REGULATING THE USE AND SHARING OF ENERGY CONSUMPTION DATA: ASSESSING CALIFORNIA'S SB 1476 SMART METER PRIVACY STATUTE

*John R. Forbush**

I. INTRODUCTION

The rise of digital technologies has permanently altered how human beings interact, communicate, and function in the modern world. The marriage of enhanced data processing and internet-based communication enables average citizens and industry to easily access information and efficiently marshal control over complex systems in the physical and virtual world. While these advances have led to breakthroughs in efficiency, convenience, and an ability to tap new markets, the ubiquity of networked digital applications raises questions regarding the loss of individual autonomy, anonymity, and privacy to faceless, unaccountable corporate and government databases. In 2010 alone, both Google, Inc. and Facebook, arguably the world's leading providers of personalized web-based services, acknowledged inappropriate (and potentially illegal) collection of personal data as well as unauthorized dissemination of user information to third parties.[1] Increasingly, networked devices and services that purport to better our lives are being used as portals to collect data about our preferences, behavior, and lifestyles.[2]

Over the next decade, technological changes in the electricity sector will force utilities, regulators, and ratepayers to balance the availability of powerful new capabilities and service offerings with legitimate concerns about consumer privacy. Through what is

* Senior Editor; J.D. Candidate, Albany Law School, 2012.

[1] In 2010, Google admitted to accidentally collecting email messages and passwords as it collected pictures for its StreetView mapping service, while Facebook shared user information with internet marketing companies without first obtaining user permission. Eric Pfanner, *E.U. Says It Will Overhaul Privacy Regulations*, N.Y. TIMES, Nov. 4, 2010, http://www.nytimes.com/2010/11/05/technology/05privacy.html?emc=tnt&tntemail1=y.

[2] *See, e.g.*, LAWRENCE LESSIG, CODE: VERSION 2.0 219 (2006) ("Some 92 percent of [websites] collect personal data from web users, which they then aggregate, sort, and use.").

currently referred to as the "smart grid," electric utilities will be given access to detailed and granular electricity consumption information as a means to improve service reliability, reduce generation costs through reductions in "peak demand," and accommodate the introduction of renewable energy sources and plug-in electric vehicles into the nation's energy portfolio.[3] The U.S. government adopted the creation of a more efficient and reliable electric grid in the Energy Independence and Security Act ("EISA") of 2007 and has since directed nearly $4 billion in federal funding for smart grid technology deployments and demonstration projects.[4] The key to enabling this vision of a "smarter" grid lies in achieving three overarching capabilities: (1) activating communication and digital sensors with capabilities to automate the electricity distribution and transmission systems, (2) providing digitally enhanced metering systems for all customers, and (3) linking direct interfaces between metering systems and customers through "home area network" technologies.[5]

From a privacy perspective, there are concerns that, in the course of helping grid operators establish real-time situational awareness over large swaths of the electric power system, these so-called "smart" technologies will also be collecting, aggregating, and reporting detailed energy consumption information from individual residences.[6] The potential for utilities and other vendors to collect and aggregate energy consumption data from individual homes and businesses raises significant questions about the access, use, and ownership of energy consumption information.[7] Although electric utilities have long accessed customer energy usage for billing purposes, the collection of energy consumption data has not previously raised privacy concerns because (1) electrical meters had

[3] ASHLEY BROWN & RAYA SALTER, GALVIN ELEC. INITIATIVE, SMART GRID ISSUES IN STATE LAW AND REGULATION 3 (2010), *available at* http://www.galvinpower.org/sites/default/files/SmartGridIssuesInStateLawAndRegulation_Whitepaper_Final(1).pdf.

[4] Energy Independence and Security Act ("EISA") §§ 1301–06, 42 U.S.C. §§ 17381–86 (2007); American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, 138 (2009).

[5] NAT'L CONSUMER LAW CTR. ET AL., THE NEED FOR ESSENTIAL CONSUMER PROTECTIONS: SMART METERING PROPOSALS AND THE MOVE TO TIME-BASED PRICING 1 (2010), *available at* http://www.nclc.org/images/pdf/energy_utility_telecom/additional_resources/adv_meter_protection_report.pdf.

[6] ELIAS LEAKE QUINN, COLO. PUB. UTIL. COMM'N, SMART METERING & PRIVACY: EXISTING LAW AND COMPETING POLICIES 9 (2009), *available at* http://www.dora.state.co.us/puc/docketsdecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-SmartGridPrivacy.pdf.

[7] *Id.* at 15.

to be physically accessed to obtain usage data directly from buildings, (2) traditional meters recorded energy usage over longer time periods and were not capable of collecting the type of granular, appliance specific data possible with smart meters, and (3) under the traditional model, utilities have not had the means nor the economic incentive to share consumer energy consumption data with third party vendors and others.[8]

Recognizing that the collection and storage of data derived from smart meters and appliances raises potential for surveillance of customers and related "physical, financial, and reputational risks,"[9] California recently became the first U.S. state to establish guidelines and protections for the collection and treatment of energy consumption data.[10] California Senate Bill ("SB") 1476 requires aggregators of energy consumption data to obtain consumer consent before sharing customer information with third parties; mandates that third parties may only have access to such data when they are contracting with the utility to provide energy management-related services; stipulates that data be kept secure from unauthorized parties; and mandates that electricity ratepayers "opt in" to authorize any sharing of their energy consumption data for any "secondary commercial purpose[s]."[11] In an effort to spur investment, SB 1476 provides protections for utilities regarding liability of third party service providers and establishes a clear right to continue using customer information once ratepayer consent is obtained.[12] Outside of California, there is a dearth of regulation providing guidance on how to treat energy consumption data in the private and public sectors.[13] Assuming the role of legal and policy "laboratory" for the nation, the California smart meter privacy law will serve as a model and case study for state and federal policymakers as smart grid technology proliferates and its capabilities evolve.[14]

---

[8] NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 9 (2010) [hereinafter NIST 2010 PRIVACY REPORT], *available at* http://www.smartgridinformation.info/pdf/3000_doc_1.pdf.

[9] *Id.* at 13.

[10] CAL. PUB. UTIL. CODE §§ 8380–81 (West 2011); BROWN & SALTER, *supra* note 3, at 32.

[11] PUB. UTIL. §§ 8380–81.

[12] *Id.*

[13] *See, e.g.*, David Greising, *Promise and Peril in Utilities' Smart Grid*, N.Y. TIMES, May 28, 2011, http://www.nytimes.com/2011/05/29/us/29cncgreising.html?emc=tnt&tntemail1=y ("Before ComEd's customers pay for a smart grid in Illinois, regulators and lawmakers should insist that ComEd disclose what it plans to do with the information it collects from customers, and how much ComEd is likely to profit from the data.").

[14] *See* Gonzales v. Raich, 545 U.S. 1, 42–43 (2005) (O'Connor, J., dissenting) (lamenting the

The aim of this article is to analyze California's SB 1476 from a privacy perspective, assessing whether and how this statute will impact the energy efficiency goals of the smart grid movement, and evaluate the law's suitability for wider adoption in other jurisdictions. Section II of the article explains what is meant by the term "smart grid" and will review the energy efficiency and economic rationales supporting smart grid implementation. Section III will explore the attendant privacy concerns raised by smart grid technology. Section IV will provide an overview of the origins and current state of privacy law in the United States. Section V will examine the provisions and record of the Gramm-Leach-Bliley ("GLB") Act, a law passed by the U.S. Congress to regulate treatment of consumer financial information. GLB's privacy provisions will then be compared with California's approach to regulating smart grid information in order to develop a normative ideal of what future privacy regulations in the energy space should aspire towards. Section VI will examine California's SB 1476 smart grid privacy statute in detail and assess its impact on four key areas of privacy protection law: (1) limits on data sharing, (2) disclosure of privacy practices, (3) opting out, and (4) data security requirements.[15] This section will compare the California privacy law with Gramm-Leach's impact on the same areas of information privacy regulation and evaluate the effectiveness and suitability of each in the smart grid arena. Finally, the article's conclusion will advocate that a national standard modeled after aspects of the California law be adopted in order to set minimum consumer protections for energy consumption data. A national approach is preferable to a patchwork of state regulations because the nature of electricity and consumer consumption data allows these commodities to be easily transmitted, stored, and traded across state lines. A national regulatory model would provide consumers greater transparency to evaluate the trade-offs of giving their utility access to their energy consumption data and would establish clear standards for smart grid component manufacturers to innovate and operate within.

Court's decision to strike down California's legalization of medical marijuana on the basis that states should be laboratories for public policy).

[15] Chris King, *California's New Landmark Smart Meter Privacy Law*, EMETER (Sept. 30, 2010), http://www.emeter.com/2010/californias-new-landmark-smart-meter-privacy-law/.

II. WHAT IS THE SMART GRID AND WHY IS IT NEEDED?

It is a truism of the electric power industry that our nation's twenty-first century economy runs on a twentieth century electric grid.[16] Today, through a system that appears remarkably similar to what was envisioned by Thomas Edison and Nicholas Tesla a century ago, electricity is generated at large-scale power plants, transmitted over high-voltage wires to distribution substations, and distributed to customer homes or places of business where it is instantaneously consumed.[17] The modern grid is, in many ways, rather dumb. "The flow of energy and information is predominately static and one directional, from the generators to the consumer," which prevents operators from responding in real-time to fluctuations in consumer demand or disruptions in service.[18] In today's grid, energy and information each flow in a single direction, opposite from one another: energy is sent to the energy customer while daily, weekly, or monthly usage data flows back to the utility for billing purposes.[19] While the reliable and secure delivery of a commodity as valuable and unstable as electricity remains a marvel of human ingenuity, the reality is that much of the grid's antiquated technology is ill equipped to meet the complex energy challenges of the twenty-first century.[20]

While the cost of producing electricity is variable throughout a given day, electric utilities charge the same average rate for electricity throughout because they do not presently have the capability to communicate the actual cost of electricity production to ratepayers.[21] This is a costly problem because electricity generation is most expensive during "peak load" periods, when the demand for

---

[16] *See, e.g.*, *Proceeding on Motion of the Commission to Consider Regulatory Policies Regarding Smart Grid Systems and the Modernization of the Electric Grid*, 2010 N.Y. ST. PUB. SERV. COMM'N 1, 4 [hereinafter NYS PUBLIC SERVICES HEARING—SEPT. 15, 2010], http://nyssmartgrid.com/download/thoughts/psc_responses_to_the%20questions-final.pdf ("The electric grid, as we currently know it, is for the most part very much the same infrastructure that has been in place for the last 50+ years.").

[17] M. Granger Morgan et al., *The Many Meanings of "Smart Grid,"* CARNEGIE MELON U. RES. SHOWCASE (Dep't of Engineering & Pub. Pol'y), July 1, 2009, at 1, *available at* http://repository.cmu.edu/epp/22.

[18] NYS PUBLIC SERVICES HEARING—SEPT. 15, 2010, *supra* note 16, at 4.

[19] *See id.*; *see also* M. Granger Morgan et al., *supra* note 17, at 1–4 (discussing an understanding of today's grid system at various levels).

[20] U.S. DEP'T OF ENERGY, THE SMART GRID: AN INTRODUCTION 5 (2008) [hereinafter THE SMART GRID], http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf.

[21] M. Granger Morgan et al., *supra* note 17, at 1.

electricity approaches the system's overall production capacity.[22] Since electricity is a unique commodity that must be consumed the instant it is produced, electric utilities often will utilize "'peaker plants,'" which tend to be less energy and cost efficient, "when energy demand threatens to exceed supply levels."[23] Since "system reliability," meeting the public's demand for electricity with adequate supply,[24] is the highest priority of the electric industry,[25] "utilities invest in quickly dispatchable generation resources that are only used when required" and "[t]hese peak resources are very expensive and used irregularly."[26]

Therefore, in order to more evenly distribute the demand for power throughout the day, a primary motivator for smart grid is the enabling of "dynamic pricing," which would effectively allow utilities to charge ratepayers more for using power during peak periods of demand and less during times of lower demand.[27] The smart meter technology would allow utilities to communicate price fluctuations to the customer's home throughout the day.[28] In addition to receiving variable price information, smart meter technology will enable users to program "home area networks" to run certain "smart appliances" only when the cost of electricity reaches a pre-determined price.[29] Research of "dynamic pricing" demonstrates that real-time pricing feedback empowers customers to make energy consumption decisions based on the trade-offs of individual household economics, which in turn assists the utility reduce the

---

[22] *Id.*

[23] THE FUTURE OF PRIVACY FORUM, INFO. & PRIVACY COMM'R, ONT., CAN., SMART PRIVACY FOR THE SMART GRID: EMBEDDING PRIVACY INTO THE DESIGN OF ELECTRICITY CONSERVATION 5 (2009) [hereinafter SMART PRIVACY], http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf.

[24] The North American Electric Reliability Corporation ("NERC"), an industry-funded standard setting organization for electric utilities in the United States, Canada, and Mexico, defines reliability as the ability "to meet the electricity needs of end-use customers even when unexpected equipment failures or other factors reduce the amount of available electricity." *See* NERC COMPANY OVERVIEW: FAQ, http://www.nerc.com/page.php?cid=1|7|114 (last visited Oct. 19, 2011).

[25] *See* SMART PRIVACY, *supra* note 23, at 3.

[26] Elias L. Quinn & Adam L. Reed, *Envisioning the Smart Grid: Network Architecture, Information Control, and the Public Policy Balancing Act*, 81 U. COLO. L. REV. 833, 848 n.44 (2010) (citing DAN YORK ET AL., AM. COUNCIL FOR AN ENERGY-EFFICIENT ECON., EXAMINING THE PEAK DEMAND IMPACTS OF ENERGY EFFICIENCY: A REVIEW OF PROGRAM EXPERIENCE AND INDUSTRY PRACTICE iii (2007)).

[27] OFFICE OF ELEC. & ENERGY RELIABILITY, U.S. DEP'T OF ENERGY, *Demand Response* [hereinafter *Demand Response*], http://energy.gov/oe/technology-development/smart-grid/demand-response (last visited Oct. 28, 2010); SMART PRIVACY, *supra* note 23, at 9.

[28] SMART PRIVACY, *supra* note 23, at 8.

[29] *See* Quinn & Reed, *supra* note 26, at 843 n.25; *Demand Response*, *supra* note 27.

overall strain on the power system during peak load.[30] Similarly, smart grid technology will allow utilities to adopt demand side management techniques such as "shedding," a process in which the utility, with the consumer's consent, can send a signal to an air conditioner or water pump that would temporarily shut down or decrease output during peak usage.[31]

The rationale for a "smarter grid" is that incorporation of information technologies into the existing system will enable customers to make more efficient energy choices and to enhance operators' situational awareness throughout the system.[32] In turn, the grid will facilitate efforts to bring distributed generation resources, plug-in electric vehicles, and intermittent renewable energy sources (such as solar or wind power) online while improving overall system reliability, efficiency, and security.[33] Rather than being a single product or service, the term smart grid refers to a collection of technologies and capabilities that will lead to more efficient and reliable use of electric power.[34] Certain features of the smart grid will be designed for the sole or discrete use of electricity customers, utilities, or even third party vendors.[35] This paper will focus on the implications of "two-way communications, real-time [smart] meters . . . appliance controls and other products [that] have the potential to make electricity use far more efficient"[36] upon consumer privacy and the state of California's recent legislative effort to prevent and mitigate future adverse privacy events.

III. PRIVACY CONCERNS ABOUT SMART GRID

In light of reliability and efficiency deficiencies in the modern electric grid, many have advocated installation of advanced metering infrastructure to enable demand side management and demand response capabilities.[37] "[S]mart grid information is useful for facilitating demand response initiatives and the development of

---

[30] *See Demand Response*, *supra* note 27.

[31] M. Granger Morgan et. al., *supra* note 17, at 2 ("'[S]hedding' as little as 5% of the load can halve the need for expensive peaking generation. Since more than 5% of total load is being wasted . . . on activities such as washing dishes and clothes that can easily be shifted to periods when electricity usage is low, the cost to customers is minimal.").

[32] *See id.*

[33] *See* Mariusz Swora, *Intelligent Grid: Unfinished Regulation in the Third EU Energy Package*, 28 No.4 J. ENERGY & NAT. RESOURCES L. 465, 468–69 (2010).

[34] *See* THE SMART GRID, *supra* note 20.

[35] *See id.* at 10–23.

[36] BROWN & SALTER, *supra* note 3, at 3.

[37] QUINN, *supra* note 6, at 3–5.

new business models in the nascent energy management industry."[38] While the "as advertised" environmental and efficiency benefits of smart grid technology are clear, the push to collect more information about utility customers' activities in the home may raise palpable consumer privacy concerns. The sheer amount and specificity of data collected from "smart" electric applications can "reveal much more detailed information about the activities within a dwelling or other premises than was [possible] in the past."[39] To enable demand response, advanced metering infrastructure and other smart devices will provide utilities with more "granular" customer energy usage information than previously possible under the traditional distribution-focused grid and monthly meter reading systems.[40] Placing these new and powerful technologies throughout the grid and inside customers' homes will allow utilities to access more frequent "meter readings," correlate usage information with individual home appliances,[41] and monitor the battery charge time and charge location of plug-in electric vehicles ("PEV") and other plug-in portable devices.[42] "The proprietary business information of non-residential customers could also be revealed through the release of energy consumption data, [possibly risking] competitive harm."[43] Consumer advocates and data security experts caution that collection of detailed energy consumption data will allow data aggregators—utilities, third party service providers, and outside data marketers, each hungry for a new source of customer data—to glean information about the in-home activities, preferences, and potentially, even the travel patterns of energy customers.[44]

Beyond any general apprehension over allowing service providers access to detailed information about ratepayers' home lives, most opposition and, incidentally, law surrounding smart grid and

[38] *Id.* at 1.

[39] NIST 2010 PRIVACY REPORT, *supra* note 8, at 13.

[40] *Id.* at 11–12.

[41] Application of "non-intrusive appliance load monitor" ("NALM") technology allows utilities to distinguish "load signatures" of individual household appliances. "[A] NALM is capable of providing utilities or researchers with detailed information about the electricity consumption habits of residents. . . . [A] remarkable number of electric appliances can be identified by their load signatures, and with impressive accuracy." Elias Leake Quinn, *Privacy and the New Energy Infrastructure*, 23–24 (Ctr. for Energy and Envtl. Sec., Working Paper No. 09001, Fall 2008).

[42] NIST 2010 PRIVACY REPORT, *supra* note 8, at 14–15.

[43] U.S. DEP'T OF ENERGY, DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES 2 (2010) [hereinafter SMART GRID TECHNOLOGIES], Oct. 5, 2010, http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf.

[44] *See* SMART PRIVACY, *supra* note 23.

privacy stems from a recognition of the potential for commercial application of energy consumption data outside of the energy context. For example, there may be opportunity for insurance underwriters to leverage consumption data in setting premiums according to "correlative relationships between . . . appliance uses or load profiles and health or driving risks." Information about personal habits and the use of consumer products may useful to an advertiser's direct marketing efforts. Perhaps most unsettling, the government may find use for smart grid data as a surveillance tool to investigate whether illegal activities are occurring inside a dwelling.[45] Others have warned that this data could be vulnerable to outsiders with more malicious intentions such as hackers.[46] California's SB 1476, the only state law to regulate the handling of smart grid data as of early 2011, imposes no restrictions on a utility's ability to access and retain ratepayer energy consumption data, instead regulating only the transfer of data between the utility and its business parties and the use of the data by third parties for a "secondary commercial purpose."[47]

For many, corporate and government access to details about the daily routines of citizens represents an unprecedented violation of the traditional "sanctity of the home" ideal.[48] Types of behavior that can be derived from energy consumption data include "whether a house has an alarm system and how often it is activated; when occupants usually shower, [] how often they wash their clothes," and whether an electric vehicle is being charged at home, work, or an acquaintance's home.[49] Although it is rare for "a single piece of information or a single source [to] permit the identification of an individual or group of individuals," SSNs and credit card numbers being noteworthy exceptions,[50] several studies have raised the

[45] *See* QUINN, *supra* note 6, at 5.

[46] "Given the degree of seriousness that the Obama administration is applying to cybersecurity and the smart grid, we can look forward to the kind of things happening here that happened to Brazil, where hackers successfully brought down the power." Kim Zetter, *Feds' Smart Grid Race Leaves Cybersecurity in the Dust*, WIRED.COM, Oct. 28, 2009, http://www.wired.com/threatlevel/2009/10/smartgrid/ (quoting Richard Clarke, CEO of the security consulting firm Good Harbor).

[47] CAL. PUB. UTIL. CODE § 8380(c), (e)(2) (West 2011).

[48] "[Just as] we do not expect the postman to look inside our windows when he is delivering the mail, or the cable person to monitor the TV shows we watch . . . so too do customers not expect there to be any surreptitious profiling of their in-home energy-related behavioral patterns." SMART PRIVACY, *supra* note 23, at 3, 10.

[49] Brian Krebs, *Experts: Smart Grid Poses Privacy Risks*, WASH. POST, Nov. 18, 2009, http://voices.washingtonpost.com/securityfix/2009/11/experts_smart_grid_poses_priva.html.

[50] NIST 2010 PRIVACY REPORT, *supra* note 8, at 25.

possibility that a single piece of anonymized data (e.g., date of birth, gender, zip code) may be correlated with other easily accessible information to reveal a specific smart meter user's identity.[51] These possibilities raise concerns regarding how energy consumption information will be collected, used, and shared. From a legal standpoint, there is a tension between providing consumers with greater protections and the risk deterring innovation in a market with the potential to address a myriad of energy-related challenges.[52]

Smart grid's success is dependent on the willingness of energy customers to participate. However, customers may become increasingly leery of smart grid services if they are concerned that their electric utility will share personal energy consumption data with database and telecommunications networking firms as a matter of course in operating these systems.[53] If information sharing between corporate entities is inevitable, then legal protections and rights must be built in and stated unambiguously from the outset in order for customers to willingly participate and remain enrolled as the system continues to evolve. A lack of customer confidence in the security and use of their data may undermine the business case for and overall impact of smart grid technology.[54] The Department of Energy has echoed the importance of earning ratepayers' trust and buy-in to the technology, stating that "[t]he ultimate success of the Smart Grid depends on the effectiveness of these devices in attracting and motivating large numbers of consumers."[55]

IV. PRIVACY LAW IN THE UNITED STATES

The underpinnings of American privacy law begin with Louis

---

[51] *Id.*

[52] *See* Jeff St. John, *Smart Grid Data: Too Much for Privacy, Not Enough for Innovation?*, GIGAOM (Mar. 22, 2010), http://gigaom.com/cleantech/smart-grid-data-too-much-for-privacy-not-enough-for-innovation/.

[53] *See* NYS PUBLIC SERVICES HEARING—SEPT. 15, 2010, *supra* note 16, at 77 (containing the response of the New York State Consumer Protection Board).

[54] *See* Quinn & Reed, *supra* note 26, at 833 ("[T]he interstate market for consumer usage data [is] a unique source of innovation within the electric industry, as well as an example of the opposing interests [(consumer privacy and information access)] that regulators will need to balance.").

[55] Erica Watson-Currie, *Blowback Attack: The Smart Grid's Greatest Danger?*, SMARTGRIDNEWS (Feb. 9, 2010), http://www.smartgridnews.com/artman/publish/Business_Strategy/Blowback-Attack-The-Smart-Grid-s-Greatest-Danger-1875.html (quoting U.S. DEP'T OF ENERGY, THE SMART GRID: AN INTRODUCTION 15 (2009)).

Brandeis and Samuel Warren's *The Right to Privacy*, an 1890 article published in the *Harvard Law Review* arguing in favor of recognizing a new common law tort for invasion of privacy. The authors' proposal was a response to the so-called "yellow journalism" of the day and its increasing use of flash photography to intrude on the private lives of citizens.[56] The authors' "right to be let alone" focused primarily on deterring the unauthorized use of a person's likeness for commercial gain.[57] However, the piece also articulates the well-documented and still ongoing tension that arises whenever new technology that makes it easier to record and document individual behavior bumps up against the status quo's conception of "personal space." The authors presciently feared that, as technology continued to evolve, ever-increasing slices of citizens' intellectual expressions and explorations would be vulnerable to unauthorized access and disclosure.[58] Brandeis and Warren viewed the right "to be let alone" as both a fundamental tenet of individual liberty as well as a critical component to a viable democracy. They feared that unauthorized disclosure of controversial thoughts and ideas would have a chilling effect on the freedom of expression.[59] While monitoring the use of electric appliances may not risk chilling free speech, Warren and Brandeis would likely view the disclosure and subsequent aggregation of intimate details from the home—"a word hitherto sacred among us"—as an ill-conceived step toward a less democratic society.[60]

Similar to the widespread availability of flash photography in Brandeis and Warren's day, the advent of digital technologies, enhanced computing power, and the Internet pose challenges to today's notions of privacy. "On one hand, [the Internet] appears to offer great freedom and anonymity. On the other, it ferrets out and stores everything from our most banal behaviors to our deepest

---

[56] "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[57] "For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons . . . ." *Id.* at 195.

[58] "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." *Id.* at 198.

[59] *Id.* at 195, 198.

[60] *Id.* at 202 n.1. "The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands." *Id.* at 220.

secrets."[61] In recognizing both the emerging promise and dangers of information collection, aggregation, and storage capabilities,[62] the U.S. Department of Health, Education, and Welfare ("HEW") chartered the landmark *Records, Computers, and Rights of Citizens,* a report that established five principles of information privacy for all federally owned "automated systems" that were capable of collecting and storing the personal information of citizens:

1) There must be no personal-data record-keeping systems whose very existence is secret.
2) There must be a way for an individual to find out what information about him is in a record and how it is used.
3) There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
4) There must be a way for an individual to correct or amend a record of identifiable information about him.
5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[63]

Now referred to as the Fair Information Practice Principles ("FIPs"), these five principles were encapsulated in the Privacy Act of 1974—applying the report's principles to the federal government's handling of personal information[64]—and have since become the "internationally accepted standard for what constitutes adequate privacy protection."[65] While no statute mandates that the

[61] Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439 (2011).

[62] "Computers linked together through high-speed telecommunications networks are destined to become the principal medium for making, storing, and using records about people." U.S. DEP'T OF HEALTH, EDUC., & WELFARE, SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., *Foreword* to RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973) [hereinafter 1973 HEW Report].

[63] *Id.* at 41.

[64] Privacy Act of 1974, Pub. L. No. 93-579, § 552(a), 88 Stat. 1896 (1974); *see* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶ 42 (2001).

[65] Hirsch, *supra* note 61, at 455–56; *see also* Rotenberg, *supra* note 64, at ¶ 44 ("The most well known . . . international guidelines are the [OECD's] Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data . . . [which] set out eight principles for data protection that are still the benchmark for assessing privacy policy and legislation . . . .").

private sector follow FIP principles, these standards will continue to inform privacy considerations in a variety of contexts, including the smart grid space.

The concerns raised by Brandeis and Warren remain relevant in a twenty-first century context, "[a]s our expressive activities of thinking, reading, and communicating are increasingly mediated by electronic communications technologies, [and] the number and importance of these sorts of records is expected to increase."[66] However, while the immediate impact of Brandeis and Warren's article was passage of state statutes protecting control over personality rights,[67] the United States has since been hesitant to set universal legal guidelines over private handling of "personal information." The history of privacy regulation in this country has been characterized by a series of one-off initiatives to close privacy gaps in specific sectors, a heavy reliance on industry self-regulation, and a reticence by Congress to overburden private industry with too many privacy-motivated restrictions.[68] "In the United States, . . . private sector compliance with FIPs principles [laid out in the 1973 HEW Report], while increasing, is mostly voluntary and sporadic."[69]

California's SB 1476 must be understood in the context of California's unique consumer privacy regime, as California is the state with the strongest privacy protection standards in the nation.[70] California is the first state to have an office dedicated solely to protecting consumer privacy[71] and the state has been a leader in passing privacy protection statutes that go beyond the

---

[66] Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1347 (2010).

[67] *See, e.g.*, N.Y. CIV. RIGHTS LAW § 50 (McKinney 2010) ("A person . . . that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person . . . is guilty of a misdemeanor.").

[68] *See, e.g.*, Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 714 (2010) ("Information-privacy regulation in the United States is most often identified with discrete, sector-specific statutory schemes governing the treatment of personally identifiable information, such as HIPAA, the regime governing data in the health sector.").

[69] Robert Gellman, *Fair Information Practices: A Basic History* 8 (Working Paper Version 1.85, 2011), http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

[70] *See California Financial Information Privacy Act: Senate Bill 1*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/ar/SB1Info.htm (last visited Oct. 21, 2011).

[71] The California Office of Privacy Protection opened in 2001, with a "mission . . . to identify consumer problems in the privacy area and encourage [the development of] fair information practices." *About the California Office of Privacy Protection*, CAL. OFF. OF PRIVACY PROTECTION, http://www.privacyprotection.ca.gov/aboutus.htm (last visited Oct. 21, 2011).

minimum "floor" protections set out in various federal laws.[72] In addition to recognizing a citizen's "inalienable right" to pursue and obtain privacy under the state Constitution,[73] California has established a litany of regulatory compliance measures for database owners that maintain unencrypted personal information.[74] California recognizes that any party who is injured by an unauthorized disclosure of "personal information" may bring a cause of action against either the party who commits the disclosure or fails to promptly notify those affected of an unauthorized security breach resulting in a disclosure.[75] California imposes an obligation on businesses to protect consumer data from unauthorized breaches, to destroy consumer information once it is no longer needed, and to prevent consumer information from being shared with third parties without the consumer's consent.[76] As we will see, this comprehensive privacy regulatory regime informs how the state's smart meter privacy law will be applied to the handling of energy consumption data.

V. PRIVACY PROVISIONS OF THE GRAMM-LEACH-BLILEY ACT

Similar to the requirements imposed on utilities by California's SB 1476, the Gramm-Leach-Bliley Act (GLB) obligates financial institutions to respect the privacy of customers and protect the security and confidentiality of those customers' "nonpublic personal information" by monitoring their sharing of customer information with third parties.[77] Congress passed GLB in the wake of enforcement actions by the FTC and state attorney generals against "several major financial institutions that were selling customer information, including account numbers and other sensitive information, to telemarketing firms . . . charg[ing] customers for additional, unwanted services."[78] Although the federal government

[72] DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW 717 (2d ed. 2006). In passing the California Financial Information Privacy Act (SB1), "the California legislature found that the Gramm-Leach-Bliley Act 'increases the likelihood that the personal financial information of California residents will be widely shared . . . between companies' . . . ." *Id.*

[73] CAL. CONST. art. 1, §1 (West 2011).

[74] California defines "personal information" as an individual's name plus one or more of the following: social security number, driver's license, or California identification card number, financial account numbers, medical information, or health insurance information. CAL. CIV. CODE § 1798.82(e) (West 2011).

[75] *Id.* § 1798.82–1798.84.

[76] *Id.*

[77] 15 U.S.C. §§ 6801–09 (2011).

[78] Ryan L. Waggoner, *Privacy of Personal Information in the Financial Services Sectors of*

has passed numerous laws relevant to consumer electronic privacy,[79] federal privacy laws regulating the treatment of citizen information outside of discrete sectors of the economy tend to focus on protecting citizens from unauthorized government surveillance.[80]

The Congress enacted GLB to regulate the private sector's treatment of personal information within a single, discrete industry (personal finance), a sector-based approach that is consistent with how California has chosen to regulate energy consumption data and with U.S. privacy law in general.[81] Although SB 1476 regulates information privacy in an entirely separate sector of the economy, California's treatment of energy consumption information can be compared to Gramm-Leach's treatment of "nonpublic information" because both statutes impose similar demands and obligations on the respective industry being regulated.[82] Given these parallels, it is useful to examine Gramm-Leach's successes and shortcomings in protecting consumer privacy and facilitating commerce when comparatively evaluating California SB 1476's strengths and weaknesses towards the same ends.

Both GLB and SB 1476 establish protections for data transmitted in a discrete set of business transactions. They regulate when and how consumer information can be shared with third parties and, to varying degrees, they require third party data aggregators to maintain user confidentiality. Finally, both statutes allow electricity and financial services customers varying degrees of control on the issue of with whom their information is shared.[83] From a comparative standpoint, the longevity of GLB (passed by Congress in 1999) provides a track record of jurisprudence and commentary interpreting and applying the law's provisions. This record represents a useful tool to predict how courts and potentially

the United States and Japan: The Gramm-Leach-Bliley Act and the Financial Services Agency Guidelines, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 873, 876 (Winter 2008–09).

[79] The centerpiece of the Gramm-Leach-Bliley Act was a provision that repealed a requirement under the Glass-Steagall and Bank Holding Company Acts, allowing banks, brokerages, and insurance companies to merge. The law's privacy provisions reflected an understanding of the risk of one institution holding a considerable amount of personal financial data. *See* 15 U.S.C §§ 6801–09.

[80] The Electronic Communications Privacy Act ("ECPA") modernized federal wiretap law by setting guidelines for the treatment of oral communications, wire communications, and electronic communications in three contexts: wiretaps, stored communications (primarily email), and pen registries. *See* 18 U.S.C. §§ 2510–22 (2011) (Wiretap Act); 18 U.S.C. §§ 2701–11 (2011) (Stored Communications Act); 18 U.S.C. §§ 3121–27 (2011) (Pen Register Act).

[81] *See* Bamberger, *supra* note 68, at 714.

[82] *See* 15 U.S.C. §§ 6801–09; CAL. CIV. CODE §§ 8380–81 (West 2011).

[83] *Id.*

aggrieved customers may react to rules and protections set out under SB 1476. The next two sections of this article will examine how GLB and SB 1476 regulate four areas of information privacy law: information sharing with third parties, disclosure of information practices to the consumer, customer control over data via "opting out," and the legal obligations of service providers to protect data from unauthorized releases. This GLB analysis will establish baseline standards against which similar provisions of the California smart grid privacy law can be assessed.

A. Gramm-Leach: Sharing Consumer Information with Third Parties

Aside from paving the way for consolidations between investment and depository banking institutions,[84] GLB established ground rules for the collection, sharing, and unauthorized disclosure of "nonpublic" customer financial information by "companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance."[85] GLB broadly defines "nonpublic personal information" as any "personally identifiable financial information—(i) provided by the consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."[86] Under GLB, such "nonpublic information" may be shared between "affiliate companies"—those which are "under common control with another company"—but may not be shared with "nonaffiliated companies" *unless* (1) customers have been provided an opportunity to "opt-out" of such sharing before it occurs, or (2) the nonaffiliated party "perform[s] services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services."[87] Therefore, under the law, customers are not provided an opportunity to "opt-out" of information sharing between affiliated or non-affiliated firms

[84] *See* William R. Gruver, *A Big Regulator for the Little Investor*, N.Y. TIMES, Sept. 13, 2008, http://www.nytimes.com/2008/09/13/opinion/13gruver.html ("[Financial regulation should] start . . . with a re-examination of the Gramm-Leach-Bliley Act of 1999, which removed the 66-year-old separation between commercial banks (the kind that accept deposits and make loans) and investment banks (the kind that underwrite securities).").

[85] BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, IN BRIEF: THE FINANCIAL PRIVACY REQUIREMENTS OF THE GRAMM-LEACH-BLILEY ACT (July 2002), *available at* http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act.pdf. *See also* 15 U.S.C. §§ 6801–6809.

[86] *See* 15 U.S.C. § 6809(4)(A).

[87] *Id.* §§ 6802(b)(2), 6809(6).

who provide services to the primary financial institution. However, even where customers are not given opportunity to opt-out, GLB requires that financial institutions must disclose when customer information has been shared with nonaffiliates and that nonaffiliates are contractually obligated to maintain confidentiality of customer data.[88]

The inability of customers to control the sharing of their "nonpublic information" ("NPI") with affiliate companies as well as the law's exemption for nonaffiliates "perform[ing] services for or functions on behalf of the financial institution[s]" has been the focus of criticism.[89] Although the term "affiliate" may evoke a close business relationship critics have pointed out that "[i]n today's world of mega-mergers, a bank may have over one thousand affiliates, some of which may be completely unrelated to financial services."[90] According to this view, instead of facilitating the sharing of customer information between closely partnered business entities, GLB merely encourages financial institutions to acquire marketing companies as a means of getting around the law's privacy and disclosure requirements. Additionally, privacy advocates perceive GLB's exception permitting the sharing of customer NPI with "nonaffiliates" as severely undermining GLB's opt-out provision, which is discussed below.[91] With such broad exceptions allowing banks to share NPI with a variety of entities—who may or may not even be affiliates or financial companies—GLB has largely failed to create meaningful restrictions against corporate sharing of customer's NPI.

B. Gramm Leach: Information Sharing Annual Reports

While GLB's restrictions on information sharing between banks have been criticized as illusory due to the broad exceptions for affiliates and nonaffiliated service-providers, the law does contain a requirement that financial companies disclose all exchanges of NPI with nonaffiliated institutions to the consumer within a "clear and conspicuous" annual privacy report.[92] "[I]f the institution [does not] intend[] to disclose 'nonpublic personal information' about the

---

[88] *Id.* § 6802(a)–(c).

[89] *Id.* § 6802(b)(2).

[90] *The Gramm-Leach-Bliley Act*, ELECTRONIC PRIVACY INFORMATION CENTER ("EPIC"), http://epic.org/privacy/glba/ (last visited Oct. 21, 2011) [hereinafter "EPIC – GLB"].

[91] *Id.*

[92] 15 U.S.C. § 6803(a)–(c).

consumer to a 'nonaffiliated third party' . . . then no privacy or opt-out notices need to be provided."[93] FTC regulations enforcing GLB characterize a "clear and conspicuous" privacy report as "reasonably understandable and designed to call attention to the nature and significance of the information in the notice."[94] The purpose of these annual reports is to communicate (1) the "categories" of nonaffiliated parties with which a customer's financial data is shared, (2) the financial institution's "policies" regarding use of NPI belonging to individuals who are no longer customers of the bank, and (3) the institution's information protection policies and practices.[95] "The idea of notice under the GLB Act is to convey information that is critical to an individual's decision making" regarding their personal data.[96] GLB defenders have argued that the disclosure provision empowers customers with information about their bank's information practices but that a "principal effect . . . has been to require financial institutions to inspect their own practices . . . [i]n order to draft the [disclosure] notice[s]."[97] While the GLB mandated annual privacy reports may compel corporations to conduct internal audits of their data sharing practices that they would not have pursued otherwise, the law has failed to produce annual reports that are useful in assisting customers choose how their information is utilized.[98]

GLB's critics have pointed out that, while the law calls for reports to disclose the "categories of persons"[99] with which information is shared and the "categories of nonpublic personal information" that is shared, the law would have greater utility for customers if it compelled institutions to provide "a description [of information sharing practices] explicit enough . . . that an individual can reasonably ascertain how the data handling entity will use the information."[100] Similarly, by not requiring financial institutions

---

[93] Therese G. Franzén & Leslie Howell, *Financial Privacy Rules: A Step by Step Guide to the New Disclosure Requirements Under the Gramm-Leach-Bliley Act and the Implementing Regulations*, 55 CONSUMER FIN. L. Q. REP. 17, 18 (2001).

[94] 16 C.F.R. § 313.3(b)(1) (2011).

[95] *See* 15 U.S.C. § 6803(c).

[96] Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1225 (2002).

[97] Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1316 (2002).

[98] *See id.* at 1267–68, 1316 (describing annual reports received by customers, a customer's ability to control how their information is used via opt-outs, and the internal audits conducted by financial institutions in order to provide GLB notices).

[99] 15 U.S.C. § 6803(c)(1).

[100] Waggoner, *supra* note 78, at 887, 889.

"to announce any specific usage for the personal information, but rather just their privacy policies" critics allege that GLB does not encourage banks to transparently communicate how customer NPI is shared outside of their firm.[101] Therefore, when the law's annual privacy report requirement was implemented, firms tended to provide reports that were "general" in nature.[102] Furthermore, "[Congress'] failure to specify any understandable disclosure terms led the financial institutions to mail out large policies that customers were very unlikely to read or understand."[103] GLB's annual reporting requirement is widely perceived as an ineffective means of communicating the implications of corporate data sharing practices[104] and has been criticized as giving short-thrift to the purported legislative goal of informing customers of their rights to opt-out of sharing with unaffiliated third parties, a topic addressed in the next section.[105]

C. Gramm-Leach: Opting-Out of Information Sharing

The aspect of GLB that has received the most attention and criticism has been the law's "opt-out" provision.[106] "First, [Gramm-Leach-Bliley] does not protect consumers. It unfairly places the burden on the individual to protect privacy with an opt-out standard . . . weaken[ing] customer power to control their financial information."[107] Widely recognized as "a congressional attempt to facilitate the efficient [and open] sharing of [consumer] information throughout the financial services industry,"[108] GLB's opt-out exemption permits sharing of customer NPI with nonaffiliated third

---

[101] *Id.* at 889.

[102] *See* SOLOVE ET AL., *supra* note 72, at 714.

[103] Gideon Parchomovsky & Philip J. Weiser, *Beyond Fair Use*, 96 CORNELL L. REV. 91, 129 (2010).

[104] Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, PRIVACY RIGHTS CLEARINGHOUSE, July 1, 2001, http://www.privacyrights.org/ar/GLB-Reading.htm.

[105] A letter sent to various federal regulatory agencies pointing out that, among many other deficiencies, the privacy notices being sent in compliance with Gramm-Leach-Bliley Act ("GBLA") often buried information regarding consumer's rights to "opt-out" at the end of "ten pages of fine print." David Arkush & David C. Vladeck, *Petition for Rulemaking*, PUBLIC CITIZEN LITIGATION GROUP (July 26, 2010), http://www.epic.org/privacy/consumer/glbpetition.pdf.

[106] *See* EPIC – GLB, *supra* note 90.

[107] *Id.*

[108] Steven Robert Roach & William R. Schuerman, *Privacy Year in Review: Recent Developments in the Gramm-Leach Bliley Act, Fair Credit Reporting Act, and Other Acts Affecting Financial Privacy*, 1 I/S: J.L. & POL'Y FOR INFO. SOC'Y 385, 390 (2005).

parties so long as the third-party is an "affiliate" company or a "nonaffiliated" firm performing any number of enumerated "services for or functions on behalf of [a] financial institution."[109] GLB broadly defines the type of services third parties may provide financial companies in order to qualify for exemption from the opt-out requirement.[110] As addressed previously, these activities include, "marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions."[111]

Thus, if a customer reads through her bank's annual "privacy report" and discovers the bank is engaged in objectionable information sharing practices with unaffiliated, possibly unnamed, third parties who are performing "marketing" services on the bank's behalf, the customer will be unable to exercise opt-out rights to prevent her information from being shared.[112] The customer's only recourse will be to find a new financial institution. Therefore, it would seem that GLB's statutory description of the type of privacy notices financial companies are required to provide[113] encourages companies to employ practices designed to discourage—or at the very least, confuse—customers from exercising their right to decline sharing of their data with third party service providers.[114] As stated by Michael Hatch, the Attorney General for the State of Minnesota, "[t]he opt-out notices flooding consumers' mailboxes . . . have not meant much for the typical consumer. The notices are dense and impenetrable."[115]

D. Gramm-Leach: Data Security Requirements

Under authority granted by GLB,[116] the Federal Trade Commission ("FTC") has established the "safeguards rule," which

---

[109] 15 U.S.C. § 6802(b)(2) (2011).

[110] *Id.*

[111] *Id.*

[112] *See id.*

[113] "A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless—(A) such . . . institution *clearly and conspicuously* discloses to the consumer . . . that such information may be disclosed to such third party . . . ." 15 U.S.C. § 6802(b)(1)(A) (emphasis added).

[114] *See* Janger & Schwartz, *supra* note 96, at 1230–32.

[115] *Oversight Hearing on "Financial Privacy and Consumer Protection" Before the S. Comm. on Banking, Housing & Urban Affairs*, 107th Cong. 1 (2002), *available at* http://banking.senate.gov/02_09hrg/091902/hatch.htm (statement of Mike Hatch, Att'y Gen. of the State of Minnesota).

[116] 15 U.S.C. §§ 6801(b), 6805(b)(2).

requires financial institutions to "develop, implement, and maintain a comprehensive information security program" appropriate to risks related to the "size" of the "institution" and "sensitivity of any customer information" being stored.[117] GLB also requires that financial institution nonaffiliates possessing customer data be bound by contract to maintain the data's "confidentiality."[118] In instances where injury has been alleged based on a financial institution's unauthorized disclosure of information, courts have thus far stymied plaintiffs' attempts to bootstrap the security standards set by GLB into a recognizable cause of action for *negligence per se*.[119] Although GLB was never framed as a vehicle for civil actions and the law's text unambiguously assigns the database security enforcement responsibilities to various federal agencies,[120] several plaintiffs have filed common law tort claims for negligence, attempting to use GLB's security provisions as the established "standard of care" that database owners and information aggregators owe to clients.[121] The courts have consistently held that GLB's information security requirements do not create an individual cause of action and are meant only to be administratively enforceable by the FTC and other federal agencies.[122] Although plaintiffs' attempts to sue under GLB for data security violations by financial service providers have thus far been unsuccessful, a regulated entities' noncompliance with the law can result in a $10,000 per infraction fine from the federal government.[123] However, this $10,000 penalty may not be a sufficient deterrent for the financial services companies regulated by the statute.

In general, plaintiffs whose personal data has been breached or disseminated by a data aggregator or service provider can expect

---

[117] 16 C.F.R. § 314.3(a) (2011).

[118] 15 U.S.C. § 6802(b)(2).

[119] *See, e.g.*, Dunmire v. Morgan Stanley DW, Inc., 475 F.3d 956, 959 (8th Cir. 2007) (plaintiff filed suit for negligence per se, breach of contract, and breach of fiduciary duty on the basis that defendant violated GLB when it served plaintiff's estranged wife with a summons containing financial information plaintiff wanted kept confidential).

[120] 15 U.S.C. § 6805(a)(2)–(7).

[121] *See* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 266–67 (2005).

[122] *See* Menton v. Experian Corp., 2003 WL 21692820, at *3 (S.D.N.Y. July 21, 2003); *see also* Borninski v. Williamson, 2004 WL 433746, at *3 (N.D. Tex. Mar. 1, 2004) (holding that plaintiff's claim failed as a matter of law).

[123] Stephanie Francis Cahill, *Cyber Insecurity: Lawyers May be Missing a Big Piece of Gramm-Leach-Bliley*, 1 NO. A.B.A. J. E-RPT. 5 (Dec. 6, 2002) (on file with the Albany Law Review).

courts to recognize their claims as a legitimate "injury in fact" *only if* they experienced "actual or imminent" harm resulting from the unauthorized disclosure.[124] Therefore, plaintiffs who can identify only an "increased risk" of a data breach sometime in the future will typically not survive a defendant's motion to dismiss. Even where courts have recognized a plaintiff's prudential standing to bring a negligence claim against the perpetrator of an unauthorized data disclosure, they have repeatedly "ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy."[125] Others have also raised concern that statutes laying out security requirements for database operators function as poor stand-ins for established "standards of care" in negligence actions. These commentators point out that statutes like GLB are "vague and speak[] of an obligation to protect data security without indicating what must be done to fulfill that obligation."[126] It should be pointed out that in data breaches where injury to an individual has been more tangible than the inconvenience of having to guard against future identity theft, courts have been less reticent to award damages.[127]

VI. SENATE BILL 1476: CALIFORNIA'S SMART METER PRIVACY LAW

While EISA assigned responsibility for development of smart grid security and privacy to the National Institute for Standards and Technology ("NIST") within the Department of Commerce, there is no guarantee these standards will be ratified into law, and even so, NIST's recommendations are more likely to take the form of sweeping principles rather than detailed rules governing the specifics of how business partners should interact.[128] Therefore,

[124] *See* Hammond v. Bank of N.Y. Mellon Corp., 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010). The court granted the defendant's request for summary judgment because, even though defendant lost unencrypted computer back-up tapes containing plaintiff's personal information, the plaintiff's case lacked standing because their alleged injuries were "future-oriented, hypothetical, and conjectural." *Id. See also* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 637 (7th Cir. 2007) ("Indiana law would not recognize the costs of credit monitoring that the plaintiffs seek to recover in this case as compensable damages.").

[125] Shafran v. Harley-Davidson, Inc., 2008 WL 763177, at *3 (S.D.N.Y. Mar. 20, 2008).

[126] Johnson, *supra* note 121, at 269.

[127] *See* Jaikumar Vijayan, *Heartland Payment Systems to Pay $4 Million Compensation After Data Loss*, COMPUTERWORLDUK, May 10, 2010, http://www.computerworlduk.com/news/it-business/20200/heartland-payment-systems-to-pay-4-million-compensation-after-data-loss/.

[128] EISA requires that NIST's final privacy recommendations be submitted to the Federal Energy Regulatory Commission ("FERC"), a federal regulatory agency with jurisdiction over

unless Congress passes a new law governing private sector treatment of energy consumption information, federal smart grid privacy standards will be derived from pre-existing federal statutes that govern information exchanges in the telecommunications, financial, energy, and other sectors of the economy.[129] In response to this regulatory void,[130] the California legislature passed SB 1476 to: (1) "prohibit [private and publicly owned utilities] from sharing, disclosing, or otherwise making accessible to any [third-]party a customer's electrical or gas consumption data, . . . except as specified,"[131] (2) "protect . . . [the customer's personal information] from unauthorized access, destruction, use, modification, or disclosure,"[132] and (3) "ensure that . . . customer[s] [have] an option to access [their energy consumption] data without being required to agree to the sharing of his or her personally identifiable information with a [third-]party."[133]

With SB 1476 becoming state law in January 2011, this section of the paper will (1) evaluate this landmark piece of legislation across four areas of impact (information sharing, disclosure of utility privacy practices, opting out and opting in, and data security), (2) anticipate how legal issues raised by the statute will impact customers, and (3) compare the protection of consumer energy data under the California law with the protection of financial data under the Gramm-Leach-Bliley Act.

---

the nation's interstate electricity transmission networks. *See* Energy Independence and Security Act, 42 U.S.C. § 17382 (2011). It is unclear whether they have the authority to regulate smart grid at the distribution level, traditionally the province of state public utility commissions. *See id.* § 17381.

[129] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2011); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–22 (2011); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09 (2011). Additionally, there is a cybersecurity bill pending in Congress that could affect the treatment of smart grid information by utilities; third parties; and state and federal governments. *See generally* S. 1535, 112th Cong. (2011) (as reported with an amendment Sept. 22, 2011).

[130] "[T]he [California Public Utilities Commission] authorized Southern California Edison to install approximately 5.3 million smart meters, San Diego Gas and Electric Company 1.4 million electric smart meters and 900,000 natural gas meters, and Pacific Gas and Electric Company approximately 5 million electric meters and 4.2 million natural gas meters." *Senate Bill Analysis Before the Senate Energy, Utilities, & Communications Subcommittee*, 2010 Leg., Reg. Sess. (Ca. Apr. 6, 2010).

[131] S.B. 1476, 2010 Leg., Reg. Sess. (Ca. 2010) (Leg. Counsel's Digest) (statement of Sen. Padilla).

[132] *Id.*

[133] *Id.*

A. SB 1476: Limits on Sharing Information with Third Parties

A lasting recommendation of the widely-influential 1973 report, *Records, Computers and the Rights of Citizens* by the U.S. Department of Health, Safety, and Welfare was that, within all "Automated Personal Data Systems," "[t]here must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent."[134] With SB 1476, California attempts to address this tenet of privacy law by prohibiting utilities from "sell[ing] a customer's electrical or gas consumption data or any other personally identifiable information for any purpose," without the consumer's consent.[135] Given smart grid's ability to collect "granular" information about utility customers' energy use habits, the most significant aspect of SB 1476 may be what the California legislature decided not to regulate or restrict: collection and storage of such information by the electric utilities themselves.[136] Objectively, this represents an unsurprising and pragmatic approach from an environmentally progressive state intent on encouraging smart grid technology's long-term viability. Further, since electric utilities have "'always [had access to] information about customers' usage,'" the law recognizes that the electric industry does not have a track record of abusing their privileges to customer data.[137] Rather than restrict what utilities collect about users via smart meters, the law focuses on regulating information sharing between utilities and third parties.

An initial reading of the SB 1476 may give the impression that California is endorsing draconian restrictions on utility operators' ability to share consumer data. "This bill would prohibit [a utility] from sharing, disclosing, or otherwise making accessible to any third party a customer's . . . data . . . *except as specified*."[138] However, that law's "as specified" caveat carves out two important instances when utilities are free to disclose and share customer

---

[134] 1973 HEW Report, *supra* note 62.

[135] CAL. PUB. UTIL. CODE § 8380(b)(2) (West 2011).

[136] *See generally id.* § 8380 (regulating the sharing, disclosing, and selling of consumer consumption data, but not the collection and storage of the data).

[137] Felicity Barringer, *New Electricity Meters Stir Fears,* N.Y. TIMES, Jan. 30, 2011, http://www.nytimes.com/2011/01/31/science/earth/31meters.html?pagewanted=all (quoting David K. Owens, the executive vice president for business operations at the Edison Electric institute).

[138] S.B. 1476, 2010 Leg., Reg. Sess. (Ca. 2010)(Leg. Counsel's Digest) (statement of Sen. Padilla).

energy user information with partnering firms: (1) when a customer gives explicit consent to do so and (2) when "system, grid, or operational needs, or the implementation of demand response, energy management, or energy efficiency programs" require that information be shared with a third party service provider.[139] This second exception for "demand response, energy management, or energy efficiency programs"[140] is essentially a catchall provision, encompassing a large swath of the smart grid's core functionality.

SB 1476 recognizes that utilities will need to contract with third parties possessing telecommunications networking expertise to enable full smart grid functionality, particularly during the nascent stage of smart grid development. Compared with GLB, where third party marketing "nonaffiliates" are permitted access to customer data in exchange for providing the primary *financial institution* with a service,[141] the California law allows third party access to customer data only when *the customer* receives an energy related service from that third party.[142] In this respect, the California law explicitly presumes third party handling of customer information[143] will be a routine characteristic of the state's energy system; "[n]othing in this section shall preclude an electrical corporation . . . from disclosing a customer's electrical . . . consumption data to a third party for system, grid, or operational needs, or the implementation of demand response, energy management, or energy efficiency programs."[144] From the perspective of privacy protection, the SB 1476 provisions that allow for third party sharing are more narrowly tailored than those in Gramm-Leach. SB 1476 requires at a minimum that paying customers receive some sort benefit related to energy service for sharing their energy consumption data. However, like GLB, SB 1476's provisions regulating utility information exchanges with third parties do not exist in a vacuum. Consistent with the values espoused by Brandeis and Warren and the HEW Report, California energy

---

139 PUB. UTIL. § 8380(b)(1), (e)(2).

140 *Id.* § 8380(e)(2).

141 15 U.S.C. § 6802(b)(2) (2011).

142 PUB. UTIL. § 8380(e)(2). Section 8380(b)(1) bars utilities from selling or sharing customer energy consumption data or personally identifiable data for purposes outside those allowed by this statute. *Id.* § 8380(b)(1).

143 SB 1476 defines a customer's "electrical or gas consumption data" as "data about a customer's [energy] usage that is made available as part of an advanced metering infrastructure, and includes the name, account number, or residence of the customer." *Id.* § 8380(a).

144 *Id.* § 8380(e)(2).

customers must be given notice of how their data is being put to use and retain the right to modify or cancel uses they find objectionable.[145]

B. SB 1476: Disclosure of Information Practices and Opting-In

The term "disclosure" means different things to different stakeholders within the privacy and consumer protection communities.[146] For the purposes of this section, unless specified otherwise, "disclosure" can be equated with the privacy notifications a service provider—such as a bank, electric utility, or a website—provides to consumers as a means of *disclosing* the corporation's information collection and sharing practices.[147] In general, privacy notices or reports may be distributed through the mail, a privacy statement may be on a webpage, or a statement may be contained in piece of software downloaded from a compact disk.[148] The purpose of disclosure notices "is to convey information that is critical to [a person's] decision making . . . [regarding his] personal data"[149] and, in sectors where information privacy is actively regulated, disclosure of customer data collection practices is required.[150]

SB 1476 requires disclosure of utility information sharing practices in two circumstances: (1) whenever a utility uses advanced metering infrastructure to "allow[] a customer to access the customer's electrical and gas consumption data," the utility must "ensure that the customer has an option" of accessing this information without sharing their "personally identifiable information . . . with a third party," and (2) whenever a third party is given access to customer data, "the contract between the [utility] . . . and the third party [must require] the third party to

---

[145] The 1973 Report by the U.S. Department of Health, Education, and Welfare noted, in regard to computerized information gathering and storage systems, that "[t]here must be a way for an individual to find out what information about him is in a record and how it is used," and "[t]here must be a way for an individual to correct or amend a record of identifiable information about him." 1973 HEW REPORT, *supra* note 62.

[146] For example, "disclosure" even takes on two meanings within SB 1476, California's smart meter privacy law. Within section 8380(f), the term refers to an individual's authorized release of their own personal information to another party. PUB. UTIL. § 8380(f). However, in section 8380(c) and for this paper's purposes, "disclosure" will refer to a company providing notice to a customer of their privacy practices and policies. *Id.* § 8380(c).

[147] *See* 15 U.S.C. § 6803(c); Janger & Schwartz, *supra* note 96, at 1224–26.

[148] *See* 15 U.S.C. § 6803(a).

[149] Janger & Schwartz, *supra* note 96, at 1225.

[150] *See* 15 U.S.C. §§ 6801, 6803(a)–(b).

prominently disclose[]" to the ratepayer the use of energy consumption data for any "secondary commercial purpose" and to obtain the ratepayer's consent to engage in such "secondary commercial purpose[s]," which are "[un]related to the primary purpose of the contract" between the utility and third party.[151] Section 8380(b)(4), the first and more sweeping of the two provisions provides customers with an opportunity to "opt-out" of information sharing with third parties, and will be addressed in the following section of this article.[152] Conversely, section 8380(e)(2)'s requirement that third parties obtain customer consent before data may be used for "secondary commercial purpose[s]," embraces a more consumer protectionist "opt-in" approach.[153]

The California statute's disclosure requirement is activated only when "[a] third party . . . uses [the ratepayer's data] for a *secondary commercial purpose*," in which case, the third party—not the utility—must "prominently disclose[] that secondary commercial purpose to the customer" and obtain their consent.[154] Although SB 1476 does not define the term "secondary commercial purpose," potential commercial uses for smart meter data include use by "[r]etailers of appliances, extended warranties, or repair services [who] may want data [from advanced metering infrastructure] to provide advertising . . . before an appliance fails," and "[i]nsurers [who] may want to look for evidence of unauthorized conduct, to determine when a loss occurred, or to deduce who was present" during an incident.[155] By placing the onus to disclose "secondary commercial purpose[s]" on the *third party*, section 8380(c) shifts the burden of monitoring third party information practices away from the utility.[156] However, due to California's strict Security Breach Information regime,[157] which obligates owners and licensers of California residents' personal data to "maintain reasonable security

---

[151] PUB. UTIL. § 8380(b)(4), (c), (e)(2).

[152] *Id.* § 8380(b)(4).

[153] *Id.* § 8380(e)(2). "[A]n opt-in system sets the default rule to 'no information flow,' under the presumption that customers harbor greater concern about the risk of information usage than the loss of benefits consequent to shutting off the flow." Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets*, 52 DUKE L.J. 745, 766 (2003).

[154] PUB. UTIL. CODE § 8380(c), (e)(2) (emphasis added).

[155] Mark F. Foley, *The Dangers of Meter Data (Part I)*, SMARTGRIDNEWS.COM, Jun. 2, 2008, http://www.smartgridnews.com/artman/publish/Technologies_Metering_News/The_Dangers_of_Meter_Data_Part_1-446.html.

[156] *See* PUB. UTIL. § 8380(c).

[157] *See generally* CAL. CIV. CODE §§ 1798.80–1798.91 (West 2011) (defining businesses and reasonable disclosure policies).

procedures and practices,"[158] California utilities could potentially face liability for failure to conduct due diligence of a business partner's "secondary commercial purpose[s]" or data protection efforts.[159] SB 1476 thus improves upon GLB's requirement that financial institutions provide "general" privacy policy overviews,[160] by stipulating that customer privacy notices "prominently disclose[]" the precise "secondary commercial purpose" to which the third party vendor is using customer data *and* that the third party first obtain the customer's consent to pursue that secondary commercial use.[161] SB 1476's "prominently disclose[]" language seems specifically designed to avoid the type of vague and confusing information conveyed by financial services companies under GLB.[162] Thus, a third party that neglects to disclose and obtain consent for a "secondary commercial purpose" to which ratepayers' personally identifiable information is used could be held derivatively liable for breach of contract with the utility since they are not under privity of contract with ratepayers.

From a consumer protection standpoint, SB 1476's disclosure and "opt-in" provisions represent the areas of greatest differentiation with GLB. GLB does not contain an "opt-in" measure, instead requiring that individuals be given an ability to opt-out of information disclosure with nonaffiliated third parties.[163] As discussed, financial firms' communication of opt-out rights to the customer has been accused of being at best vague and at worst intentionally duplicitous.[164] Alternatively, SB 1476 requires prominent disclosure of any secondary commercial use by third parties and, furthermore, that the third party obtain the ratepayer's consent to the third party's proposed use.[165] According to Staten and Cate, information privacy laws that "permit an organization's internal use of personal information about customers or members, but [ ] require opt-in consent before personal information [can] be disclosed to third parties" constitute the least burdensome "opt-in" requirements for a regulated business.[166]

---

158 *Id.* § 1798.81.5(b).

159 *See id.* § 1798.81.5(a).

160 *See* SOLOVE ET AL., *supra* note 72, at 714.

161 PUB. UTIL. § 8380(c).

162 *See id.*; *see also* Janger & Schwartz, *supra* note 96, at 1230–32.

163 15 U.S.C. § 6802(b) (2011).

164 *See* Janger & Schwartz, *supra* note 96, at 1230–32.

165 PUB. UTIL. § 8380(c), (e)(2).

166 Staten & Cate, *supra* note 153, at 762. The authors labeled the type of "opt-in" requirement used in SB 1476 as "[t]hird-[p]arty-[s]haring [o]pt-[i]n" and found that it was less

Although SB 1476 marks an improvement over GLB in terms of promoting transparency among utilities and other energy service providers, GLB actually imposes greater restrictions on third parties' ability to use customer data for *any* secondary commercial purpose.[167] In this regard, consumer advocates may be concerned that (1) SB 1476 leaves open the question of how and through what medium third parties are to provide ratepayers with appropriate disclosure notices, (2) SB 1476 fails to define what data sharing activities constitute "secondary commercial purpose[s],"[168] (3) that distribution of privacy notices to customers from a third party companies may cause unnecessary confusion among the general public, and (4) because certain industries have become adept at designing "opt-in questionnaires" in a manner that essentially undermines the spirit of consumer choice and control in which opt-in requirements were developed, questions remain over how strictly SB 1476's opt-in requirement will be construed by courts and regulators.[169]

C. SB 1476: Opt-out Provisions

The third precept of the 1973 HEW Privacy Report called for every database containing information about private citizens to include, "a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent."[170] The term "opt-

burdensome than opt-in regimes that require consent to share customer data among "affiliate" corporations or for any non-stipulated internal use. *Id.* at 762–65.

[167] "[A] nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate . . . disclose such information to any other person that is a nonaffiliated third party . . . ." 15 U.S.C. § 6802(c).

[168] Other efforts to confine the use of consumer data to the purpose to which the consumer intended have tended to embrace a rather broad definition of "commercial purposes." For example, in addressing Congress' intent in enacting the privacy provisions of the GLB, Congresswoman Judy Biggert referenced, "the growing use and sale of consumers' personal information for marketing, profiling and other commercial purposes by banks . . . and other bona fide financial institutions." John Gibeaut, *ABA Sues Over Privacy Statute*, 1 NO. 37 A.B.A. J. E-REPORT 1 (Sept. 27, 2002).

[169] "Some of the largest U.S. companies currently use similarly ambiguous questions to collect and disclose their users' personal information. Companies often create opt-in questions asking whether the consumer would like more information about products or services, rather than a straightforward question." Suzanna Shaub, *User Privacy and Information Disclosure: The Need for Clarity In "Opt-In" Questions for Consent to Share Personal Information*, 5 SHIDLER J. L. COM. & TECH. 18, ¶ 2 (2009), https://digital.lib.washington.edu/dspace-law/bitstream/handle/1773.1/432/vol5_no4_art18.pdf?sequence=1.

[170] 1973 HEW Report, *supra* note 62.

out" refers to "a method by which customers instruct financial institutions to stop certain marketing activities" that make use of the consumer's personal information.[171] Like the GLB, the California smart grid law does not expressly lay out detailed instructions on how utilities "shall ensure that the customer has an option" not to share their data with third party service providers.[172] As noted in the previous subsection, SB 1476 requires "prominent[]" disclosure of information sharing deemed to be the most risky: the use of energy consumption for "secondary commercial purpose[s]" by third party vendors or contractors.[173] However, contrary to the requirement that third parties "prominently disclose[]" the nature of any secondary commercial uses, SB 1476 does not hold utilities to the same standard and fails to delineate the clarity or prominence with which energy companies are to communicate their opt-out notices to ratepayers.[174] The law also fails to indicate how one message from a third party detailing their use of customer information for "secondary commercial purpose[s]" is to be linked with the utility's message regarding the customers' right to opt-out of such third party usage. This is more than a matter of semantics. For a technology still in its infancy, clear statutory lines of direction will allow the industry to focus on innovating where they know they are to operate and will calm any unwarranted fears among the general public. Consumer experience with deceptive tactics and substandard information privacy practices[175] raises questions regarding the viability of a self-regulatory regime in the information privacy context.

Compared with GLB, SB 1476's opt-out provision is more informal and less heavy on procedure. As noted earlier, under GLB, a financial institution generally may not disclose a customer's "nonpublic" personal information to a nonaffiliated party until "(1) the financial institution . . . provide[s] a privacy policy to the customer, and (2) the customer [is] provided [with] a notice and the opportunity to opt-out of the financial institution's information sharing with nonaffiliated third parties."[176] SB 1476 on the other

---

171 Lynn Goldstein, *Evolution of the Opt-out and its Exceptions*, 1472 PLI/CORP 591, 595 (2005).

172 CAL. PUB. UTIL. CODE § 8380(b)(4) (West 2011).

173 *Id.* § 8380(c).

174 *Id.*

175 *See* Kim Zetter, *TJX Hacker Charged with Heartland, Hannaford Breaches*, WIRED.COM Aug. 17, 2009, http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/.

176 Goldstein, *supra* note 171, at 599 (citations omitted).

hand does not stipulate when or how the utility must present an opportunity to opt-out to the customer; the utility "shall ensure that the customer has an option to access [their own energy consumption] data without being required to agree to the sharing of his or her personally identifiable information."[177] Read literally, this subsection appears to require an impossible feat: a utility contracting with a third party to provide smart grid services to ratepayers must continue to provide such services to customers who opt-out of the third party's involvement. However, SB 1476 can be interpreted to allow the utility more flexibility. Since the term "electrical or gas consumption data" is not defined in the law and could technically be interpreted to include a basic home energy bill (e.g. last month consumer *X* consumed 900 kilowatt hours), the language of SB 1476 allows utilities to deny smart grid services from customers who opt-out of sharing their consumption data with third party service providers.[178] Assuming that section 8380(b)(4) allows customers to opt-out of all unwanted sharing with third parties is somewhat of a departure from GLB's approach, which must continue to provide the same service to customers after they opt-out of sharing with nonaffiliated service providers.[179]

D. SB 1476: Enforcement of Data Protection Standards

The fifth "privacy principle" recognized in HEW's *Records, Computers, and the Rights of Citizens* was that organizations entrusted with personal information have a responsibility to protect that information from unauthorized disclosures and uses.[180] "Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data."[181] Both Gramm-Leach and the California smart grid privacy statute impose requirements on regulated entities to "develop, implement, and maintain a comprehensive information security program"[182] or "use reasonable security procedures and practices."[183] While it is unclear whether the new smart meter privacy law can be used as the foundation of a

[177] PUB. UTIL. § 8380(b)(4).
[178] *See id.*
[179] 15 U.S.C. § 6803(a)(1) (2011).
[180] *See* 1973 HEW Report, *supra* note 62, at 44–45.
[181] *Id.* at 41.
[182] 16 C.F.R. § 314.3(a) (2011).
[183] PUB. UTIL. § 8380(d).

private cause of action, the text of the law goes a step further than GLB by requiring that electric utilities not only institute "reasonable security" measures but also that their contracts with third party vendors hold their business partners accountable to the same security standards.[184]

Unlike GLB, California's SB 1476 does not specify whether the law's data security provisions will be enforced administratively by state agencies or litigated through civil actions.[185] However, due to previous state based privacy legislation, utilities and third party smart grid vendors in California should expect state courts to be sympathetic to claims stemming from disclosures of energy consumption data through negligence. California's Security Breach Information Act ("SBIA") explicitly recognizes that database service providers have a legal duty to protect consumer's personal information providing, "[a]ny customer injured by a violation of this title may institute a civil action to recover damages."[186] Since California's SBIA applies to any "business that owns or licenses personal information about a California resident," SB 1476's data protection provision is somewhat redundant; however, by requiring that holders of energy consumption data apply the identical standard of care as other database companies,[187] the California legislature evinced an intent to expose utilities and third party contractors to civil liability for negligent handling and protection of smart grid data. Therefore, electricity and smart grid stakeholder groups should anticipate SBIA being leveraged to bring future energy consumption information claims now that SB 1476 has recognized energy consumption data as a new category of protected information.[188] Since California's SBIA does not speak to liability of a database manager who puts information to use for a "secondary commercial purpose" without customer consent, a third party who committed such an act with energy consumption data would, at worst, be derivatively liable for breach of contract with the utility rather than negligence action from a ratepayer.[189]

---

184 *See id*. § 8380(e)(2).

185 *See* S.B. 1476, 2010 Leg., Reg. Sess. (Cal. 2010).

186 CAL. CIV. CODE § 1798.84(b) (West 2011); *accord id.* §§ 1798.80–1798.91.

187 Both the SBIA and SB 1476 require regulated parties to "maintain reasonable security procedures and practices appropriate to the nature of the information." *Id.* § 1798.81.5(b); PUB. UTIL. § 8380(e)(2).

188 *See* S.B. 1476, 2010 Leg., Reg. Sess. (Cal. 2010).

189 *See* PUB. UTIL. § 8380(e)(2). A utility in California may disclose customer data to a third party provided "the utility has required by contract . . . [that] prohibits the use of the data for a secondary commercial purpose not related to the primary purpose of the contract

VII. CONCLUSION

The purpose of SB 1476 is to encourage necessary technological advances in the electricity sector while protecting individual ratepayers from experiencing financial or reputational harm through misuse of energy consumption data collected from smart meters and appliances. Regulation over the sharing, storage, and protection of energy consumption information is necessary due to the fact that smart meters can convey detailed information about ratepayers' routines, habits, and behaviors. Because this information has the potential to reveal intimate details about the in-home activities of residents, laws that prevent unauthorized information sharing are essential to establishing the credibility and legitimacy of smart grid technology among the public.[190] Despite the best efforts of states and consumer advocates to protect energy consumption data, it is likely that marketers, consumer products manufacturers, and even government entities will continue to press for energy consumption data to be made available in some regard. As demonstrated by the use of consumer credit information for purposes beyond assessing individual credit worthiness,[191] society should anticipate a similar push to commoditize and unlock energy consumption information for secondary business ventures.

A. An Overall Assessment of California SB 1476

Whereas privacy regulation in other sectors has placed the onus on customers to change default positions that automatically permit information sharing, the U.S. Department of Energy has advocated that within the smart grid space, "consumers should be able to decide whether and for what purposes any third-party should be able to access or receive the usage data, and that utilities should not disclose the data to third parties unless the consumer has opted in to such disclosure."[192] As was discussed in Section V, California's

without the customer's consent." *Id.*

[190] *See* SMART GRID TECHNOLOGIES, *supra* note 43, at 2 ("DOE also recognizes that long-term success of Smart Grid technologies depends upon understanding and respecting consumers' reasonable expectations of privacy, security, and control over who has access to potentially revealing energy-usage data.").

[191] "In addition to selling your credit report to lenders with whom you wish to do business, the three major credit bureaus -- Equifax, Experian and TransUnion . . . [sell] 'header' information from . . . credit report[s] to credit card companies and other lenders interested in mass marketing credit offers to consumers." Jeanne Sahadi, *Your Identity … For Sale*, CNNMONEY.COM, May 9, 2005, http://money.cnn.com/2005/05/09/pf/security_info_profit/.

[192] Elinor Mills, *Energy Dept. Report: Make Smart-Grid Data Sharing Opt In*, CNET NEWS,

SB 1476 embraces this "opt-in" model by restricting use of energy consumption data in two important ways: (1) California utilities are not permitted to sell their customers' energy consumption data under any circumstances, and (2) requiring third parties given access to electricity ratepayer consumption data to "prominently disclose[]" to the ratepayer any "secondary commercial purpose[s]" of the data and to obtain the ratepayer's consent for such uses prior to the use of the data.[193] Notably, SB 1476 also permits utilities and third parties to offer their customers financial incentives to allow their data to be used for a "prominently disclose[d]" "secondary commercial purpose."[194] So long as the privacy notices from third parties clearly and accurately explain their intended "secondary commercial purpose[s]" for the customer's commercial data, it is appropriate to recognize consumers' own property interest in their privacy. Ideally, this will incentivize companies to adopt more transparent practices as a means of attracting customers. Allowing energy consumption customers to weigh the benefit of a reduced energy bill, or some other financial incentive, against their personal privacy values is an economically efficient approach to privacy rights. This approach is in some ways preferable to blindly choosing a baseline privacy standard and applying it uniformly across all users, each of whom may value the secrecy of their consumption data differently.[195] SB 1476 acknowledges that, if data generated by the proliferation of the smart grid will be as valuable as anticipated,[196] the private sector should be free to negotiate with ratepayers to access that data for secondary commercial purposes.

In this respect, California's SB 1476 provides consumers with tangible privacy protections without overburdening service providers with disclosure and consent requirements to the point of

Oct. 18. 2010, http://news.cnet.com/8301-27080_3-20019913-245.html (discussing SMART GRID TECHNOLOGIES, *supra* note 43).

193 PUB. UTIL. § 8380(c), (e)(2).

194 "The electrical corporation . . . or its contractors shall not provide an incentive or discount to the customer for accessing the customer's electrical . . . consumption data without the prior consent of the customer." *Id.* § 8380 (b)(3), (c).

195 *See* LESSIG, *supra* note 2, at 228 ("[A] privacy property right would create strong incentives in those who want to use that property to secure the appropriate consent. . . . This [privacy property right] also recognizes . . . that people value privacy differently.").

196 "Vendors may purchase [energy consumption] attribute lists for targeted sales and marketing campaigns . . . . Universities might purchase information to study student attributes and target a new student profile with simple application question profiling. . . . [P]rofiling could extend to . . . employment selection, rental applications, and other situations . . . ." *See* Linda R. Evers, *High Voltage Insight on Smart Grid Issues*, SMART GRID LEGAL NEWS, Sept. 16, 2011, http://www.smartgridlegalnews.com/privacy-issues-1/.

stifling innovation. Recognizing that utilities will almost certainly require outside telecommunications expertise from third party contractors, SB 1476 puts no restrictions on whom the utility may share consumption data so long as the sharing is for the purpose of supporting the utility's energy service.[197] On the other hand, California's SB 1476 is quite stringent with regard to ratepayer control over energy consumption data, allowing for third parties providing an energy related service to use ratepayer information for "secondary commercial purpose[s]" only if they obtain the ratepayer's express permission.[198] Proper use of the "opt-in" model alone will go a long way towards preventing unauthorized or unintended leaks of personal data into the marketplace. California regulators should be mindful to remain vigilant of "opt-in" questionnaires deceptively designed to obtain a customer's consent.

B. Post-SB 1476 Regulation of Smart Grid Data

The very real possibility of ratepayer energy consumption data being unevenly regulated by state legislatures and public service commissions demonstrates the need for a baseline privacy standard set at the national level. If we acknowledge from the outset that smart grid data will have tremendous value to a myriad of commercial interests, then we must anticipate increasing pressures by third party firms, utilities, and policymakers to allow energy consumption data to be released and leveraged for economic gain. Under the current model, where regulation of energy consumption data will vary in each state, it may be tempting for a third party service to avoid more onerous state regulation by storing data in out-of-state servers. Furthermore, the state-by-state regulatory model encourages a regulatory race to the bottom, where states interested in attracting investment from the marketers and consumer products manufacturers will adopt an approach to ratepayer privacy more akin to Gramm-Leach-Bliley than to California's SB 1476. Such an uneven approach to regulation could undermine ratepayer confidence in the smart grid and create an unwanted backlash against adoption of these technologies.

Energy consumption regulation at the national level should establish baseline consumer protection standards influenced by

---

[197] "[T]his section shall [not] preclude an electrical corporation . . . from disclosing a customer's . . . consumption data to a third party for system, grid, or operational needs . . . ." PUB. UTIL. § 8380(e)(2).

[198] *Id.* § 8380(c), (e)(2).

aspects of SB 1476, federal privacy guidelines, and other privacy statutes, including aspects of GLB. The goal of a national regulatory policy should be to encourage ratepayers to become active participants in determining how their energy consumption data is utilized, while also establishing a default position that prohibits commercial use of energy consumption data unless ratepayer consent is obtained through use of opt-in provisions.[199] Regulators should consider allowing utilities to share certain types of data without restriction for the sole purpose of improving smart grid services, however, the use of consumption data for "secondary commercial purpose[s]" should be permitted only after obtaining the consumer's express consent. Any state or national regulation of energy consumption data should seek to improve upon SB 1476 by requiring utilities to provide ratepayers a means to annually review and modify their personal data "privacy settings." This could be achieved through GLB-type annual statements (albeit hopefully with less obfuscation on the third party's behalf) or a web-based interface that enables users to manage their privacy from an Internet connection. Conceivably, the system could be designed to allow ratepayers to set and update their privacy preferences through their smart meter or home area network.

Given that we are still in the nascent stage of smart grid development, the federal government believes it prudent to give states the room to experiment with different regulatory approaches for energy consumption data. The Department of Energy has encouraged states to independently regulate smart grid data because "it may be difficult or impossible to predict the uses to which a 'smarter' . . . grid will ultimately be put. Our federal system of state and local governments was intended to provide opportunities to experiment so debates about the relative merits of differing approaches can be assessed by practical experience."[200] While the prudence of this approach is self-evident and consistent with the tradition of using states as laboratories for policy development, this proposed hands-off regulatory approach fails to appreciate the risks facing consumers if energy consumption data were to fall in the wrong hands. It is also somewhat at odds with the approach currently being advocated in the U.S. Congress, where an Internet privacy law is taking shape that would require "[c]ompanies that track people's activities online [to] obtain people's

199 *Id.*

200 *See* SMART GRID TECHNOLOGIES, *supra* note 43, at 6.

consent first. . . . [and] specify what data they are collecting and how they will use it."[201] Although it is questionable whether a law regulating "internet privacy"[202] would also apply to data derived through electricity infrastructure, it is difficult to see the rationale for restricting corporate access to data about citizens' online behavior while taking a hands off approach to data that characterizes citizens' behavior inside their own homes.

[201] Editorial, *A New Internet Privacy Law?*, N.Y. TIMES, Mar. 18, 2011, http://www.nytimes.com/2011/03/19/opinion/19sat2.html.

[202] *Id.*