2015) http://www.itpro.co.uk/hacking/24543/hard-rock-hotel-loses-customer-data-in-seven-month-hack (stating that the Hard Rock Hotel was hacked and consumer credit card information was accessed). Finally, employee malfeasance has resulted in the recent release of private consumer information. *See, e.g.,* Brian Fung, *AT&T Will Pay $25 Million After Call-Center Workers Sold Customer Data*, WASH. POST (Apr. 8, 2015) http://www.washingtonpost.com/blogs/the-switch/wp/2015/04/08/att-will-pay-25-million-after-call-center-workers-sold-customer-data/?hpid=z3 (noting that as a result of such employee actions, AT&T recently made a large payout to customers after call-center workers sold private customer data.).

First, access to energy-use data could assist a malfeasor in committing a harmful act. For example, by observing a pattern of relatively low energy use in a household, a person with ill intent may be able to predict when a home is vacant and therefore the best time to break into the home.[46] Generally speaking, the shorter the time range for the data (e.g., minute-by-minute vs. day-by-day vs. week-by-week), the more recent the data (e.g., real-time vs. one day prior vs. one month prior), and the more granular the data (e.g., one home vs. block-level vs. neighborhood-level), the more useful the data would be to malfeasors.

Second, businesses may be able to make socially undesirable decisions based on the information gathered. Some might exploit this data to discriminate. As a hypothetical example, if working late hours were strongly correlated with increased medical costs, then a health insurance company would likely be interested in the hours a potentially insured party is generally awake. They may then make judgments about the kind or cost of medical coverage based off the energy data that reveals when the person is awake or asleep. Other insurers could make similar evaluations, based on the assumptions of this hypothetical.

Third, some may use this information to engage in irritating business activities. For instance, some businesses may engage in targeted advertising campaigns. If entertainment companies were able to determine which consumers spend the most time watching television based off their energy-use data, these consumers could get flooded with unwanted advertisements to switch to a different television service provider.[47]

Fourth, broad access to this data may threaten dignity interests. Consumers may not want others to know what activities they conduct within the privacy of the home, and so, to the extent that their energy-use data is capable of being used to identify those activities, it may present a challenge to this privacy interest. One can imagine a "nosy" neighbor, an

---

46. Some consumers may worry that law enforcement could use this information against them. By observing which consumers have abnormally-high energy usage—due to growing marijuana under artificial lights, for example—law enforcement could predict which consumers are engaging in illicit activities in their homes and target them for searches. However, this possibility raises a host of complex constitutional issues that have not been directly addressed by the courts. Such issues are outside the scope of this report.

47. In fact, security researchers have already figured out how to determine how many personal computers and televisions are in a home and even what type of media is being consumed within the home by hacking smart meters. *See* Open Technology Institute, *Data and Discrimination*, NEW AMERICA (Oct. 2014) at 39, https://www.newamerica.org/downloads/OTI-Data-an-Discrimination-FINAL-small.pdf (citing to Stephen Brinkhaus et al., Smart Hacking for Privacy, Presentation to the 28th Chaos Communication Congress (2011), https://events.ccc.de/congress/2011/Fahrplan/events/4754.en.html (last visited June 20, 2016)). Therefore, it is possible that a hacker can determine what types of activities are going on inside the home with access to data from a single smart meter—confirming the value of a consumer's smart-meter data. Employing the aggregation and anonymization techniques described in Section II.A. *infra* will help to reduce the risk of these potential harms.

acquaintance, a friend, or a family member seeking out energy-use information if available.[48] It has been suggested that some detailed forms of this data may allow others to determine what types of devices are being used (e.g., medical devices) as well as the occupants' movements throughout the home,[49] giving others insight into the details of the occupants' private lives. Although this may seem fairly innocuous to some, others would likely have a problem with a broad range of people having access to information about how they act within their homes.

D. Implementation Concerns

Deploying technology for securely and efficiently transmitting data to EESPs will require time and money. Setting up a system for transferring information requires implementing tools for sorting through, processing, and sharing the data with third parties. Utility administrators and information technology experts will need to inform the process as the transfer mechanism is created. New staff may need to be hired to administer the process once it is implemented.

Additionally, information technology staff may face difficulties determining whether requests for data are permissible. Legal and compliance employees may need to review these applications. Staff may need to work with applicants to frame their requests appropriately. These increased demands may lead to the need to hire new compliance staff.

Finally, data release and transfer rules and standards are unlikely to remain static. Utilities will need to spend money on updating their procedures, policies, and even possibly their technologies when changes occur.

The utilities may be concerned that they will be required to bear these costs without a means of recovering them from others. In theory, in regulated jurisdictions, utilities could build these costs into their rates. However, any such change in rates would need to be approved by the public utilities commission, and the utilities may be worried that the

48. For example, it would become increasingly risky to excuse oneself from an event because of "prior commitments" if one's friends and family could use the information provided by one's smart meter to determine that one spent the night at home. As another example, one person could use this information to determine the travel patterns of another. While one can think of cases in which this would be beneficial—a friend confirming that another friend got home safely—in other cases it could intrude upon the traveler's privacy.

49. *See* Frederico Guerrini, *Smart Meters: Between Economic Benefits and Privacy Concerns*, FORBES (June 1, 2014), http://www.forbes.com/sites/federicoguerrini/2014/06/01/smart-meters-friends-or-foes-between-economic-benefits-and-privacy-concerns/ (suggesting that information about energy use can potentially reveal what devices we are using).

regulators would not approve them. In deregulated jurisdictions, the utilities still may want or need legislative or regulatory approval for charging EESPs or consumers more generally. Utilities are unlikely to be inclined to bear these implementation costs without receiving reimbursement or being required to do so.

E. Revenue Concerns

Releasing residential energy data to third parties could negatively utilities' revenues.[50] First, utilities, like most businesses, do not want consumers to purchase less of their product, and EESPs work to reduce demand for energy. Second, utilities may be unwilling to disclose energy-use data to EESPs because of its inherent value. It could be most financially beneficial to the utilities to monetize the data by charging for access to the data or by offering their own services that rely on this data. As a result, the utilities may want to exclude others from the data.

It is generally not in a utility's best interests to sell less electricity. By selling more electricity, a utility can spread its fixed costs over a broader base and lower its average costs. The more electricity a utility sells, the greater the returns to its shareholders, holding all other factors constant.

Additionally, a utility may want to sell its data rather than give the information away. If there is value to the data, then the EESPs should be willing to pay for it, as long as the value to the EESPs is greater than what the utility wants to charge for it. The utility may want to capture some of this value by selling this data.

Finally, a utility can potentially reap rewards from investing in energy efficiency and therefore would benefit from exclusive access to data that identifies good opportunities for energy-efficiency investments. A state may allow a utility to recover for investments in energy efficiency in a manner similar to which it otherwise deploys capital, i.e. a guaranteed rate of return.[51] If the utility can generate appropriate revenues and return from energy-

50. An alternative perspective would start by noting that utilities have requirements to serve the public interest. *See* Peskoe, *supra* note 35, at 212-16 (detailing the history of how electric utility companies were established). Therefore, unlike companies functioning in a fully competitive marketplace, the state can require utilities to take actions that provide societal benefits even though the actions may not directly benefit the utility and may even limit the utility or impose costs on it.

51. *See, e.g.*, MO. REV. STAT. § 393.1075 (2015) ("It shall be the policy of the state to value demand-side investments equal to traditional investments in supply and delivery infrastructure and allow recovery of all reasonable and prudent costs of delivering cost-effective demand-side programs. In support of this policy, the commission shall: (1) Provide timely cost recovery for utilities; (2) Ensure that utility financial incentives are aligned

efficiency investments, then it would not want to enable competitors (i.e. the EESPs) by sharing consumer energy data with them; the utility would want to hold on to the information for its sole benefit.

* * *

The remainder of this document identifies a variety of solutions to concerns about liability, reputation, privacy, implementation and revenues. In doing so, this report proposes various legislative and regulatory options that can help ensure that energy-use data is sufficiently secure before release, is only released to a limited class of people, and provides sufficient anonymity to consumers in order to protect both consumer privacy as well as to make utilities more willing to release the data. This report examines tools that the legislature and the utilities can employ to ensure that utilities are not subject to liability for data breaches that do not result from their misconduct. This document discusses how implementation costs can be borne and recovered. Ultimately, the authors of this report believe that the release of this data to appropriate parties with appropriate safeguards will lead to more cost-effective investment in energy efficiency, less greenhouse gas emissions, and a reduced rate of global warming than if utilities held on to this information for their exclusive use (or non-use).

with helping customers use energy more efficiently and in a manner that sustains or enhances utility customers' incentives to use energy more efficiently; and (3) Provide timely earnings opportunities associated with cost-effective measurable and verifiable efficiency savings.").

II. A Slate of Solutions

Although many industries have developed sophisticated data-disclosure rules, many states are just beginning to regulate energy-use-data disclosures. Presently, utilities will generally not disclose data to third parties in part because many jurisdictions do not have clear-cut rules that control disclosures, and, as a result, the utilities are unsure what they are permitted to share and what happens if disclosure goes awry. However, by regulating what data utilities can disclose to third parties, and the manner in which they can do so, it is possible to provide legal clarity, protect consumer privacy, and give EESPs access to crucial residential energy-consumption data that will lead to substantial energy-efficiency benefits.[52]

Because states are just beginning to regulate energy-efficiency data disclosure, most have a great deal of discretion as to the policy stance they take in picking what open data rules to adopt as well as the methods they will employ to implement the new rules.[53] In order to make utilities comfortable disclosing data to EESPs, most new state laws and regulations will likely address both the privacy measures that will need to be taken before data is released and the liability for data disclosures. Therefore, this report aims to provide possible solutions to these concerns in turn.

---

52. Rules relating to data ownership vary depending on the state, and in many states, there are no rules relating to data ownership in the context of energy usage. However, many states and regulators have been able to regulate consumer privacy rights in the realm of data disclosure without resolving the ownership issue, i.e. do utilities, consumers or both "own" the data? Ultimately, a discussion over ownership rights invokes areas of property law and intellectual property that are outside the scope of this report. *See* U.S. Dep't of Energy, *Data Access and Privacy Issues Related to Smart Grid Technologies*, SEPA AND ADS (Oct. 5, 2010) at 26, http://www.demandresponsesmartgrid.org/Resources/Documents/Reports-Govt-NFP/DOE_SG_Data_%20Privacy_OCT%2010.pdf.

53. Currently, there is a consensus among states that have passed laws relating to energy-use disclosures that at minimum consumers should have access to their own data if they ask for it. *See A Regulator's Privacy Guide, supra* note 30, at viii; *see also* Murray & Hawley, *supra* note 26, at 4 (stating "Consumers—who ultimately pay for advanced meter functionality through rates—ought to be able to see detailed information about how much energy they purchase.").

A. Aggregation and Anonymization

The most valuable data is unaltered, granular information about individual energy consumption. Granular data provides EESPs with the most information with which to work, and from it, they can derive the best insights into potential ways to decrease energy usage in any given residence. Any reductions in the granularity of the data reduces the usefulness of the information.

However, sharing of highly granular data also contains the largest privacy risks. Aggregation and anonymization are approaches for reducing the granularity of the data—and thereby reducing threats to privacy—while still providing useful information to EESPs.

1. Definitions

In the energy-use context, anonymizing means removing or modifying personally identifiable information. One method of anonymization requires completely deleting all personally identifiable information—such as names, addresses, and account numbers—from the data transferred in an attempt to eliminate the possibility of identifying an unique customer.[54] Another method involves "generalizing" personally identifiable information.[55] This method requires that the party responsible for anonymization alter—rather than delete—identifying information.[56] For example, the consumer's date of birth could be generalized to a year or a five-digit ZIP code could be generalized to a three-digit ZIP code, with the last two digits obscured. Certain pieces of information, such as consumer names, would therefore still need to be removed from the data in order to make it anonymous.

Aggregation means combining energy use data across groups of people or across time. Aggregating across groups could occur at the block, neighborhood, or even town level. Aggregating across time could combine statistics for a single person (or multiple individuals) across sections of time, such as over a month, week, or day.

---

54. A Colorado administrative decision described anonymized data as having "all potential customer identifying information removed." Pub. Utils. Comm'n of the State of Colorado, *In the Matter of the Proposed Rules Regulating the Data Access and Privacy for Electric Utilities, Colo. Code Regs. § 723-3 and Data Access and Privacy Rules for Gas Utilities, Colo. Code Regs. § 723-4*, Decision No. R15-0406, Proceeding No. 1R-0394EG, 13 & n. 20, 5 (May 1, 2015), https://www.sos.state.co.us/CCR/Upload/AGORequest/BasisandPurposeAttachment2014-00436.pdf [hereinafter *Colorado PUC Energy Data Decision*].

55. With medical data, for example, removing information about next of kin would be essential to anonymization. For student records, student identification numbers would need to be removed. Paul Ohm, *Broken Promises of Privacy*, 57 UCLA L. REV. 1701, 1703 (2010).

56. *Id.*

2. Benefits

a. Improving privacy

Anonymizing data helps to protect privacy. If all identifying information is removed, then the individual cannot be identified. If identifying information is generalized, then it can be difficult or impossible to identify the individual.[57]

Aggregating information across multiple individuals can address privacy concerns as well. For example, if energy-consumption data associated with 100 homes in a particular area is aggregated, one could still review the average energy consumption per home in that area without seeing the energy consumption for any particular household.

Aggregating information across time reveals fewer details about a consumer's habits at any particular point in time. For example, one method of aggregation would be to combine data from the similar slices of time on a weekly basis. This would require the utility to average the energy consumed in a household over, for instance, two-hour intervals (e.g., 12 a.m.-2 a.m., 2 a.m.-4 a.m., 4 a.m.-6 a.m., and so on) and then to aggregate those two-hour slices across the entire week, which provides protection against third parties seeing the consumers' moment-by-moment use of energy. The resulting data set would then show the weekly average amount of energy used during each two-hour-slice. Third parties might be able to see where to target energy-efficiency measures that relate to time-of-day use, without needing to receive more detail than necessary about the consumer's activities at any given time of the week.

b. Providing energy usage insights

The exact usefulness of the data to third parties such as EESPs depends on the level of aggregation and anonymization. The smaller the grouping, the more useful the data will be to third parties; for example, they will more easily be able to identify outliers which require further investigation or to see the impact from the implementation of a product or process in a particular home or set of homes.

Low levels of anonymization or aggregation provide EESPs with data that tracks closely to the decisions faced by individual customers and their individual opportunities for savings. With individual data points, EESPs can use actuarial analysis to create detailed savings and usage models. They can also target problems on an extremely granular level, such as potentially analyzing individual household appliances or energy usage practices. This

57. *See* Section II.A.3. *infra* regarding re-identification risks.

information could then be used to assist residents in the selection of a rate plan that is best suited for them or to inform potential homebuyers of the energy-efficiency history of a given home, among other possibilities.[58]

Midlevel aggregation and anonymization, such as the aggregation of between 10 and 20 homes with their individual addresses removed but ZIP codes retained, will provide EESPs with data that can also be used for modeling. General street-wide or neighborhood-wide practices can still be analyzed even though the ability to target individual usage practices within a single home becomes significantly more difficult.

At high levels of aggregation and anonymization—such as at the ZIP code level— EESPs can use the data for more general modeling purposes. Some of these more general modeling purposes could include analyzing time-of-use demand and energy-efficiency programs implemented within a ZIP code. As a result, EESPs could use this data to identify the best avenues to pursue for reducing costs within a general area and design educational programs that ensure that energy consumers are aware of the best ways to increase energy efficiency.[59]

3. Costs and risks

The extent to which data is anonymized and aggregated affects the costs. The more the information is anonymized and aggregated, the more time and effort will be required to determine how to treat the data to protect privacy while allowing for the greatest insights and value to be derived; there will also be more computational time and costs to modify the data. However, the more the data is aggregated, the smaller the resulting data set may be, which should reduce data storage and transfer costs.

In addition, there is a risk of data reidentification. A malfeasor may be able to reverse engineer poorly-conducted anonymization and therefore identify what data belongs to which individual consumers, effectively removing privacy protection.[60]

The risk of data reidentification arises due to poorly designed anonymization and to poorly executed anonymization. Improperly designed anonymization occurs when an anonymization technique underestimates the amount of identifying data that needs to be deleted or generalized to protect privacy interests because parties who have access to the

58. Murray & Hawley, *supra* note 26, at 9.

59. *See id.*

60. *See generally* Ohm, *supra* note 55 (discussing the concept of reidentification).

data can still identify its subjects.[61] Improperly executed anonymization occurs when mistakes are made during the anonymization process and non-anonymized data is inadvertently released.

Although releasing non-anonymized data poses serious privacy concerns, sophisticated parties that anonymize data routinely seem less likely to make anonymization design or execution mistakes.[62] Overall, when an anonymization system is thoughtfully designed, and no mistakes are made in its implementation, anonymization will likely go a long way towards safeguarding personal information.

4. Policy options

Some states have already adopted rules.[63] For example, Colorado has enacted a 15/15 rule requiring aggregation of at least 15 customers, with no one customer's data comprising more than 15% of the data in the aggregated group's total.[64] During the Colorado rulemaking, cities in Colorado—including Denver—petitioned for a far less aggregated requirement such as a 4/80 rule.[65] The Commission ruled, however, that the more stringent 15/15 rule was necessary to protect consumer privacy. At whatever level of aggregation, setting in place specific ratios provides the benefit of clarity and easy of administration.

Another approach to aggregation is to create a standard rather than a rule. 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."[66] Such a standard provides more flexibility

---

61. An example of this was demonstrated when AOL released a large amount of search queries (after deleting any obviously identifying information), and bloggers were still able to determine who had conducted some of the searches. *Id.* at 1717.

62. However, even sophisticated parties like AOL (along with Netflix and the State of Massachusetts) have made serious anonymization miscalculations. *Id.*

63. It is important to note that even with aggregation, the third parties to whom the data is released must meet a variety of security requirements, or the customer must give the utility permission to release the data. *See A Regulator's Privacy Guide, supra* note 30, at viii.

64. COLO. CODE REGS. § 723-3031 (2016).

65. *See Colorado PUC Energy Data Decision*, *supra* note 54, at 13 & n.20. *See also* Vt. Pub. Serv. Bd., *Investigation into Petition Filed by Vermont Department of Public Service Re: Energy Efficiency Utility Structure,* Docket No. 7466 (2010), http://psb.vermont.gov/docketsandprojects/eeu/7466 (reviewing an approach that allows for disclosure of aggregated data at the level of a municipality (e.g., town, city)).

66. OKLA. STAT. tit.17 § 710.7(B)(2) (2016).

and fact-specific customization than the Colorado approach; however, utilities may be wary of the potential liabilities arising out of such a vague standard.

In reviewing these options, policymakers should consider the advantages and disadvantages along the dimensions of clarity, ease and cost of administration, flexibility in application, liability allocation, and protectiveness of privacy. For example, legislators and regulators must balance the risks to consumer privacy against the benefits of increased data disclosure. The greater the extent of anonymization and aggregation, the greater the privacy protections. However, it also means that EESPs will derive fewer energy-efficiency insights. Ultimately policymakers must strike the balance based on their views of the optimal tradeoff between the various positions on these different dimensions.

Policymakers should remember aggregation and anonymization techniques are simply one kind of tool in the toolkit that regulators have to protect privacy.[67] As discussed in the following sections, implementing liability rules, data-transfer and security rules, identity-based rules, and insurance coverage rules also have benefits. Furthermore, while anonymization and aggregation alone may be insufficient to keep sophisticated parties from reengineering data sets, aggregation and anonymization can do significant work in by making it more difficult for the average person to commit privacy breaches.

B. Procedures Controlling the Transfer, Receipt, and Safekeeping of Aggregated Energy Data

Policymakers will have to consider how to ensure that utilities transfer aggregated energy data to eligible EESPs securely and that EESPs protect the aggregated data adequately. While state privacy and data-security laws may already regulate the safekeeping of data by anyone, including utilities,[68] legislators could pass a law or regulators could promulgate a rule requiring that utilities and data recipients implement security measures for the type of aggregated energy-data contemplated by this report. This law or rulemaking could be a standard, a rule, or a hybrid of both.

---

67. *See generally Data Privacy and the Smart Grid: A Voluntary Code of Conduct,* U.S. DEP'T OF ENERGY (Jan 8, 2015), https://www.smartgrid.gov/files/DataGuard_VCC_Concepts_and_Principles_2015_01_08_FINAL.pdf [hereinafter *Data Privacy and the Smart Grid*].

68. *See, e.g.,* CAL. PUB. UTIL. CODE § 8380(d) (West 2010) ("An electrical corporation or gas corporation shall use reasonable security procedures and practices to protect a customer's unencrypted electrical or gas consumption data from unauthorized access, destruction, use, modification, or disclosure."); NEV. REV. STAT. § 603A.210 (2005) ("A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.").

1. Standards- and rules-based approaches to energy-data security

Instituting adequate requirements for data-security procedures requires an appreciation for the "rules-standards spectrum." On the standards end of the spectrum, there is the option of mandating that utilities and EESPs implement "reasonable" security measures without detailing what procedures would be "reasonable." For example, section 8380(d) of California Public Utilities Code requires:

> *An electrical corporation or gas corporation shall use* reasonable security procedures and practices *to protect a customer's unencrypted electrical or gas consumption data from unauthorized access, destruction, use, modification, or disclosure.*[69]

This law contains minimal specific content, as is characteristic of a standard.

On the rules end of the spectrum, there is the option of mandating specific and highly technical requirements. For example, the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce that sets computer security standards for the federal government, has issued guidance on smart-grid cybersecurity.[70] Among other recommendations, the NIST guidance suggests that recipients of smart-grid data appoint specific individuals to manage data security, implement information-tracking programs, share best practices with other third parties, train and monitor employees on data handling, and conduct audits of such procedures:

> Security personnel: *"Third Parties should appoint positions and/or personnel to ensure that security and privacy policies are properly maintained, updated, and followed."*[71]
>
> Information tracking: *"In developing and updating policies and practices, Third Parties should develop a set of Privacy Use Cases as a method to track information flows and the privacy implications of collecting and using data to help the organization to address and mitigate the associated privacy risks within common technical design practices and business practices."*[72]

---

69. ID. (emphasis added).

70. *See* The Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee, *Guidelines for Smart Grid Cybersecurity: Volume 1- Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements,* NAT'L INST. OF STAND. AND TECH. (Sept. 2014), http://dx.doi.org/10.6028/NIST.IR.7628r1.

71. The Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee, *Guidelines for Smart Grid Cybersecurity: Volume 2 – Privacy and the Smart Grid,* NAT'L INST. OF STAND. AND TECH. (Sept. 2014), http://dx.doi.org/10.6028/NIST.IR.7628r1 [hereinafter *NIST Guidelines Volume 2*] at 73, D-3.7.

72. *Id.* at 73, D-3.8.

> Best-practice sharing: *"Third Parties should share solutions to common privacy-related problems with other smart grid market participants in some appropriate manner (e.g., trade forums, associations, public policy, public outreach, external coordination, etc.)."*[73]
>
> Employee training: *"The organization should document, maintain, and monitor each employee's security and privacy training activities on an individual basis, including basic security and privacy awareness training in accordance with the organization's security and privacy policies."*[74]
>
> Audits: *"Each third party should conduct a periodic independent audit of third party's data privacy and security practices."*[75]

Compared to section 8380(d) of the California code, these NIST procedures are more specific and give limited discretion to the regulated entity.[76]

2. Hybrid approaches to energy-data security

Rules and standards can be combined. For example, California law also mandates that a utility and a third-party data recipient execute a non-disclosure agreement (NDA) with certain recommended terms.[77] The model NDA stipulates the following:

> *Security Measures shall mean reasonable administrative, technical, and physical safeguards to protect Data from unauthorized access, destruction, use, modification or disclosure, including but not limited to:*
>
> a. *written policies regarding information security, disaster recovery, third-party assurance auditing, penetration testing;*
> b. *password protected workstations at Recipient's premises, any premises where Work or services are being performed, and any premises of any person who has access to such Data;*
> c. *encryption of the Data;*
> d. *measures to safeguard against the unauthorized access, destruction, use, alteration or disclosure of any such Data including, but not limited to, restriction of physical access*

73. *Id.*

74. *Id.* at 74, D-3.11.

75. *Id.* at 74, D-3.12.

76. For example, the entity can determine a set of Privacy Use Cases. *See id.* at 73, D-3.8

77. *See* discussion *infra* Section II.C.5.

> *to such data and information, implementation of logical access controls, sanitization or destruction of media, including hard drives, and establishment of an information security program that at all times is in compliance with reasonable security requirements as agreed to between Recipient and Utility.*[78]

This provision of the model NDA constitutes a hybrid between a rule and a standard because it specifies requirements that recipient must follow regarding encryption and password protection; however, it still leaves the development of some of the "reasonably" protective policies and procedures up to the third party and the utility.

The Department of Energy (DOE) appears to support a rule-standard hybrid approach as well. In January 2015, the DOE published a Voluntary Code of Conduct related to the privacy of customer energy-usage data for utilities and third parties.[79] The report calls on utilities and third parties to adopt a cybersecurity risk-management system that has the following characteristics:

a. *Identifies, analyzes, and mitigates cybersecurity risk to the Service Provider's organization with respect to Customer Data.*

b. *Implements and maintains process, technology, and training measures to preserve data integrity and reasonably protect against loss and unauthorized use, access, or dissemination.*

c. *Maintains a comprehensive data breach response program for the identification, mitigation and resolution of any incident that causes or results in the breach of Customer Data security.*

d. *Provides complete, accurate, and timely notice to customers whose Customer Data may have been compromised while within the Service Provider's control or within the control of Service Provider's Contracted Agent, and remedies the conditions that led to the breach.*

e. *In the event that a Service Provider has modified or enhanced data that it initially received from another source (e.g., a utility or a different third party), the customer*

---

78. Pub. Utils. Comm'n of the State of Cal., *Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data While Protecting Privacy of Personal Data,* Decision 14-05-016, Attachment B: Model Non-Disclosure Agreement, at 2-3 (May 1, 2014), http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M090/K845/90845985.PDF [hereinafter *California PUC Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data*].

79. *See Data Privacy and the Smart Grid*, *supra* note 67.

> *receiving the enhanced or modified data should generally be made aware that such data may differ from the original data.*[80]

Given the use of terms like "reasonable" and "comprehensive," the DOE has given some discretion to adoptees in terms of implementation but provided more content regarding what specific procedures parties must develop than a typical standard would.[81]

3. Policy options

In light of the prior discussion of different types of data-security requirements, this section delineates three general options for legislators and regulators, as well as the benefits and drawbacks of these options.

First, the law or rule could require each of the regulated entities to develop, document, and update specific procedures to meet a reasonableness standard like the one mandated by section 8380(d) of California law. On the one hand, this option allows policymakers to avoid the burden of defining what procedures are reasonable, which may make it easier to build consensus and to pass the law or to promulgate the rule. On the other hand, leaving this determination up to individual companies may result in company-friendly procedures that make consumer groups uneasy. Moreover, these procedures may vary from firm to firm and may go unpublished unless a law or rule requires publication of such procedures online or in a

---

80. *Id.* at 11 (emphasis added).

81. Outside of the energy-data realm, government agencies have taken a similar hybrid approach to data security. For example, the Department of Health and Human Services (HHS) promulgated rules to execute the data-security program for the Health Insurance Portability and Accountability Act (HIPPA). *See Security Rule Guidance Material*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html (last visited Apr. 18, 2016). HHS guidance on the rules divide the procedures explicitly into administrative, physical, and technical categories, each of which give regulated parties a limited degree of implementation discretion. *See* 45 C.F.R. § 164.308(a)(1) (2013) ("Implement policies and procedures to prevent, detect, contain and correct security violations."); 45 C.F.R. § 164.310(a)(1) (2013) ("Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."); 45 C.F.R. § 164.312(c)(1) ("Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."). To help entities comply with these rules, HHS issued guidance documents for each category in which HHS provides sample questions for the regulated entity to consider. *See, e.g., Security Standards: Administrative Safeguards*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Mar. 2007), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf; *Security Standards: Physical Safeguards*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Mar. 2007), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf; *Security Standards: Technical Safeguards*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Mar. 2007), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf.

state registry. Some consumer groups may perceive this lack of transparency as threatening accountability of the utilities.[82] A standard may make the utilities and recipients themselves uneasy; both groups may want more specific guidance on what constitutes reasonable security measures to help shield them from liability.

Second, regulators could promulgate rules obligating utilities and recipients to implement specific security measures. Because rulemaking gives stakeholders the opportunity to participate in the formulation of the rule through the commenting process, regulators can learn and take into account the interests of multiple stakeholders. At the same time, this approach will require policymakers to become experts on data-transfer procedures, which may delay the rulemaking process. There is also a concern that industry may capture regulators, leading them to adopt policies that fit the industry's desires. Furthermore, real-world practices can change more frequently or quickly than regulations can be updated. However, these concerns may be overstated given that NIST, DOE, and HHS have all released relevant data-security related guidance documents that policymakers could review so that they would not have to reinvent the wheel.[83] Moreover, as the California model NDA and DOE's Voluntary Code of Conduct demonstrate, even more specific rules can still leave some discretion to the regulated entities, which relieves policymakers of the burden of getting into the minutia and making regular updates.

Third, policymakers could mandate that the utilities and recipients adopt industry standards. For example, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), both independent non-governmental organizations, have developed industry standards, or codes of practice, for security management systems.[84] Firms can even seek ISO compliance certification.[85] This type of option has several virtues. Like the first approach, one would relieve the policymakers of the responsibility of becoming experts of data-transfer protocols. Unlike the first option, this approach would lead to greater uniformity in the procedures the utilities and recipients employ. Also, by requiring the adoption of the "latest" industry standard, for example, the rule would build in a mechanism for updating the technologies the utility and recipient employ without requiring regulators to undergo time-consuming rulemaking. Additionally, the

82. Such an issue could be solved through auditing or disclosure requirements.

83. *See, e.g., NIST Guidelines Volume 2*, *supra* note 71; *Data Privacy and the Smart Grid*; *supra* note 67; *Security Rule Guidance Material*, *supra* note 81.

84. *ISO/IEC 27001:2013(en), Information technology—Security techniques—Information security management systems—Requirements,* INT'L ORG. FOR STAND. (2013), https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

85. *ISO/IEC 27001- Information security management*, INT'L ORG. FOR STAND., http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (last visited Dec. 16, 2015).

possibility of certification may reassure consumers and other stakeholders that the utility and data recipients are following adequate security measures. At the same time, the desirability of this option, though, depends on how much various stakeholders respect and trust the industry standards.

There are benefits and drawbacks to each of these approaches. Different factors will likely make certain options more or less desirable in different states, and therefore this report does not argue that one approach is always superior to the others.

C. Liability Rules and Liability Shifting Mechanisms

Utilities fear being held liable for harms arising from releasing energy-use data, even when the data is aggregated and anonymized and is given to authorized EESPs. Third parties may be concerned that they will be held liable for the actions of others. Privacy rights advocates are concerned that consumers whose privacy is compromised or who suffer other harms may not have sufficient redress.

Policymakers can address these concerns by adopting rules to allocate liabilities among the utility, data recipients, and other actors. In developing these rules, lawmakers will want to consider when enforcement rights for data breaches lie with the government, with consumers, with individuals, or with all of the above.[86] The options discussed in this section are not necessarily mutually exclusive, and many can be used in combination with one another.

1. Liability shield

One way to address the concerns of utilities is to absolve them of liability for any harms that result from data disclosures. Given that consumer and privacy advocates would likely have significant concerns about a blanket release from liability for utilities, a more realistic provision would protect a utility from liability if it follows procedures such as those described above with regard to anonymization and aggregation and data security.

For example, the Colorado Code absolves the utility of liability if the utility follows the disclosure rules:

86. Although enforcement rights can be either criminal or civil in nature, this report focuses primarily on civil liability mechanisms.

> *A utility and each of its directors, officers and employees that discloses aggregated data as provided in these data privacy rules shall not be liable or responsible for any claims for loss or damages resulting from the utility's disclosure of aggregated data.*[87]

The Colorado rule disclaims liability for utilities and their personnel who follow the state's data privacy rules.

Such provisions create additional incentives for the utilities to implement the mandated policy and procedures. Consumer and privacy advocates may be willing to accept these provisions if the required policies and procedures offer sufficient protections.

2. Administrative fines

State legislatures and public utilities commissions could mandate that utilities or EESPs which disclose data to unauthorized persons pay an administrative fine. In Colorado, for example, the Public Utilities Commission has the right to impose civil penalties up to $2,000 for unauthorized disclosure of aggregated data.[88] As discussed in the aggregation and anonymization section, Colorado follows a 15/15 rule, which means that:

> *At a minimum, a particular aggregation must contain at least fifteen customers; and, within any customer class no single customer's customer data or premise associated with a single customer's customer data may comprise 15 percent or more of the total customer data aggregated per customer class to generate the aggregated data report (the "15/15 Rule").*[89]

If, for instance, a utility were to disclose 14 instead of 15 customers, then the utility could face a civil penalty up to $2,000.

Administrative fines could vary based on the knowledge or willfulness of the disclosing party. Fines could be more severe if the disclosing party was aware that it was disclosing to an unauthorized person, was aware that it did not have sufficient protective procedures in place, or otherwise acted with willfulness or gross negligence. Fines could be lower if the disclosing party did not follow the standard of care that a reasonable person would have followed under the circumstances, i.e. acted negligently.

Administrative penalties have a number of advantages. Calculating the value of a fine is relatively easy in comparison to a damages calculation. One only needs to multiply the

87. COLO. CODE REGS. § 723-3033(f) (2015).

88. § 723-3976.

89. § 723-3033(b).

number of violations by the penalty value associated with that violation; no proof of harm is necessary. Beyond administrative ease, such penalties offer deterrent benefits. For example, "agencies might seek to deter misconduct by using civil penalties to raise the expected cost of regulatory violations above the cost of compliance. Alternatively, agencies might use civil penalties as one step in an escalating series of enforcement responses to recalcitrant behavior by a regulated entity."[90] So even if no individual were actually identified as a result of the prohibited disclosure of aggregated data, the utility or EESP will have an incentive to improve data security in response to the administrative approach.

Administrative penalties have a few disadvantages. Of course, it is necessary for the state public utilities commission to impose these penalties in order for them to have a deterrent effect, and the state must use resources to investigate and to impose penalties on violators, who would also need to have an appropriate mechanism for appealing such as penalty. Furthermore, fixing the amount of the penalty in advance would sever it from the actual harms, making it economically inefficient because it would over penalize (and over deter) or under penalize (and under deter) the conduct.

3. Private rights of action

Policymakers should consider whether to give private rights of action against utilities or EESPs for non-compliant data disclosures, to withhold such a right, or to remain silent on the issue and let existing laws fill the void. Private rights could be given to consumers only or to all individuals. Private rights of action can be in place of, or in addition to, providing regulators with enforcement tools of their own.

i. Option 1: Creating a private right of action

Providing private rights of action empowers consumers to seek redress for the wrongs they have suffered and can deter utilities and EESPs from disclosing data, but doing so also creates costs and risks. Consumers would no longer be reliant solely on the actions of government officials to investigate and to deter data breaches. However, it would cost the consumer time and money to bring the claim, even if the law allowed for consumers to recover their attorney's fees and costs. It would expose the utility and EESPs to the risks and expense of civil litigation.

In crafting these laws, policymakers would also want to consider whether to tie the amount of damages that consumers could recover to the culpability of the utility, EESP, and

90. Max Minzner, *Why Agencies Punish*, 53 WM. & MARY L. REV., 853, 853 (2012), http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3416&context=wmlr.

their agents. For example, if a utility's actions were merely negligent, then recovery would likely be limited to actual damages and costs. But if the utility's actions were willful, then consumers likely could recover augmented damages.

While the Fair Credit Reporting Act addresses the release of credit information by Credit Reporting Agencies to third parties, rather than the release of energy data, it exemplifies how a statute can provide consumers with a private right of action against the source of a *negligent* data disclosure. Per 15 U.S.C. § 1681o(a):

> *Any person who is negligent in failing to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of: (1) any actual damages sustained by the consumer as a result of the failure; and (2) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.*[91]

This section gives consumers a private right of action against Credit Reporting Agencies for actual damages and legal fees and costs.

The liability of Credit Reporting Agencies for *willfully* failing to comply with the Fair Credit Reporting Act is greater.

> *Any person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of (1)[ ] any actual damages sustained by the consumer as a result of the failure or damages of not less than $100 and not more than $1,000; . . . (2) such amount of punitive damages as the court may allow; and (3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.*[92]

Persons who willfully fail to comply under the Fair Credit Reporting Act are liable for punitive damages on top of the actual damages and legal fees and costs.

In addition to the benefits of allowing consumers to pursue redress for the harms they have suffered, a two-tiered approach like the Fair Credit Reporting Act has appeal. The fact that the harshness of the penalty corresponds with the intentionality of the actor aligns with common-sense notions of "just" punishment. Furthermore, the possibility of incurring punitive damages for willful behavior deters such conduct.

---

91. 15 U.S.C. § 1681o(a) (2016).

92. § 1681n(a).

ii. Option 2: Precluding a private right of action

Conversely, policymakers could preclude consumers from bringing private rights of action against utilities or EESPs for non-compliant disclosures. The Health Insurance Portability and Accountability Act (HIPAA), for example, does not create a private right of action for individuals affected by a health-care privacy breach. If the laws and regulations do not *expressly* give individuals a private right of action, courts would likely deny that that such a private right exists by implication.[93] However, to avoid the expense of resolving this before the courts, if policymakers want to deny consumers a private right of action against utilities or EESPs, they should expressly do so. For example, lawmakers might consider the following language:

> *Nothing in this subchapter creates a cause of action or in any other way increases or diminishes the liability of any person under any other law.*[94]

This language would avoid litigation associated with trying to figure out whether a private right of action was implied; this option is also the least consumer friendly approach.

iii. Option 3: Defaulting to state privacy law or common law tort claims

If policymakers remain silent on whether consumers have a private right of action within the laws and rules establishing an energy-data-disclosure program, consumers may still have legal recourse available to them. Often states have generally-applicable personal-information and breach-of-security laws that give a consumer a cause of action.[95]

Even in the absence of privacy statutes, consumers may still be able to bring a common law tort claims. For example, the Restatement (Second) of Torts defines the tort of "intrusion upon seclusion": "One who intentionally intrudes, physically or otherwise, upon the solitude or

---

93. *See, e.g., Cort v. Ash,* 422 U.S. 66, 78 (1975) (setting forth four factors that are relevant when determining if a statute provides an implied right of action: (1) whether the plaintiff is a member of a class for whose benefit that statute was enacted; (2) whether there is an indication of Congress's intent to create or deny a private remedy; (3) whether a private remedy would be consistent with the statute's underlying purposes; and (4) whether the cause of action traditionally is relegated to state law); Donna L. Goldstein, *Implied Rights of Action Under Federal Statutes: Congressional Intent, Judicial Deference, or Mutual Abdication?*, 50 FORDHAM L. REV. 611, 612 (1982), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4557&context=flr (discussing the strong presumption against implication).

94. 15 U.S.C. § 2649 (1986) (limiting private rights of action under the Asbestos Hazard Emergency Response Act).

95. *See generally Data Breach Charts*, BAKERHOSTETLER, http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf (last visited Dec. 16, 2015) (providing a breakdown of which states do and do not permit a private cause of action).

seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[96] The comment to the Restatement explains that this tort may occur when a defendant investigates or examines the private affairs or another by, for example, opening a person's private and personal mail, searching the person's wallet, or looking into the person's home.[97] In addition, the Restatement defines "publicity given to private life": "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[98] In this scenario, the tortfeastor shares the private information with others. It seems plausible to draw an analogy between the unwanted mail opener or window peeper and an unwanted third party who acquires information about how consumers use energy inside their homes; it also seems possible that such intrusion would be highly offensive to a reasonable person.

Before policymakers decide to remain silent on a private right of action—and thereby default to background laws and principles—they should consider how robust already existing state privacy statutes and common law torts actually are. If these laws do not provide sufficient protections or do not cover clearly the types of harms that result from energy-usage data breaches, then lawmakers should include such protections directly in the energy data laws or should modify the existing privacy statutes.

iv. Additional consideration: Consumers, individuals or both

The previous three options have listed consumers as the persons who would or would not have causes of action. This parallels the Fair Credit Reporting Act approach.

One could easily imagine broadening the range of claimants to all individuals. Limiting the definition of those who can bring a claim to a "consumer" could exclude other persons who live in a household but who are not the account holder, i.e. the person who has the contractual relationship with the utility. It could also limit the claims of person about whom inferences can be drawn from the data but whose information is not contained in the data.[99]

---

96. *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

97. *Id.* at CMT. b.

98. *Id.* § 652D.

99. For example, a dataset might reveal that it is highly unlikely that anyone in a neighborhood is at home at a particular time (e.g. Friday night, Sunday morning). Theoretically, a malefeasor could that information to decide to break into homes in the neighborhood and could happen to select a home to burgle that is not in the dataset.

Broadening the range of persons would increase the liability and the deterrent effect on those who handle data. It would also likely be linked to the harm suffered by these persons, which would ensure that unaffected parties are not suing to vindicate the rights of others. A broader approach would comport with the notion that all who suffer harm are able to seek redress.

4. Penalties for persons seeking to obtain data under false pretenses

Policymakers should consider whether to pass a statute or to promulgate a rule that allows the state to impose civil and criminal penalties on persons trying to obtain aggregated data under false pretenses. Anyone who knowingly or willfully obtains aggregated data under false pretenses could be fined, imprisoned, or both. This law could also establish a civil cause of action for any injured private plaintiffs and for targeted utilities and EESPs[100] to recover damages from parties that fraudulently obtain data.

The Fair Credit Reporting Act illustrates how lawmakers could affix such liability for fraudulent behavior. Per 15 U.S.C. § 1681q:

> *Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under Title 18, imprisoned for not more than 2 years, or both.*[101]

Civil liability accrues to those who willfully obtain information under a false pretense:

> *[I]n the case of liability of a natural person for obtaining a consumer report under false pretenses or knowingly without a permissible purpose, actual damages sustained by the consumer as a result of the failure or $1,000, whichever is greater.*[102]

Another key provision of the Fair Credit Reporting Act dealing with requester liability grants Credit Reporting Agencies a private right of action against fraudulent requesters for damages sustained by the Credit Reporting Agency:

> *Any person who obtains a consumer report from a consumer reporting agency under false pretenses or knowingly without a permissible purpose shall be liable to the*

100. If EESPs transmit data, for example, to third-party contractors in order for third-party contractors to render their services to EESPs, then EESPs may also need protection from fraudulent data-solicitation.

101. 15 U.S.C. § 1681q (2016).

102. § 1681n(a).

consumer reporting agency for actual damages sustained by the consumer reporting agency or $1,000, whichever is greater.[103]

Thus both the government and private individuals and entities can pursue those who fraudulently obtain this data.

State policymakers should penalize fraudulent requesters. Expressly giving consumers, individuals, EESPs, and utilities a private right of action against fraudulent requesters bolsters the legal rights of those who would be affected by such deception. Moreover, civil and criminal penalties would deter actors who might be inclined to abuse the program if less stringent policies were in place.

5. Contractual allocation of liability

Utilities and the EESPs could sign an agreement that addresses who bears the financial costs of a data breach, among other issues. Regulators could require agreements that address these issues and could provide model agreements, similar to what California does.

These agreements could address a number of concerns of the utilities, albeit with an important caveat. The third party could agree not to disclose the data to others. It could agree not to sue the utility, to defend the utility if the utility is sued, and to assume the liabilities of the utility if there is a data breach.[104] Such an arrangement shifts risks and potential costs from a utility to a third party. If the third party were insolvent, however, the utility would still bear the burdens of misuse.

California has required non-disclosure agreements (NDAs) that covers many of these kinds of issues as part of its data-disclosure program. In May 2014, a California Public Utilities Commission decision established a protocol for utilities to follow when providing highly granular customer-usage data to eligible third parties.[105] The decision required the utility and the third parties to execute an NDA and provided a model one as an attachment to the decision.[106]

---

103. § 1681n(b).

104. Unaccompanied by a law or rule precluding private rights of action against the utility, however, reallocating the liability would not preclude a private right of action against the utility should the third party be unable to pay.

105. *See generally California PUC Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data, supra* note 78, at 2. The only eligible parties were the University of California and other nonprofit education institutions using the data "for research purposes," as long as the institutions followed the requirements of the decision. *Id.*

106. *Id.* at Attachment B: Model Non-Disclosure Agreement, 4.

For example, the California model NDA:

- Requires the third party to accept liability for the harm resulting from disclosure of data: "Recipient shall be liable for the actions of any disclosure or use by its Representatives contrary to the Commission Order and this Agreement."[107]
- States that generally neither party is liable to the other for certain kinds of damages: "[N]either Party shall have any liability to the other for any special, indirect, incidental or consequential loss or damage whatsoever, even if such party has been advised in advance that such damages could occur."[108]
- Requires the third party to defend a utility from claims of harms that resulted from the third party's possession or use of the data:

  > *Recipient shall defend and hold harmless Utility and its affiliates, officers, directors, employees, agents, representatives, successors and assigns, from and against any and all losses, causes of action, liabilities, damages and claims, and all related costs and expenses, fines, penalties, or interest, including reasonable outside legal fees and costs, arising out of, in connection with, or relating to Recipient's use, maintenance and/or disclosure of Data.*[109]

In addition, the California NDA requires that the third parties use the data only for the purposes outlined in the NDA, comply with state privacy and information security laws and regulations, return or destroy the data once the agreed upon usage of the data was complete, and abstain from attempting any reidentification of customers using publically available information.[110]

State legislatures and regulators should consider mandating a similar agreement between utilities and third-party recipients that transfers liability from the utility to the third party. It is important to keep in mind that reallocating liability through the agreement would not protect a utility against claims against it, should the EESPs be unable to pay; this is an important consideration for policymakers because EESPs may be thinly capitalized, particularly in the early phases of their development.

---

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id.* at Attachment B: Model Non-Disclosure Agreement, 1-2.

6. Data-breach insurance coverage

Most businesses purchase general liability insurance, which may cover physical damage or loss of property but would not necessarily cover liabilities arising from a data breach.[111] This creates coverage gaps that state policymakers may want to consider closing before initiating an energy-data access program. Requiring EESPs to offer proof that they hold data-breach insurance coverage prior to receiving energy usage data from a utility is one solution.

Smaller, more thinly capitalized companies may go bankrupt before consumers harmed by an illegal disclosure of data can file a lawsuit and redress their injuries. Thus, data-breach insurance coverage may be most warranted where energy-data programs permit small, emerging companies to access highly-granular information. Purchasing coverage simultaneously signals the EESP's seriousness about preventing energy-data security risks and provides compensation to consumers that fall victim to a data breach, should one occur. Insurance, through use of deductibles, exclusions, and experience rating, also gives EESPs strong incentives to reduce risks of a privacy breach; and in doing so, insurance arrangements can alleviate monitoring and enforcement burdens on public utility regulators.[112]

Mandating data-breach insurance coverage does invite some difficulties. Many insurance carriers offer data breach insurance policies, but there are no standardized documents across the industry.[113] Uncertainty about how the policies would work in practice and how courts will interpret policy language without a body of precedent have slowed adoption of data breach insurance.[114] To implement successfully a rule requiring that third-party recipients have data-breach insurance coverage, state policymakers would have to determine: (1) how much insurance coverage third-party recipients are required to purchase for accessing different levels of data; (2) whether insurers are willing to underwrite policies that cover harms to consumers; (3) what the cost of such insurance could be and the financial capacity of the third parties to pay for such insurance; and (4) to what degree data recipients will be dissuaded from requesting data if an insurance coverage requirement is implemented, among other questions that will arise along the way.

In light of these challenging questions, state policymakers should keep the prospect of adopting a data breach insurance mandate in mind but recognize that there are costs.

---

111. *See* Lance Bonner, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 274 (2012).

112. *See* Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197, 199 (2012).

113. *See* Dwayne Shelton, *Cyberliability—an Uninsured Risk*, 50 ARK. LAW. 26, 27 (2015).

114. *See* Bonner, *supra* note 111, at 274.

Excessive reliance on insurance, especially for the disclosure of less sensitive datasets, could make data access framework uneconomical for many third-party recipients.

D. Eligible Recipients

Policymakers designing an energy-data program must eventually decide who may receive data from utility companies and for what purposes. The identity of the third-party recipient and the recipient's proposed use of data matter because they relate directly to the policy goals behind energy data programs, including the facilitation of commercial activity and growth in industries like energy efficiency, which benefit the public-at-large.

Limiting the pool of eligible third-party recipients mitigates privacy concerns by reducing the likelihood of inappropriate uses of data.[115] Compared to a data-access regime in which the general public can obtain energy data, a restricted-access data program can place more useful datasets in the hands of high-value users. These users will typically be willing to take safeguards to protect data, as discussed in Section II.B, and are unlikely to breach the privacy of specific consumers in the dataset because of the negative impact on their businesses.

The purposes of data anonymization/aggregation and restricting receipt will often be the same: to safeguard against inappropriate disclosures of individual-level customer data. Policymakers should visualize a sliding scale between data anonymization/aggregation and receipt restrictions—from high anonymization/aggregation and low recipient restrictions to low anonymization/aggregation and high recipient restrictions. For heavily anonymized/aggregated datasets, a recipient's identity would matter less or not at all, because consumer-specific data would be impossible to determine from the dataset. That data could be disseminated broadly because anonymization/aggregation would have addressed privacy concerns. For dataset with no or low levels of anonymization/aggregation, it is essential to screen the identities and motives of the individual data recipients to minimize potential harm. Thus, when crafting data rules, policymakers should recognize that successful energy data programs balance the requirements of anonymization/aggregation and recipient restrictions and should not set both simultaneously too leniently or strictly.

It can be helpful to think about limiting access by type of person, by purpose, or both. By person we mean which kinds of entities are appropriate holders and users of the energy data. By purpose, we mean for what end the entities will use the energy data. In California, for example, data disclosures are limited to academic institutions (persons) and for research only (purpose).

115. *See A Regulator's Privacy Guide, supra* note 30, at vi.

Broadly speaking, defining third-party requesters is partly accomplished by reference to what they are not. A utility customer who wants access to his or her data is not a third-party requester.[116] In many states, electricity consumers have special rights of access to their own usage data.[117] A third-party recipient is also not a utility, a governmental body, or a program administrator chosen by a utility or a governmental body.[118] Colorado's definition provides a real-world example: "'Third party' means any entity other than the customer of record, the utility serving such customer, or a contracted agent [of the utility] . . . ."[119] "Third party" thus is a recipient that operates separately from the utilities and the government.

Regulators should consider defining expansively the types of entities that qualify to receive the data. An expansive understanding of "any entity," as mentioned above, would provide a wide range of entities with the opportunity to provide energy solutions. This expansive reading would include more entities than just the energy-efficiency service providers that this report has focused on and could include nonprofit organizations, academic institutions or other energy service providers (e.g., renewable energy or energy-storage companies).

Accordingly, a sensible rule would define broadly which entities can participate but make access to energy data depend upon the purpose for which data is being requested. Policymakers can accomplish this by setting criteria that outline permissible purposes for a data request.

The Fair Credit Reporting Act includes person and purpose restrictions for accessing privacy data. FCRA reduces the risk to consumers by limiting eligible recipients to credit and insurance companies, which the Credit Reporting Agency "has reason to believe":

> *intend[ ] to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or*
>
> *. . .*
>
> *intend[ ] to use the information in connection with the underwriting of insurance involving the consumer.*[120]

116. *A Regulator's Privacy Guide, supra* note 30, at 23.

117. *Id.*

118. *Id.*

119. COLO. CODE REGS. § 723- 3001(gg) (2015).

120. 15 U.S.C. § 1681b(a)(3) (2010)

Additionally, the three nationwide Credit Reporting Agencies are required to establish and maintain jointly a system through which consumers can opt out of this service.[121]

As another example, the California Public Utilities Commission created rules in 2014 to make energy data more available to academically-affiliated researchers. The commission found that "strict eligibility and confidentiality rules will permit better analyses of California energy policies while protecting the privacy of consumers and ensuring that security protocols are followed."[122] California's rule limits the identity of prospective data recipients to academic researchers.[123] Furthermore, the rule requires researchers to identify how their proposed use of the data will benefit energy efficiency, demand response, or renewable-energy programs:

> *The researcher should demonstrate that the proposed research will provide information that advances the understanding of California energy use and conservation. Research may include, but is not limited to, analysis of the efficacy of [energy-efficiency] program, or demand response programs, or the quantification of the response of electricity consumers to different energy prices or pricing structures. In addition, research pertaining to greenhouse gas emissions, the integration of renewable energy supplies into the electric grid, and the analysis of grid operations are also topics vested with a public interest and will advance the understanding of California energy use and conservation. In addition to these research topics, research tied to any energy policy identified in the Public Utilities Code as serving a public purpose is also appropriate.*[124]

This extra step of making third-party requesters dictate how their usage of data will generate a positive public benefit to energy-efficiency services decreases the likelihood of data ending up in the hands of users whose motives are harmful to the public or unrelated to the purposes of the energy data program.

While Fair Credit Reporting Act and California Public Utilities Commission examples demonstrate how strong eligible recipient and permissible purpose restrictions can operate, this report advocates for a broader range of permissible persons and permissible purposes. Anonymization and aggregation methods can help to mitigate privacy concerns from the outset, so that data may be released to a wider population of users. Eligible recipient and

---

121. *Id.*

122. *California PUC Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data*, *supra* note 78, at 145; *see also id.* at 40 ("Research into the effectiveness and efficiency of these programs is critical if California wishes to maintain its status as a national leader in these energy program areas.").

123. *Id.* at 145.

124. *Id.* at 145-46.

permissible purpose restrictions are only necessary in the context of anonymized and aggregated datasets when there is meaningful residual risk of customer reidentification that warrants shielding the datasets from the general public.

To balance the benefits of disclosing the data against the risks of misuse, policymakers must consider the sliding scale between front-end treatment of data, like anonymization and aggregation, and back-end protections to consumer privacy, like eligible recipient classifications, permissible purpose restrictions, and standardized data handling and receipt measures.[125] The "eligible recipients" and "permissible purposes" sections of the compiled model language available in Section III.D can aid in tailoring rules that enhance data utilization for energy efficiency and other programs while protecting privacy.

A final, subsidiary consideration is determining who is responsible for evaluating the identity of and purpose offered by a third-party requester. In California, this duty belongs to the utilities, but the Public Utilities Commission is involved on an ongoing basis in an oversight capacity.[126] In many states, administrative ease will lead to rules requiring that utility companies evaluate identity and purpose before releasing data to third-party requesters. In these states, it is highly important that policymakers clearly define the liability to utilities, or lack thereof, for harm to consumers arising from mistakes in applying the person and purpose tests.

125. See Section II.B *infra* for a discussion of data handling and receipt measures.

126. See *California PUC Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data, supra* note 78, at 147 ("It is reasonable to require that when a utility provides data to eligible academic researchers that it provide this Commission with a description of the information disclosed, and the name, title and business address of the researcher and institution to whom the disclosure was made in a letter to the Executive Director at least four weeks prior to the transfer.").

III. Model Rules

If state policymakers want to implement a non-consent-based energy-data release program, they have a number of different legislative and regulatory options to consider.[127] A few rules will benefit all three major categories of stakeholders—utilities, data recipients, and consumers—while other provisions will generally benefit a specific set of stakeholders. Stakeholders may be ambivalent about another category of rules either because the rules' appeal depends upon the existence or non-existence of other rules or because different members of the stakeholder group may have different perspectives on the costs and benefits.

Policymakers should understand that these rules are interrelated. The choice of one type of rule and its particular formulation may change the desirability of another rule or series of rules. For example, if policymakers choose to adopt a broad definition of "eligible recipient," that may increase the desirability of a rule that requires data recipients to have insurance because, as access to data increases, so does the risk of unauthorized disclosure. Another example is the choice of adopting administrative penalties for unauthorized disclosures. Such a penalty system, combined with the general desire to have utilities embrace, or at least not fight, the aggregated energy-data release program, may reduce the need to give consumers a private right of action against those who disclose in an unauthorized manner. Policymakers should commit to working through—rather than shying away from—the interrelationships among different choices of law as they anticipate what challenges may arise after codification or promulgation.

Equally as important as the interrelated nature of these rules is how financially burdensome the rules may be. How high an administrative penalty will be or how much insurance recipients are compelled to have, for example, will affect the impacts and the appeal of certain rules, and different stakeholders may change their preferences at different dollar amounts. As an illustration, if a rule requires third-party recipients to buy a significant amount of insurance coverage, and if that level of coverage is expensive, then the third-party recipients may oppose the rule as too costly; however, if the insurance is affordable, and if the acquisition of insurance is a necessary condition for utilities and consumers to agree upon for

127. For a discussion of consent-based options, see the Appendix.

disclosure, then the third-party recipients may accede to an insurance requirement. Conversely, requiring third-party recipients to purchase less insurance—or not requiring them to purchase insurance at all—may lead stakeholders to reverse their preferences. As a result, policymakers should carefully consider the consequences of rules imposing direct costs because they may determine how resistant certain stakeholders are to the certain aspects of the rules package.

Rules Generally Benefitting All Stakeholders	Rules Generally Favoring One Stakeholder Group			Rules Triggering Ambivalence Among Stakeholders
	Rules Favoring Utilities	*Rules Favoring Recipients*	*Rules Favoring Consumers*	
• Limiting requesters to "permissible persons" and requiring a "permissible purpose" related to the policy goals of the rule • Banning reidentification • Requiring that utilities and recipients create and execute reasonable security measures for enumerated—but non-exhaustive—purposes • Explicitly stating how the implement-tation of rules affect pre-existing rights and legal authorities	• Mandating an agreement that transfers the costs of liability from the utility to the recipient • Absolving the utility of liability • Restricting private rights of action • Establishing a mechanism by which others pay implement-tation costs	• Clarifying that the purpose of the rule is to enhance access to data for energy efficiency • Requiring aggre-gation at a "4/80" level • Restricting private rights of action	• Resolving data ownership in favor of consumers • Creating a private right of action for for illegal data disclo-sures • Requiring recipients to hold data breach insurance • Requiring aggre-gation at a "15/15" level	• Implementing a reasonable reidentifi-cation standard • Requiring utilities to pay administrative fines for unauthorized data disclosures • Requiring utilities and recipients to follow very specific data-security procedures • Requiring utilities and data recipients to follow an industry standard for data-security procedures

Equally as important as the interrelated nature of these rules is how financially burdensome the rules may be. How high an administrative penalty will be or how much insurance recipients are compelled to have, for example, will affect the impacts and the appeal of certain rules, and different stakeholders may change their preferences at different dollar amounts. As an illustration, if a rule requires third-party recipients to buy a significant amount of insurance coverage, and if that level of coverage is expensive, then the third-party recipients may oppose the rule as too costly; however, if the insurance is affordable, and if the acquisition of insurance is a necessary condition for utilities and consumers to agree upon for disclosure, then the third-party recipients may accede to an insurance requirement. Conversely, requiring third-party recipients to purchase less insurance—or not requiring them to purchase insurance at all—may lead stakeholders to reverse their preferences. As a result, policymakers should carefully consider the consequences of rules imposing direct costs because they may determine how resistant certain stakeholders are to the certain aspects of the rules package.

Because such an energy-data program is so valuable in the long run in terms of improving energy efficiency, we believe that a package can be worked out that is to the benefit of every set of stakeholders. Regardless of whether one stakeholder group is benefitted more than another, many combinations of these rules would be better for all stakeholder groups than the status quo, in which there is no program for releasing energy data. While policymakers should carefully consider the interrelationship and consequences of language choices, they should take solace in the fact that whatever system emerges should offer more benefits than costs or harms.

A. Model Language Generally Benefiting All Stakeholders

All groups of stakeholders generally benefit from rules that define clearly permissible recipients and permissible purposes, that ban reidentification, that require implementation of data-security procedures, and that state explicitly how the statute or rulemaking should be interpreted. Knowing clearly who should and should not have access to energy data and for what purposes helps utilities, third parties, and consumers know who is going to be doing what with the data. A clear statement that reidentification of aggregated consumer-energy data is illegal clarifies for all that the conduct that is forbidden and thereby discourages it from occurring. Everyone has an interest in protecting data from malfeasors if the costs are not exorbitant. Any rule that clarifies how to read the requirements will save time and money when problems arise later that require statutory or regulatory interpretation.

1. Limiting disclosure to authorized "third-party recipients" for "permissible purposes"

Model Language: *Within this rule, "third party" indicates that the recipient operates separately from the utilities and government. Any entity other than the customer of record, the utility serving such customer, or a contracted agent of the utility can be considered a third party.*[128]

The third-party recipient must disclose to the [utility / the public service utilities] the recipient's proposed use for aggregated energy datasets prior to any transfer of data. In order to be eligible to receive aggregated energy datasets, the requester must demonstrate that the proposed use of data will [advance the understanding of or promote the effectiveness of / lead to increased implementation of] energy-efficiency measures.[129]

The first paragraph, adapted from Colorado's energy-data rules, simply clarifies the meaning of third-party recipient throughout the remainder of the model rule. Colorado has a broad definition, in contrast to California, which focuses on academic institutions.[130]

Limiting the pool of eligible recipients mitigates the risk of disclosure by reducing the number of potential recipients and by focusing on ones which will be likely to protect and to use the data wisely, e.g., energy-efficiency providers, academic institutions, etc. This benefits utilities, third-party recipients, and consumers.

A balance will need to be struck though. Policymakers may also allow data at a more granular level to be provided if the class of eligible data recipients is more limited and controllable, because the risk of unauthorized access or misuse is reduced. However, an extremely narrow definition may limit the innovation that could arise from opening the data to a wider range of entities, which would harm consumers and entrepreneurial third-party recipients. Such provisions could be coupled with other protections listed elsewhere in this Section III.

The second paragraph in this model rule limits data transfers for permissible purposes. The purposes provided in the model rule are illustrative but should track the purposes section of the rules and legislation, e.g., to advance understanding and deployment of cost-effective energy-efficiency measures.

---

128. COLO. CODE REGS. § 723-3001(gg).

129. *See generally California PUC Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data*, *supra* note 78, 41-42.

130. *See* Section II.D. *infra*.

It is generally in the interests of consumers and third-party recipients that recipients demonstrate they will use the data for permissible purposes. The law is designed to help third parties who want to get access to this information for these purposes, so they should not be opposed to this provision. Consumers should be willing to take slight incremental risks regarding the disclosure of their data—whether in an aggregated or granular form—in exchange for the benefits of improved energy efficiency, so it makes sense to impose this kind of requirement to make sure that the data disclosure is for the right objectives.

Utilities should generally be in favor of such provisions as well. Simple criteria that relate to the policy aims of the rule coupled with clear delineations in the liability section of the rule can lessen the extent to which eligible recipients and permissible purposes are a concern for utilities.[131] However, utilities may want the public utilities commission to make a determination as to whether any individual data request fits the purposes provision so that the utility is not liable if it makes an incorrect decision.

2. Banning reidentification

Model Language: *No person may attempt to reidentify aggregated or anonymized consumer energy data.*[132]

This language establishes clearly that no one may take a data set covered by this program and attempt to determine the individual consumers whose data is being reported. Consumers benefit because it forbids an action that threatens their privacy. Utilities and legitimate third-party recipients benefit because it establishes that reidentification is a bad act, which may have the practical effect of shifting attention and liability to those malfeasors and away from the utilities and lawful third-party recipients.

3. Requiring that utilities and data recipients create and execute reasonable security measures for enumerated—but non-exhaustive—purposes

Model Language: *A utility and data recipients shall use reasonable security measures to protect a customer's unencrypted data from unauthorized access, destruction, use, modification, or disclosure. These measures shall include but are not limited to:*

1. *written policies regarding information security, disaster recovery, third-party assurance auditing, penetration testing, and aggregated data transfers;*

131. See, for example, model rule on "absolving the utility of liability."

132. *See California PUC Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data*, *supra* note 78, at Attachment B: Model Non-Disclosure Agreement, 2.

2. *password protected workstations at recipient's premises, any premises where work or services are being performed, and any premises of any person who has access to such data;*
3. *encryption of the data;*
4. *measures to safeguard against the unauthorized access, destruction, use, alteration or disclosure of any such data including, but not limited to, restriction of physical access to such data and information, implementation of logical access controls, sanitization or destruction of media, including hard drives, and establishment of an information security program that at all times is in compliance with reasonable security requirements as agreed to between recipient and utility.*[133]

This language is adapted from the model language provided as part of the California-mandated non-disclosure agreement between a utility and a third-party recipient.

As a floor, this rule favors all three stakeholder groups. This rule gives the utility and the recipient some guidance on the areas in which they are expected to develop data-security procedures. Whether utilities and recipients would favor a rule that specifies the procedures they must implement with even more precision is debatable and is discussed in Sections III.C.3 and III.C.4. Such measures are also inherently pro-consumer because they should help protect the integrity and privacy of consumer data.

4. Stating explicitly how the implementation of certain rules affect or do not affect pre-existing rights and legal authorities

The following three rules benefit all stakeholders because they tell stakeholders, administrative agencies, and courts *how* to interpret the legal authority governing the energy-data transfer program. Policymakers may want the substance of the rules to be the exact opposite of what is provided here in the examples, although that is doubtful; regardless, all stakeholders benefit from reducing ambiguities that may arise after the codification or promulgation of the program because they will be able to save themselves from the risks of ambiguity and from spending large sums of money to litigate how to interpret such ambiguities.

133. *See California PUC Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data*, *supra* note 78, at Attachment B: Model Non-Disclosure Agreement, 2-3. The authors of this report added "and aggregated data transfers" to the original language.

i. Proclaiming that the law or rule does not limit a consumer's right to provide his or her data to anyone

Model Language: *Nothing in these rules shall limit a customer's right to provide his or her customer data to anyone*.[134]

Stakeholders may question whether the energy-data program contemplated by this report would change a consumer's ability to give his or her data to anyone. The model language above, which is identical to one adopted in Colorado, would answer this question.

ii. Stating that the implementation of a rule does not prevent subsequent waiver, repeal, or revision

Model Language: *Nothing in paragraph [ ] shall prevent the Commission from waiving, repealing, or revising any Commission rule in a manner otherwise consistent with applicable law*.[135]

Should policymakers decide to implement this energy-data program through rulemaking, such a rule, based off of a Colorado rule, would clarify the leeway that a public utilities commission would have in changing the regulatory approach and the lack of vested rights in those rules.

iii. Codifying a presumption against implied repeal

Model Language: *The [act name] being a general act intended as a unified coverage of its subject matter, no part of it shall be deemed to be impliedly repealed by subsequent legislation if such construction can reasonably be avoided*.[136]

If policymakers decide to implement parts or all of this program by statute rather than rulemaking, it would be helpful to clarify now how future legislation should be interpreted.

B. Model Language Generally Favoring One Stakeholder Group Rather Than Another

Some policies and model language favor the interests of one stakeholder group more than another. The following subsections present these options, organized by each major

134. COLO. CODE REGS. § 723-3027(e) (2015).

135. *See id.* § 723-3660(g)(VI).

136. *See* U.C.C. § 1-104 (AM. LAW INST. & UNIF. LAW COMM'N 1977).

stakeholder group. Policymaking is the product of compromise, so a state's final statute or rule may include elements from all three categories.

1. Rules favoring utilities

Utilities benefit from rules that transfer liability or the costs of it from them to others, such as absolving them from liability. The stronger these rules are, the more likely the utilities are to embrace—or at least not to resist—an energy-data transfer program.

i. Mandating an agreement that transfers the costs of liability from the utility to the recipient

Model Language: *Recipient shall defend, hold harmless and indemnify the utility and its affiliates, officers, directors, employees, agents, representatives, successors and assigns, from and against any and all losses, causes of action, liabilities, damages and claims, and all related costs and expenses, fines, penalties, or interest, including reasonable outside legal fees and costs, arising out of, in connection with, or relating to recipient's use, maintenance and/or disclosure of data.*[137]

This language borrows from the California model non-disclosure agreement (NDA). Shifting the costs of liability may go a long way in reducing utility resistance to this program, although utilities might be concerned about whether the recipients will be financially solvent or will fail to perform their obligations.

ii. Absolving the utility of liability

Model Language (Stronger Version): *A utility and each of its directors, officers and employees that discloses data as provided in these data privacy rules shall not be liable or responsible for any claims for loss or damages resulting from the utility's disclosure of data.*[138]

Model Language (Weaker Version): *If and only if a utility follows the data-security measures in section [ ] and releases data only to eligible recipients as defined in section [ ], a utility and each of its directors, officers and employees that discloses aggregated data as provided in these data privacy rules shall not be liable or responsible for any claims for loss or damages resulting from the utility's disclosure of data.*

---

137. *See California PUC Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data*, *supra* note 78, at Attachment B: Model Non-Disclosure Agreement, 4. The authors of this report added "and indemnify" to clarify that legal protections extend to claims brought by others.

138. *See* COLO. CODE REGS. § 723-3033(f).

Policymakers have a choice between implementing a stronger or weaker version of this rule. Based on the Colorado rule, the stronger version provides a full release, whereas the weaker absolves the utility of liability only if the utility were to follow certain predefined procedures. The stronger version protects utilities more than the weaker version, and the weaker version would require utilities to take greater care than the stronger version.

iii. Restricting private rights of action

Model Language: *[No person / no consumer / no one who is not a consumer] shall have a private right of action against a utility for harm arising from release of data under this [act / rule /chapter].*[139]

This rule is inherently utility friendly by precluding private rights of action against the utility. The rule also has the benefit of resolving in advance, through express language, the issue of whether the law or rule precludes private rights of action as discussed in the chapter on liability.

Policymakers have a choice as to how much to limit the private right of action. Not allowing anyone to sue provides the most protection for the utility. Not allowing consumers or non-consumers to sue also limits the kinds of people also provides protections for the utility; which option is selected depends on what categories of potential harm policymakers are trying to exclude.

iv. Establishing a mechanism by which others pay implementation costs

Model Language: *A utility that provides data shall be reimbursed for its reasonable expenses by [the recipient / ratepayers].*

This provision is designed to address the concern of utilities that they will incur costs to implement the data transfer program—such as IT and personnel costs—but not be reimbursed for those costs. This language is designed to address this concern. Regulators may need to modify this language so that it comports with the ways in which utilities are allowed to charge consumers as a whole for other kinds of administrative costs.

---

139. *Compare* 15 U.S.C. § 2649 (1986) (limiting private rights of action under the Asbestos Hazard Emergency Response Act) ("Nothing in [this subchapter] creates a cause of action or in any other way increases or diminishes the liability of any person under any other law"); H.R. REP. 99-763, 31, 1986 U.S.C.C.A.N. 5004, 5022 ("The goal of the legislation is to accomplish the rapid, safe, effective and appropriate responses to asbestos in schools, not to influence in either the plaintiff's or defendant's favor the disposition of any state product liability cases.").

2. Rules favoring third-party recipients

Third-party recipients benefit from the existence of this kind of program generally. Furthermore, the greater granularity in the data they are able to access and the greater the acceptance of and compliance with the program by utilities, the better off third-party recipients are.

i. Clarifying that the purpose of the rule is to enhance access to data for energy-efficiency purposes

Model Language: *Findings and Intent. It is declared to be the policy of the state that electric utilities are required to make energy usage datasets available to third parties as a means to facilitate increased investment in energy efficiency. Increasing investment in energy-efficiency measures will reduce direct and indirect costs to consumers by decreasing environmental impacts and by avoiding or delaying the need for new generation, transmission, and distribution infrastructure. As long as both utilities and data requesters take all steps reasonably necessary to secure against inadvertent or unauthorized disclosure of personally identifiable energy data, it serves the public interest to require electric utilities release energy usage datasets.*[140]

Statements of state policy are common in energy regulations and statutes; the example here is a modified version of the policy preamble from Illinois' utility-led energy-efficiency procurement statute.[141]

It may not be self-evident from a data access program why the state public utility commission or legislature has chosen to require utilities to release data. This language would resolve this ambiguity, and in doing so, it also provides a platform for the rule's drafters to clarify the public policies underlying the release of data. Clarifying the public policy behind the rule also establishes a form of legislative intent, which can be used to interpret other sections of the rule. For example, the meaning of a potentially ambiguous phrase like "permissible purpose" in the context of an eligible recipient rule[142] is more easily understood when paired with language clarifying that the overall purpose of the rule is to "facilitate increased investment in energy efficiency."

140. *Compare* 220 ILCS 5/8-103 (2013).

141. *Id.*

142. *See* Section II.D. *infra*.

ii. Requiring aggregation at a "4/80" level

Model Language: *In aggregating customer data to create an aggregated data report, a utility must take steps to ensure the report is sufficiently anonymous in its aggregated form so that any individual customer data or reasonable approximation thereof cannot be determined from the aggregated amount. At a minimum, a particular aggregation must contain: (1) at least four customers or premises, and (2) within any customer class, no single customer's data or premise associated with a single customer's customer data may comprise 80 percent or more of the total customer data aggregated per customer class to generate the aggregated data report (the "4/80 Rule").*[143]

This language is borrowed from the Colorado rule, but rather than providing for disclosure at the 15/15 level, it allows recipients to receive data coming from as few as four customers at a time, so long as no customer's data comprises over 80% of the data. This language is recipient friendly because it provides data at a fairly granular level and therefore helps them with analysis and targeting.

iii. Restricting private rights of action

Model Language: *[No person / no consumer / no one who is not a consumer] shall have a private right of action against recipients for harm arising from release of data under this [act / rule /chapter].*[144]

Similar to the model rule for utilities in Section III.B.1.iii, this language is inherently friendly to recipients by precluding private rights of action against the recipients. Again, policymakers have a choice as to how much to limit the private right of action by selecting who cannot sue, with "no person" being the most protective of the third-party recipients.

3. Rules favoring consumers

The energy consumers contemplated by this report are those who recognize the value of data disclosure and have reasonable concerns about privacy. There is middle ground between a program that would allow all data to be shared and a ban on data sharing. Consumers should appreciate the value of data disclosure but should also want reasonable safeguards in

143. *Compare* COLO. CODE REGS. § 723-3031 (adopting the "15/15" standard).

144. *Compare* 15 U.S.C. § 2649 (1986) (limiting private rights of action under the Asbestos Hazard Emergency Response Act) ("Nothing in [this subchapter] creates a cause of action or in any other way increases or diminishes the liability of any person under any other law"); H.R. REP. 99-763, 31, 1986 U.S.C.C.A.N. 5004, 5022 ("The goal of the legislation is to accomplish the rapid, safe, effective and appropriate responses to asbestos in schools, not to influence in either the plaintiff's or defendant's favor the disposition of any state product liability cases.").

place to prevent their privacy from becoming unduly compromised. Consumers generally benefit from rules that resolve data ownership in consumers' favor, create private rights of action, require insurance, and demand a high level of anonymization and aggregation.

i. Resolving data ownership in favor of consumers

Model Language: *Customer is principal owner of retail electric consumption data. The customer has the ability to authorize third parties to access individual customer data, and the customer can revoke that access at the customer's discretion. The utility serves as the guardian of retail electric consumption data and must allow access to third parties where the customer has authorized it*.[145]

The legal importance of ownership over energy data varies from state to state. Nonetheless, resolving ownership in favor of customers would, at a minimum, give each customer certain rights—or confirm that he or she has the rights—to acquire his or her individual-level usage data and to share that data with third parties.

ii. Creating a private right of action for illegal data disclosures

Model Language (Stronger Version): *Any person who fails to comply with any requirement imposed under this subchapter with respect to any [consumer / individual] is strictly liable to that [consumer / individual] in an amount equal to the sum of: (1) any actual damages sustained by the [consumer / individual] as a result of the failure; and (2) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.*

Model Language (Weaker Version): *Any person who is negligent in failing to comply with any requirement imposed under this subchapter with respect to any [consumer / individual] is liable to that [consumer / individual] in an amount equal to the sum of: (1) any actual damages sustained by the [consumer / individual] as a result of the failure; and (2) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.*[146]

---

145. Citizens Utility Board & Environmental Defense Fund, *Open Data Access Framework*, ENVIRONMENTAL DEFENSE FUND, at 1, http://blogs.edf.org/energyexchange/files/2014/08/14-CUB-EDF-Exhibit-1-1-Open-Data-Access-Framework-FINAL.pdf (last visited Dec. 16, 2015).

146. *See* 15 U.S.C. § 1681o(a) (2016) (establishing civil liability for negligent noncompliance under the Fair Credit Reporting Act, which regulates the release of credit information by Credit Reporting Agencies (CRAs) to third parties).

Policymakers have a choice between implementing a stronger or weaker version of this rule. The stronger version implements strict liability for damages suffered by a customer or an individual. The weaker version, which is based upon the FCRA rules regarding private rights of action, implements a negligence standard. Strict liability regimes are generally easier to administer than negligence standards because no proof of negligence is required, which both judges and potential consumer plaintiffs would value; however, strict liability may lead utilities and recipients to invest more in security measures, which they may be reluctant to do.

Policymakers have an additional choice: Do they limit the right to sue to consumers or open it to all individuals? Allowing anyone to sue—regardless of whether he or she has a contract with the utility or the EESP—broadens the potential scope of liability for the utility or EESP, but it also likely comports with the motivation for including such a provision in the first place, i.e. giving those who have been harmed the opportunity to recover.

iii. Requiring a recipient to have data-breach insurance

Model Language:

(1) Obtaining insurance. Every eligible third-party recipient of covered[147] *energy data shall obtain data breach insurance coverage to provide protection and indemnity against the release of nonpublic confidential information in the legal care, custody or control of the third-party recipient to an untrusted or unauthorized environment, as well as agents and independent contractors of the third-party recipient, which includes, but is not limited to, employees of the third-party recipient, subcontractors, and affiliates.*

(2) Coverage requirements. The data breach insurance coverage shall contain a provision that coverage will not be canceled, or not renewed, or allowed to lapse for any reason until at least sixty (60) days prior written notice has been given by the insurer to the utility or utilities responsible for dispensing data and state public utilities commission. A certificate of insurance or similar documentation showing such data breach insurance coverage to be in force shall be provided to the utility or utilities and the state public utilities commission prior to the third-party recipient engaging in any covered energy data acquisition activities. The data breach insurance coverage shall be obtained from an insurance company licensed to do business in this state that continuously maintains an A.M. Best Company rating of at least A: VII while the policy is in effect. Such data breach insurance coverage shall continuously remain in full force and effect subject to state public utilities commission approved revisions to

147. See Section II.C.5. "Covered" activities must be defined elsewhere in the rule.

the amount of coverage for as long as the third-party recipient continues to receive covered energy data from the utility or has access to covered energy data received from a utility previously.

(3) Duty to report to the state public utilities commission. The amount of the initial data breach insurance coverage obtained by the third-party recipient, as well as any subsequent amendments to the amount, shall be approved by the state public utilities commission in writing prior to the third-party recipient obtaining the data breach insurance coverage or revising the amount of coverage. It shall be in the commission's sole discretion to determine the amount of required data breach insurance coverage.

(4) Coverage amounts. In order for the state public utilities commission to make the determination in paragraph (3) related to the appropriate amount of data breach insurance coverage, a third-party recipient, upon request by the state public utilities commission, shall provide the state public utilities commission with a written justification setting forth the third-party recipient's rationale for the appropriate and necessary amount of data-breach insurance coverage. Such justification shall set forth in detail the safeguards or protections that will be employed to mitigate the risks of an intentional or unintentional release of the data in the third-party recipient's possession or in the possession of agents, affiliates, and independent contractors of the third-party recipient, which shall include, but not be limited to, an evaluation of potential exposures under various stress scenarios that include intentional and unintentional releases of data in the third-party recipient's control environment and the sufficiency of the proposed data breach insurance coverage to mitigate such exposures. In addition, the third-party recipient's justification for the proposed proper amount of data breach insurance coverage shall evaluate the potential costs to the third-party recipient as a result of a breach, which shall include, but not be limited to, forensic costs, legal fees, first-party liabilities (e.g., harm to the third-party recipient directly), third-party liabilities (e.g., harm to the affected consumers), notification requirements, remediation costs, restoration costs, and business impact.[148] *Members of the public may comment on the proposal from a third-party.*

A data-breach insurance requirement protects consumers from insolvent or judgment-proof third-party recipients by providing a pool of money for victims of data theft or data

148. This language is adapted from a data breach insurance provision in Georgia regulations. *See* GA. COMP. R. & REGS. § 80-12-7-.04 (2013).

misuse.[149] It also helps consumers because the expense of insurance discourages third parties that have only a casual interest in the data from seeking it.

This rule sets a framework for requiring third-party recipients to purchase data-breach insurance as a prerequisite to receiving energy data. Paragraphs (3) and (4) intentionally leave the level of coverage and the details of the coverage policy open for the state public utilities commission to determine in consultation with third-party recipients. This allows flexibility for the public utility commission to consider statewide priorities regarding energy-data access, the status of data-breach insurance markets, and coverage status under a variety of hypothetical risk-exposure scenarios. For example, because such a requirement might dissuade legitimate third-party recipients if the cost is too high, one way to manage the reasonableness of the expense would be to require insurance only for transfers of the most sensitive and granular forms of data that a utility is required to disclose.

iv. Requiring aggregation of customers at a "15/15" level

Model Language: *In aggregating customer data to create an aggregated data report, a utility must take steps to ensure the report is sufficiently anonymous in its aggregated form so that any individual customer data or reasonable approximation thereof cannot be determined from the aggregated amount. At a minimum, a particular aggregation must contain: (1) at least fifteen customers or premises, and (2) within any customer class, no single customer's customer data or premise associated with a single customer's customer data may comprise 15 percent or more of the total customer data aggregated per customer class to generate the aggregated data report (the "15/15 Rule"). Notwithstanding the 15/15 Rule, the utility shall not be permitted to disclose aggregated data if such disclosure would compromise the individual customer's privacy or the security of the utility's system."*[150]

In its energy-data decision, the Colorado Public Service Commission decided that the 15/15 rule was necessary to protect consumer privacy and rejected the more lenient 4/80 or 3/50 options.[151] The greater the aggregation, the less the likelihood of consumer harm. Consumers are likely to favor a 15/15 rule as compared to the other less aggregated options, although implementing such a rule trades off some potential innovation opportunities that could arise from the disclosure of more granular information.

149. Utilities may also benefit if the state's liability rules hold that a utility is jointly responsible with the recipient for a data breach. Third-party recipients also derive a benefit as the holder of the insurance policy if the coverage allows the recipient to shift liabilities to the insurer, albeit at a cost to the third-party recipient which purchases the insurance.

150. COLO. CODE REGS. § 723-3031.

151. *Colorado PUC Energy Data Decision*, *supra* note 54, at 13 & n. 20.

C. Model Language That May Trigger Ambivalence Among Stakeholders

Stakeholders may be ambivalent about some rules either because the rule's appeal depends upon the existence or non-existence of other rules or because different members of the stakeholder group may have different perspectives on the costs and benefits.

1. Implementing a reasonable reidentification standard

Model Language:

Stronger version: *Energy-use data may only be released to third parties if the data is aggregated to the point where it contains the data of a sufficient number of similarly situated customers so that the daily usage routines or habits of an individual customer cannot reasonably be deduced from the data.*[152] *The data must not include any identifying information (including names, addresses, account numbers) that would enable third parties to identify or reidentify individual customers.*[153]

Weaker Version: *Energy-use data may only be released to third parties if the methodology used to aggregate or to anonymize customer data strongly limits the likelihood of reidentification of individual customers or their customer data from the aggregated or anonymized data set.*[154]

This language may trigger ambivalence among stakeholders because it is a standard and not a rule.

The standard gives flexibility; it allows for subsequent interpretation by utilities, third parties, consumers and ultimately regulators. It also allows for creating an energy-data program without making legislators resolve questions about whether a 4/80 level, a 15/15 level, or some other level is optimal.

But flexibility creates concerns. Utilities may be worried that they may be held liable if someone reidentifies the data, even though the utility took what it thought was reasonable precautions under the circumstances. Third parties may be concerned for the same reasons. Conversely, third parties may be concerned that a standard provide a rationale for the utilities to provide more aggregated (and therefore less useful) data to them. Consumers may be similarly unsure. If the aggregation is too low and there is a breach, consumers will be

152. *See* OKLA. STAT. tit.17 § 710.7(B)(2) (containing substantially similar language).

153. *See California PUC Privacy and Security of the Electricity Usage Data Decision, supra* note 31, at 150-51.

154. *Data Privacy and the Smart Grid*, *supra* note 67.

concerned about their privacy. If the aggregation is too high, then consumers will not benefit from energy-efficiency opportunities as much as they would have otherwise.

2. Requiring utilities and third-party recipients to pay administrative fines for unauthorized data disclosures

Model Language. *The public utilities commission reserves the right to impose civil penalties up to [____] [per ____] for unauthorized disclosure of consumer energy data*.[155]

This model language gives the public utilities commission the ability to impose civil fines. There could be a set amount (e.g., $1,000) that is multiplied by a factor that relates to impact (e.g., the number of times the data was released in an unauthorized manner, the number of customers affected, the number of days that the data was released in an unauthorized manner before it was disclosed to consumers or regulators, etc.). There could be a range for the fine that relates to severity, e.g., $100 to $500 if moderate, $1,000 to $5,000 if serious, $10,000 to $25,000 if severe.

It may seem that utilities and EESPs would oppose administrative-penalty systems like the one promulgated in Colorado because the public utilities commissions may levy sizeable fines. However, their level of opposition may depend on the level of the fine, e.g., a utility or EESP may have different views if a fine is likely to be $1,000 or $1,000,000. Moreover, such a system would constrain the cost and could therefore be somewhat more manageable and predictable than the potential damages under a private rights of action.

Conversely, if administrative fines were accompanied by restrictions on private rights of action against violators, then individuals may be ambivalent about the system. In such a scenario, the penalty schedule would still deter the utility or EESP from unauthorized data disclosure. However, an individual would not be able to recover because the penalties would be paid to the government, not to the individual. Furthermore, if the penalty was low relative to the harm inflicted, it would lead to under deterrence, under investment in security measures, and less than optimal protections for individuals. Thus, in a situation where a penalty schedule substitutes for a private right of action, a penalty schedule may be less desirable for individuals.

Despite this ambiguity, such penalties are important tools to consider given their deterrent effects and ease of administration.

155. This language is adapted from the Colorado administrative code. *See* COLO. CODE REGS. § 723-3976 (changing "aggregated data" to "consumer energy data").

3. Requiring that utilities and third-party data recipients follow very specific data-security procedures

Model Language (non-exhaustive examples):

Security personnel: Utilities and third parties shall appoint positions and/or personnel to ensure that security and privacy policies are properly maintained, updated, and followed.[156]

Information tracking: In developing and updating policies and practices, utilities and third parties shall develop a set of privacy use cases as a method to track information flows and the privacy implications of collecting and using data to help the organization to address and mitigate the associated privacy risks within common technical design practices and business practices.[157]

Best-Practice Sharing: Third parties shall share solutions to common privacy-related problems with other smart grid market participants in some appropriate manner (e.g., trade forums, associations, public policy, public outreach, external coordination, etc.).[158]

Employee Training: Each utility and third-party organization shall document, maintain, and monitor each employee's security and privacy training activities on an individual basis, including basic security and privacy awareness training in accordance with the organization's security and privacy policies.[159]

Audits: Each utility and third party shall conduct a periodic independent audit of its data privacy and security practices.[160]

The language from these rules has been borrowed from some that has been contemplated by the National Institute of Standards and Technology, an agency of the Department of Commerce that sets computer security standards for the federal government. These rules are not exhaustive but are merely examples of ones that policymakers could choose to implement.

On the one hand, specific rules would restrict the freedom of the utilities and third-party recipients in creating and maintaining data security policies and procedures. On the other hand, specific rules would give stakeholders guidance and could help shield them against

156. *See NIST Guidelines Volume 2*, *supra* note 71.

157. *See id.* at D-3.8.

158. *See id.* at D-3.8.

159. *See id.* at D-3.11.

160. *See id.* at D-3.12.

liability if they follow the rules. Whether utilities and third parties support such rules depends on which of these two considerations is more important to them.

Consumers may also be ambivalent. They may want strong data protection procedures. However, consumers may not want those rules if they impose costs and restrictions that make it too difficult for third-party recipients to innovate. Also, consumers may not like such provisions if they are coupled with an explicit liability release.

As discussed in Section II.B, promulgating specific security rules may require policymakers to become experts on data-transfer procedures, which may delay the rulemaking process. However, this fear may be overstated given that guidance documents from federal agencies administering data-privacy rules offer resources for policymakers.

4. Requiring that utilities and third-party data recipients follow an industry standard for data-security procedures

Model Language: *A data recipient shall comply with the most recent data-security guidelines issued by the [International Standards Organization] to protect aggregated data from unauthorized access, destruction, use, modification, or disclosure. The data recipient must seek [ISO] certification.*

This language is not based off of an existing rule or standard, and policymakers could easily substitute other industry groups for the International Standards Organization.

The tradeoffs are similar to those with the previous model rule. Utilities and third-party recipients may not welcome the specific requirements being imposed on them, and furthermore, they may chafe at the expense of certification. They may be more willing to accept these requirements if compliance with the standards shields them from liability.

Consumers may feel assured knowing that utilities and recipients must seek third-party certification with regard to their data procedures. However, it is unclear if calibrating the law to industry standards would lead empirically to less unauthorized access to data.

With this choice in language, policymakers can avoid becoming experts in data-security rules. Furthermore, the updating built into the standards provides utilities and third-party recipients with current best practices.

IV. Conclusion

"Customer data has the potential to be the fuel for innovation which unlocks vast unrealized opportunities for greater energy efficiency."[161] A few states have already started down the path to using energy data to promote innovation and greater competitiveness in the energy-efficiency services sector. It is time for other states to seize this opportunity.

Building on existing energy-data programs and analogies from similar areas of law, this report has outlined the path forward for states. With the language and analysis in this document, policymakers can design new energy data programs for their states that balance liability, reputational, consumer privacy, implementation, and revenue concerns in a way which makes sense for their individual states. As regulations are changed and more energy data programs are rolled out, it will become evident which programs are best able to fuel energy-efficiency innovation while addressing these concerns.

When legislators and regulators adopt our proposed approaches, more energy data will be unleashed—safely and securely. And with it will come the true revolution: not the information itself, but actions that arise from mining the data for insights that will in turn spur innovation, save money and protect the environment. With benefits like these, it's time to free the data and let it flow.

161. *See A Regulator's Privacy Guide, supra* note 30, at 25.

V. Appendix— Contractual Approaches

Another way that a utility could disclose customer data to third parties would be for the utility to obtain a customer's consent before disclosing the data. While this report focuses on the disclosures of aggregated consumer data without explicit consumer consent, it is useful for policymakers to know the contractual options available. There are at least two methods for securing consent by contract: through (1) a separate contract or (2) a modified service agreement. Although both methods are viable, modifying the service agreement is likely the cheaper and more efficient route, particularly for prospective data. Some efforts are already underway in this regard.

A. Separate Contract

In the context of energy-data disclosure, a consumer could expressly consent to disclosure his or her data through a separate contract between the consumer and the utility. This is a relatively straightforward proposition because the customer could consent to almost anything related to his or her data. For example, the contract could allow customers to choose how much they want to share, ranging from anonymized data to full disclosure.

However, there are drawbacks to gaining consent through a separate contract. Contracting individually creates transaction costs. The customer may be reluctant to sign a separate agreement as it would require more effort, e.g., reading, understanding and signing provisions that are in addition to the standard, take-it-or-leave-it terms of service. Also, customers may not be as likely to give consent through an individual contract because the terms of a separate agreement may garner extra attention given that the customer will be curious about the new document the utility is asking him or her to sign.

B. Service Agreement with a Built-in Option to Opt Out

Instead of pursuing separate contracts, utilities could include a "consent to disclose data" clause as part of their service agreements. A service agreement that is altered to include

these kinds of provisions is more cost-effective and will likely generate more data for third parties than seeking separate contracts.

1. Explanation of a service-agreement approach

Utilities could add a clause into their standard service agreement or terms of service that would contain an explanation of what data would be disclosed and to whom. By accepting service provided by the utility, the customer would accept the terms of the clause. This method is likely legally sound as long as the customer has notice that the terms are altered, the material terms of the contract are not altered, and the terms are not unconscionable.[162]

To avoid concerns about whether the utility is forcing consumers to agree to disclose, the service agreement should provide customers with the ability to opt out from disclosure. The opt-out provision would require affirmative action on the part of the customer to inform the utility that he or she does not consent to his or her energy-use data being disclosed.[163] A service agreement that contains these terms does not constitute an unconscionable contract so long as a customer could easily reject the new terms of the service agreement and still receive services.[164]

This opt-out provision would likely need to be easily identifiable. How to accomplish this may vary depending on how utilities present their service agreements, e.g., online, via mailer, on the bill, etc. Utilities will also have to choose how long a customer will have the right to inform the utility that they wish to keep their data private. In other scenarios, courts have held that 30 days is a sufficient time in which a customer can reject expressly the terms of an agreement.[165] It seems likely that a 30-day time limit might be sufficient for the opt-out option with regards to energy efficiency as well. Leaving the option open as long as the customer receives service, however, is even more likely considered legally permissible. Either option would likely be fine for data analysis purposes by third parties.

2. Offer, acceptance, and consideration of a service agreement

The service agreement will need to meet all the typical requirements of a valid contract. Luckily, the legal uncertainty of offer and consideration will likely not be an issue. The offer is

---

162. *See, e.g., All Am. Roofing, Inc. v. Zurich Am. Ins. Co.,* 934 N.E.2d 679, 686 (Ill. App. 2010).

163. *See, e.g., Boomer v. AT&T Corp.*, 309 F.3d 404, 414 (7th Cir. 2002) (arbitration clause under Illinois Law was enforceable as customer did not have to accept service agreement, and could have rejected the compelled arbitration clause by stopping phone service).

164. *Id.*

165. *See, e.g., Hill v. Gateway 2000, Inc.*, 105 F.3d 1147, 1148-49 (7th Cir. 1997).

from the utility to provide electricity at a cost, the acceptance is on the part of the customer saying yes, he or she will pay, and the consideration is payment. However, a brief discussion of the acceptance and consideration is warranted.

For the most part, these service agreements take the form of contracts of adhesion. A contract of adhesion is a standard form contract, prepared by one party, and given to the other party on a take-it-or-leave-it basis. The signing party has little to no choice about the terms. "An adhesion contract is generally a form agreement submitted to a party for acceptance without any opportunity to negotiate terms" and is "generally lawful."[166] A contract for electricity would fall under this category, as customers have to pay for their service or their electricity delivery will be terminated. They do not have a choice of terms.

Contracts of adhesion are accepted if the agreeing party continues to use the service or product that is subject to the service agreement. Where a party has ample time to reject an offer, continued use of the service or product will be deemed to be acceptance.[167] Thus, in our modified contract of adhesion, the continued acceptance of electricity service without opting-out of the data disclosure is acceptance and consent. The utility does not need a wet signature or click-wrap procedure for the data-disclosure provision, because the customer has a choice to consent.

Consideration is not necessary for the consent clause in the service agreement. If consent to disclose customer data is part of the service agreement, then the contract is valid, even though there is no consideration or offer for a specific clause of the contract.[168] Therefore, if the disclosure agreement is included in the service agreement, and there is no specific offer or consideration for the disclosure, the clause will still be upheld if challenged for these reasons. Because of the ease of including this in the service agreement, and the fact that a service agreement with a disclosure clause and opt-out provision will be the easiest case to have ample, valid consideration, this is likely the preferred route for utilities to gain consent to disclose energy-use data.

---

166. *Endsley v. City of Chi.*, 745 N.E.2d 708, 717 (Ill. App. 2001) (citation omitted).

167. *Boomer* at 415 (7th Cir. 2002) (In *Boomer,* the customer challenged a binding arbitration clause, which took effect if the customer continued to use the services. He sued AT&T, and when they tried to compel arbitration, Boomer said it was an unconscionable clause. Boomer continued to use AT&T's long-distance service, even when he filed suit. Despite the lack of other long-distance options, the Seventh Circuit held the clause enforceable and agreed to by Bonner.) *See also, Gateway* at 1148-49 (7th Cir. 1997) (*Gateway* was a similar case, save for the acceptance was conditioned on the continued use of a computer for more than 30 days.).

168. *All Am. Roofing, Inc.*, at 689 (Ill. App. 2010) (where a choice of law clause was included in an insurance contract, it was not invalid to due the lack of consideration for that clause or the lack of a specific offer of the clause).

3. Elements that could invalidate the service agreement

The service agreement is susceptible to the same challenges as any other contract. In Illinois, for example, the Illinois Commerce Commission holds jurisdiction over electricity delivery by for-profit entities and reviews contracts for unconscionability with especial care because electricity is an "essential service."[169]

C. Contracts Between Consumers and Third Parties

The Green Button Initiative has already developed a method of transferring extremely granular data from utilities to customers, who, in turn, transfer that data to third parties.[170] Green Button is an industry response to a call from the White House to help individual customers understand their energy usage and to reduce their consumption. Customers can chose to share the data with EESPs on an individual basis. Customers alike receive a standard format text file from the utility, which contains energy-use data. Under the Green Button framework, customer downloads his or her data and provides it to the third party.

Third-party developers under the Green Button framework already have consent clauses in their terms of service.[171] Customers consent to developers using their data after the customer has licensed the data to the developer. A utility could easily write terms similar to those found in the contracts used in the Green Button Initiative. Drafters of these consent contracts should look to language used in Green Button and pay attention to any impending legal challenges to those contracts.

This Green Button framework can be expanded in order for utilities to release data on a much larger scale. There are many third-party developers who can then use that data to market ways to reduce energy usage to the customer. The program and framework would be easily implemented on a larger scale if the utilities could secure consent. The process could then be streamlined and automated so that utilities could send these standard data files to

---

169. *See, e.g., Geary v. Dominick's Finer Foods,* 544 N.E.2d 344, 348 (Ill. 1989) ("termination of [electric] service would produce disastrous results") (citing *Ross v. Geneva*, 373 N.E.2d 1342, 1346 (Ill. 1978)).

170. *Help You Find and Use Your Energy Data*, GREEN BUTTON, http://www.greenbuttondata.org/ (last visited Dec. 17, 2015); *see also* Lydersen, *supra* note 30.

171. *See Privacy and Security*, LEAFULLY, https://leafully.com/about/privacy/ (last visited May 12, 2015); *Terms and Conditions for GreenButtonConnect.com*, GREEN BUTTON, http://www.greenbuttonconnect.com/home/tou (last visited May 12, 2015) ("3.2 Right to Create and Use Anonymous and Aggregate Data. By using the Service, you expressly authorize Tendril to create from the Information we collect non-personally identifying anonymous or aggregate data and to use and disclose such anonymous or aggregate data in a non-personally identifiable manner. Tendril owns all right, title, and interest in and to the anonymous and aggregate data it creates").

the third parties and bypass the customer, thereby reducing transaction costs and speeding the flow of data to third-party entrepreneurs.