Chapter 22. Privacy issues in smart grid deployment

Jennifer M. Urban

Forthcoming 2016 in
Research Handbook on Intellectual Property and Climate Change, Elgar

Introduction

Along with other efforts to address climate change with green technologies and greater energy efficiency, a recent push to make the electricity grid 'smart' is bringing new information technologies into homes and businesses across the United States (US) and in the European Union (EU). The new technologies—in this Chapter, I will focus on smart electricity meters and other devices that gather or process household energy signatures at high temporal resolutions—have a great deal of promise. Among other predicted benefits, smart grid technologies are expected to help us better manage energy usage, enable real-time demand-response pricing, improve efficient load balancing across the grid, and increase the capacity for solar and other edge-based energy generation. These predicted benefits depend, in part, on new, richer data models of energy flow and usage. As such, the detailed information collected by advanced metering technologies is of interest to governments, utilities, their customers, and companies developing new technologies and services intended to support efficient energy generation, transmission, distribution and use.

Smarter energy technologies promise to provide substantial support to societal efforts to mitigate and adapt to climate change. At the same time, the temporally granular data collected by advanced metering technologies can reveal detailed information about intimate life within the home, raising serious questions about how to address privacy interests. As far back as 1989, George Hart, one of the inventors of the computational technologies that make it possible to 'see' into a home by observing detailed energy consumption data, predicted the surveillance potential of what we now call smart technologies.[1] Hart argued that the ethical and legal questions they raised must be addressed.[2] Because detailed energy usage data has this capacity to reveal information about activities within a home and the habits of its occupants, it is also likely to be of interest to many beyond the energy industry, including law enforcement, marketers, insurance companies, even criminals.

The recent rapid movement to build out the smart grid thus demands that we develop and put into place clear and appropriate privacy requirements to govern the collection and use of these data. In addition, the present vision for the smart grid requires large numbers of new devices and gateways to connect from the 'edge' of the grid, raising security issues that require immediate and sustained attention. Efforts to address both privacy and security issues have begun in earnest internationally and in the US, including efforts by several Federal agencies and state public utility commissions. Thoughtful, informed design also is critical to developing technologies that address climate concerns without unduly encroaching on privacy interests.

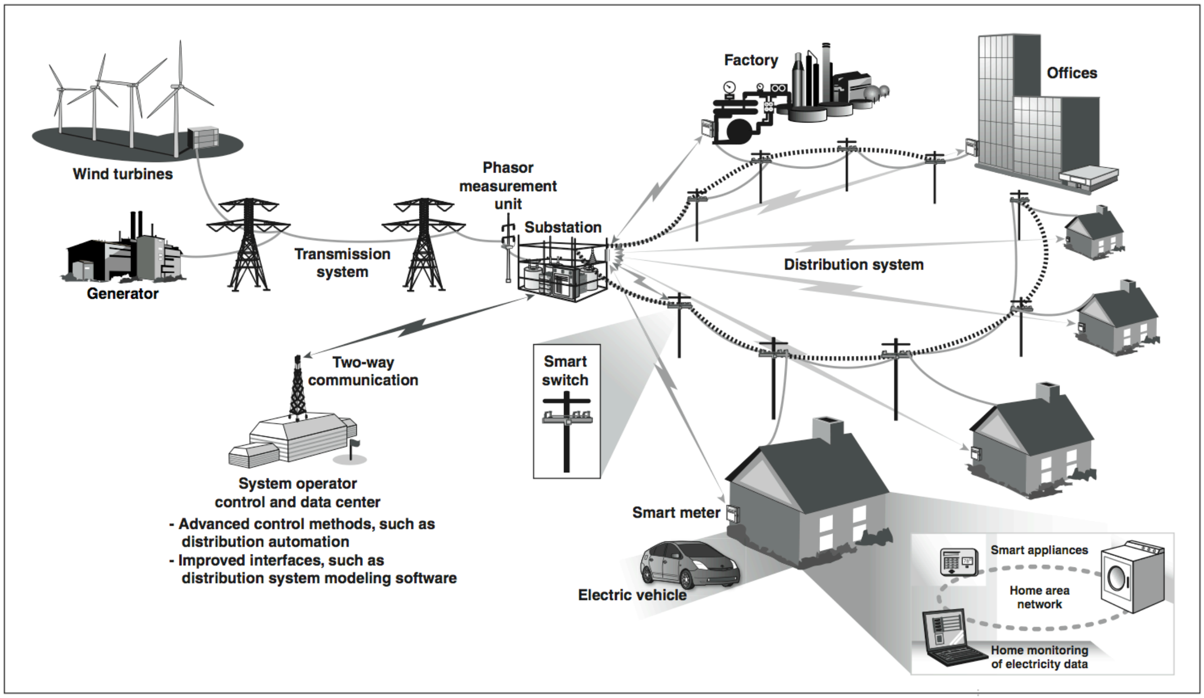
This chapter serves as an introduction to the privacy and security issues presented by advanced metering and other smart technologies, and to recent policy efforts to address them. The chapter briefly introduces the recent political and economic push to move to the 'smart grid', describes the privacy issues presented by advanced metering technologies and the data they gather, and gives an overview of regulatory and policy efforts being made to address them as the smart grid develops. Finally the chapter provides a brief background note on cyber-security issues, which have emerged as a critical area of concern.

Moving to the smart grid

The term 'smart grid' generally refers to a modernized electrical generation, transmission, and distribution system that updates the traditional grid system by integrating it with information technology and a range of new devices and service models.[3] The traditional grid structure generally supports one-way energy provisioning from an energy supplier to a premises, with little communication back to the supplier. In contrast, the smart grid features ongoing two-way communication between energy suppliers and customers.[4] In addition, smart grid models generally assume that the updated grid will feature services and devices that connect with the existing grid from its edge. Together, these changes are expected to allow for real-time, demand-response pricing for energy, distributed power generation (for example, through solar panels), and new devices and services that maximize customers' energy efficiency.

A key component of the smart grid vision is advanced metering infrastructure (AMI). AMI systems include as one of their most visible components digital 'smart meters' that can collect near-real-time energy usage data and engage in two-way communication usage data, pricing information and other information.[5] These advanced metering systems are expected to tie into home area networks (HAN) of communications devices that gather and communicate data and respond to pricing and other signals from utilities or third-party providers.[6] Finally, at their most general level, definitions of the smart grid often include new business models, new regulatory frameworks, and new energy supplier and customer behaviors that are expected to arise from modernizing the grid's physical components.[7] Figure 1 shows some of the main components of the smart grid.

Figure 1: Common Smart Grid Components[8]


Wind turbines
Generator
Transmission system
Phasor measurement unit
Substation
Two-way communication
System operator control and data center
- Advanced control methods, such as distribution automation
- Improved interfaces, such as distribution system modeling software
Smart switch
Factory
Offices
Distribution system
Smart meter
Electric vehicle
Smart appliances
Home area network
Home monitoring of electricity data

Plans to modernize the electrical grid are the subject of a concerted push by the White House and US agencies, individual states, the EU, China and other countries. As described more fully in the Chapter by Steven Ferrey, improving electricity generation and delivery is seen by government officials as key to combating climate change. Moving to a distributed generation system that supports less carbon-intensive fuels is a central part of that effort. There thus is growing investment in smart grid programs. And a substantial portion of smart grid investment worldwide is devoted to smart meter installation.

In 2007 the US Congress passed the Energy Independence and Security Act (EISA), which declared it 'the policy of the United States to support the modernization' of the electrical grid.[9] President Obama's 2009 stimulus package, the American Recovery and Reinvestment Act (ARRA), allocated $4.5 billion to develop and support a nationwide smart grid plan; this was matched by $5.5 billion from public and private investors.[10] A number of federal agencies have taken up the baton and issued reports detailing plans and recommendations for smart grid deployment, from the US Department of Energy (DOE)[11] and the US Federal Energy Regulatory Commission (FERC),[12] to the US Department of Commerce (DOC),[13] and on to the US Federal Communications Commission (FCC), which sees smart grid deployment as an important element of the National Broadband Plan.[14] To coordinate efforts, the White House in June 2011 issued 'A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future'; that framework sets out four 'pillars' to guide grid modernization: 1) enabling cost-effective smart grid investments; 2) encouraging electric sector innovation; 3) empowering consumer decision-making; and 4) securing the grid.[15]

Smart grid deployment is still in its early stages in the US. Because the 2009 federal stimulus funds focused on technology deployment and training, rather than on research and development, the funds have proven a powerful impetus for states to roll out smart grid programs—especially smart meter deployment programs—and for federal agencies to develop supporting programs. Across the US, there were over 43 million smart meters installed by 2012. FERC predicted that by 2019—one decade later—these installations would climb to 80 to 141 million meters.[16] In California, a leader in smart grid deployment within the US, utilities predicted that more than 14 million meters would be installed by the end of 2012. Overall, the US is projected to invest between $338 and $476 billion in smart grid investments by 2030.[17]

But as rapidly as the US is moving, the EU is, by some measures, further along. The EU pushed for smart meter deployment in its Third Energy Package in 2009.[18] By 2011, 45 million smart meters were already installed in EU countries, with 240 million projected to be installed by 2020.[19] China is also investing aggressively in the smart grid and in smart meters; it has created the State Grid Corporation of China (SGCC), which plans to invest $601 billion to build out a nationwide smart grid by 2020, and to install 360 million smart meters by 2030.[20] Other countries are following suit: South Korea plans to install 24 million smart meters by

2020; India plans to install 130 million, also by 2020; and Brazil plans to install 63 million by 2021.[21]

Industry investment in smart grid devices and services is also growing rapidly. The dual incentives of government funding and the opportunity to build and exploit new clean technology markets have created a so-called ‘smart grid gold rush’ to provide devices and services to consumers, utilities and organizations. New companies are in the process of rolling out personal metering systems, energy efficiency services, home area network devices, smart appliances and other innovations intended to meet the expected demand for smart grid services.[22] Taken as a whole, the implementation of AMI, the addition of consumer appliances at the grid’s edge, and the addition of new, third-party service providers is expected to expand the traditional grid into a complex energy data ecosystem.

We can expect to see profound changes in grid infrastructure within the next two decades as nation-states move aggressively to upgrade their systems and as private industry responds with new technologies and services. As this build-out occurs, the collection and use of energy consumption data will increase. As described in the next sections, new devices, new forms of data, new data uses, and new data flows, together with the greatly increased complexity and inter-connectivity of the smart grid communications network, present fundamental privacy and security issues that will need to be addressed as the smart grid build-out progresses.

Privacy issues presented by the smart grid ecosystem

Implementing the smart grid technological ecosystem, as envisioned by government agencies and industry actors, includes major changes in energy data practices. At least three dramatic shifts are included within these changes: (1) changes in the characteristics of energy usage data that make it much more revealing of activities within a premises than previous data forms; (2) changes in the purposes for which the data is used that could result in substantial privacy impacts for energy customers; and (3) changes in data flows that greatly expand the paths energy data travels and the locations in which it is held. Each of these changes presents acute questions about how to manage privacy and security issues created by smart grid technologies and business practices.

1. Changes in energy data characteristics

The first shift lies in the fact that AMI technologies collect far more comprehensive information about energy usage within individual premises than the traditional electromechanical meters with which most customers are familiar. The highly granular data collected by smart meters and smart appliances can reveal a detailed picture of activities occurring within customers' homes or other premises—spaces that traditionally have been treated as private and protected from surveillance by legal safeguards.

The data that smart meters and other smart technologies can collect is more detailed along a number of dimensions than was previously collected data. First, advanced metering devices collect much more temporally granular data than older devices. The shift is dramatic. For generations, utilities have relied on electromechanical meters that were read (usually once a month or so) by individual meter readers. These once-a-month aggregate readings reveal little about the details of energy usage within a household or other premise, and allow only for retrospective or estimated billing and for generalized comparisons of average energy use across similarly situated households. The smart electrical meters now being rolled out by utilities across the US and EU, however, are capable of collecting energy usage information as often as every few seconds.[23] Most commonly, they are programmed to collect information at 15-minute or hourly intervals.   Eventually smart meters and other devices are expected to allow real-time or near-real-time tracking of energy usage—a marked change from historical metering practices.

Second, smart grid technologies will allow utilities (and perhaps appliance manufacturers, third-party energy efficiency services, or others) to collect electricity consumption data from a single, uniquely identified home appliance. Historically, only aggregate electricity consumption data of all appliances within a household has been collected.

Third, a much greater variety of information is likely to be collected and processed by smart grid technologies than that collected and used by conventional energy devices and services. For example, in addition to energy consumption data and unique appliance identifiers, utilities or other service providers may also collect information about the efficiency of home appliances, the size of a home and the temperature inside it, location information from plug-in hybrid electric vehicles within the smart grid and so on.

The shift to a smarter grid thus represents a tremendous increase in the amount and detail of energy usage data collected compared to previous systems. At 15-minute collection intervals, a smart meter gathers approximately 3000 data points per month about an individual household's energy consumption—a profound change from the one data point per month collected from electromechanical meters by individual meter readers. Consumers can also buy devices that can be installed 'below the meter' (that is, within the house) and that can take fine-grained measurements of energy consumption. For example, 'The Energy Detective' is a consumer device that records consumption from its installation point where household circuits converge at the top of the breaker box and transmits the data to a home computer or to a third-party energy service provider for processing.[24] Further, smart appliances that communicate their specific usage patterns—for example, smart washing machines and other appliances that communicate with the utility to receive time-of-use pricing information —are increasingly available in the marketplace.[25]

Taken together or individually, these new data collection technologies gather an unprecedented amount of information about the habits and activities of residents within a household. For example, if the stove is running, then the data may reveal that someone is cooking. How revealing the data will be varies with the number and type of smart appliances communicating with the collection point; however, information from specific appliances is not needed in order to understand their patterns of use. Rather, the short-interval usage information collected by advanced metering systems alone can supply a detailed picture of activities within a premises. By collecting detailed energy usage data and analyzing it with computational techniques—a method referred to as 'non-intrusive appliance load monitoring' (NALM, sometimes referred to by other acronyms[26])—a researcher can understand what is happening within a premises at a high level of detail.

NALM uses temporally granular energy consumption data to reveal usage patterns for individual appliances within a house—for example, when a refrigerator or heating system cycles on and off, when the stove or big-screen television is in use, and in some cases even when an individual light is turned on or off.[27] While researchers originally used the term 'NALM' to mean a specific hardware monitoring device along with the computational software needed to analyze the data, smart meters and other monitoring devices now available on the market are also capable of collecting sufficiently detailed data to support the use of NALM-based computational techniques. As such, the granular energy usage data collected by smart meters and other devices can reveal, among other things, when a household's residents are home or away; their sleeping, cooking, and other habits; and approximately how many individuals reside in a household. Many such details are available from 15-minute interval[28] data. The real-time or near-real-time data that smart grid technologies are capable of collecting may in turn reveal the near-real-time activities of a household, as reflected in its use of electrical devices.

The privacy concerns that arise from revealing household activities using detailed energy usage data have only recently attracted the attention of policymakers. Many of these issues, however, were identified almost as soon as the NALM technology was developed. In 1989, George Hart, one of the inventors of NALM, observed that:

> [t]his [Nonintrusive Appliance Load Monitor] . . . by using sophisticated signal analysis techniques on the voltage and current waveforms, determines the nature and exact usage characteristics of the individual appliances within the home which constitute the load. The monitor requires only the information externally available from measurements of the load; no entry into the home is necessary to place sensors on separate appliances or branch circuits; no appliance survey or other cooperation from the residents is required.[29]

Hart also described how NALM worked to remotely identify and monitor specific appliances within a premises and explained that detailed energy load data on end-use devices could help utilities to balance loads, encourage energy-conscious individuals to reduce their monthly bills, and assist trouble-shooters to locate failing devices. But the principal point Hart wished to convey was ethical in nature, not technical. He expressed a deep concern that, although the 'intended use of the [monitoring] device is completely benign', NALM could be used to observe occupants of buildings unobtrusively. 'From [its] unseen and unsuspected vantage point, the monitor has a view deep into the workings of the residence. After observing the residence for a short while, it generates a list of objects (appliances) and events (usages) that the occupants may consider completely private'.

The granular data collected by today's advanced metering devices are assumed to be a key component of the new smartness of the upgraded electricity grid. As Hart recognized almost from the beginning, however, and as policymakers, utilities, innovators, and consumers are beginning to wrestle with today, it is also sufficiently revealing of the details of intimate home life to have very different effects on privacy from historical forms of energy data. Further, it has more recently become clear that granular energy usage data cannot easily be anonymized; like other rich types of information, 'anonymized' energy usage data is vulnerable to 're-identification' attacks that serve to tie profiling information back to specific homes.[30]

2. Changes in the uses and users of energy data

The rich details of smart grid data, and their ability to reveal appliance use and household activities, make such data attractive for a wide range of new purposes. Such granular data allows for the possibility of real-time pricing and demand-response systems and other utility-run energy management programs that could help combat climate change through lowering production emissions and energy demand. Real-time or near real-time information is widely expected to help utilities more efficiently balance load, respond to power outages, and enhance grid defenses against attack.[31] Smart grid data also can support customer devices and non-utility providers of related services that help customers lower their electricity bills and increase efficiency by tracking time-of-day usage and habits and by pinpointing inefficient appliances and behaviors.

Smart technology may eventually allow utilities to implement detailed peak-demand, time-of-use pricing, which may induce further shifts in consumer usage patterns and further reduce peak loads, strain on the grid, and consumer charges.[32] Some customer advocates, however, worry that energy bills will increase for customers who, for health or other reasons, do not have the option of changing the amount of or times they use energy.[33] Further, the overall efficiency savings predicted for these programs are disputed.[34]

Examples of such new or anticipated data uses abound. Utilities and third-party providers are rolling out a variety of devices and programs that allow customers to visualize their energy usage and to pinpoint inefficient behaviors and appliances, allowing tailored energy efficiency planning.[35] The detailed data and two-way communication capabilities provided by smart meters are expected to support and extend utility programs that reach into a home or other premises, and may request or even require that customers shut off appliances or otherwise shed loads. For example, Pacific Gas & Electric (PG&E) offers a 'SmartAC program' in which PG&E installs programmable thermostats for customers' air conditioners. These thermostats engage directly in two-way communications with the utility.[36] PG&E might use the communication channel to display messages on the screen of the thermostat, such as weather warnings, greetings and system maintenance notices.[37] Consumers can also configure their thermostats on PG&E's website,[38] giving the utility company information about consumers' temperature preference in their homes. Further, smart grid data is likely to extend existing grid management programs. Florida Light & Power (FLP), for example, has long offered customers a monthly billing credit in return for giving FLP the ability to remotely cycle off participants' air conditioners for short periods during times of peak demand.[39]

The smart grid may offer additional, unforeseen methods for combating climate change, including real-time pricing markets and edge-based green generation. Optimistic future scenarios include smart grid data use in 'smart houses'[40] (or business premises) that are in full two-way communication with the grid and energy markets. This allows such premises to adjust automatically to price and energy signals. In turn, this would allow them: to shed load or to sell energy generated from solar panels (or other sources) back to the grid when prices are high; to charge Plug-In Electric Vehicles (PEVs) when prices are low; to allocate loads throughout the house; and son on. Although the full vision of the smart house may be years from realization, a great variety of HAN-based devices and services are on the market today,[41] and others are likely to follow if smart grid communications technologies develop as planned.

Such beneficial uses are promising. At the same time, as Hart observed, such data is likely to be attractive for more generalized behavioral tracking and surveillance. The fact that smart grid data provides a virtual window into household activities is likely to make it highly attractive for a number of purposes that create strong privacy risks. Utilities, energy-efficiency service providers, or other energy-sector providers may find the data useful for marketing campaigns or for other purposes beyond energy provisioning.[42] Third parties outside of the energy industry are likely to find the data equally attractive for any number of marketing or profiling purposes. For example, information about daily habits may be valuable to marketers looking to promote new, energy-efficient appliances, as well as to other marketers of goods and services looking to add behavioral information to their consumer profiles. The data should be attractive to any sector that uses consumer profiling.

Policymakers and researchers have begun to take note of the wide range of possible uses of smart grid data. In 2010 a US National Institute of Standards and Technology (NIST) working group, in a comprehensive report on cyber security and privacy in the smart grid (NIST Guidelines 1),[43] catalogued a wide variety of potential uses of detailed energy usage and smart appliance data. The NIST group identified 'primary' uses for the data, which include load monitoring and load forecasting, demand response and efficiency programs, and consumption billing for PEVs. The group also identified a wide range of plausible 'secondary uses,' which include: use by law enforcement and litigants for investigations and evidentiary purposes; use of behavioral and location data by insurance companies to determine premiums for home, health and driving insurance; use of behavioral data by creditors to assess credit risk; use by advertisers for targeted marketing campaigns; use by law enforcement, private investigators, or criminals to determine the location of PEVs or other location-aware appliances; and use by the press to investigate the habits of famous or otherwise newsworthy individuals.[44] In September 2014, NIST issued an updated report (NIST Guidelines 2),[45] which included further recommendations for managing privacy issues in the smart grid[46] and added a legal and policy update.[47] The most substantial update consists of nearly four dozen use cases that apply the guidelines' privacy framework to concrete applications ranging from routine utility load balancing to plug-in electric vehicles. [48] This updated guideline document is a key resource.

While it is impossible at this stage in the smart grid's development to accurately predict the details of how data will be used, some of the uses identified by the NIST working group have clear historical precedents and seem very likely to occur. For example, detailed information about household activity is highly likely to be attractive to criminal investigators and other government actors who wish to investigate past acts and ongoing crimes. Less-detailed energy usage records have long been used by investigators to identify possible drug operations[49]; the richer data provided by smart grid systems almost certainly will be seen as an attractive investigative tool. As real-time data collection comes online, the use of granular energy usage data for ongoing surveillance also may become a plausible scenario. Similarly smart grid data is likely to be attractive to civil litigants, such as those involved in divorce proceedings or insurance disputes that present questions about daily habits or occupancy patterns. And smart grid data is likely to be attractive to criminals themselves, who might wish to know when a household is occupied or empty, or to gain access to a database of revealing profile information. All of these purposes raise serious questions about the appropriate legal standards for access to the data and the necessary level of security for data streams and data collections.

3. Changes in data flows

Third, data that previously flowed in one direction—from the customer to the utility—now flows in many more directions: bi-directionally between the utility and the customer; from the utility or the customer to third-party service providers; and from various entities to tertiary providers, such as marketers, insurers and data brokers. New smart appliances or other devices located at the grid's 'edge' also may generate and communicate new data when responding to price signals, requirements to shed load, or other utility communications. These new data flows create regulatory challenges, as existing legal and regulatory protections may not apply to new data paths or new data stewards.

A key resource for mapping the various smart grid data flows is the Public Interest Energy Research (PIER) Program's report 'Privacy in the Smart Grid: An Information Flow Analysis' (PIER Report).[50] While the PIER Report was prepared for the California Energy Commission and thus focuses on California's model of smart grid deployment, it maps smart grid data flows in a sufficiently generalized manner to be widely useful. The PIER Report identified privacy risks associated with a wide range of information flows, many of them new to the smart grid ecosystem:

- Meter data sent from a smart meter to the utility
- Meter data sent from a smart meter to a HAN
- Energy usage information collected by a customer-owned meter
- Data flowing within a customer-owned energy management system
- Energy usage information sent via a customer device or communication to a third party energy management system or service
- Third party access to energy usage information held by a utility
- Direct communication between a utility and HAN devices
- Data flows involving PEVs, which add information about the location—outside the home—of the PEV user.

In discussing each of the identified energy flow patterns, the PIER Report described existing legal protections, and concluded that current protections ‘apply to a narrow slice of Smart Grid data and, even then, they treat different Smart Grid actors inconsistently’.[51] It concludes that the integration of information technology with the electrical grid and the wide range of new data flows created, ‘present considerable risks to individual privacy’.[52] The PIER Report recommended a systematic approach to implementing privacy protections through architectural and information flow design as well as through policy. In making these recommendations, it joined a growing consensus view that a system-wide ‘privacy by design’ approach is necessary to protecting privacy in a modernized grid system.

Addressing smart grid data privacy: a developing policy landscape

Policymakers are only beginning to address the privacy and security issues presented by detailed energy usage monitoring. Hart identified many of them in 1989. He noted that NALM’s surveillance capabilities raised serious moral and legal questions, touching on civil liberties and due process of law. He thus raised a number of important questions related to who should have access to the data, who should control NALM devices, and who should bear responsibility for data breaches.[53] He noted, however, that his concerns were not shared by other scientists and engineers of his acquaintance. Though some offered technical ideas for improving security and avoiding identification errors, some doubted whether privacy issues even had a place in technical discussions. Privacy questions did not arise again until the recent push to expand AMI systems to create the smart grid.

Accordingly, existing legal standards for control of and access to energy consumption data, and legal protections for it, generally were developed with historical, aggregated (typically monthly) data forms in mind. Most US utilities historically required only a subpoena before they would release energy records to law enforcement.[54] The current required showing that police investigators must make before gaining access to utility data is unclear at best. While a patchwork of state statutes, federal statutes and utility commission regulations apply to various aspects of the smart grid (as the PIER Report and others have found), they apply inconsistently and incompletely.[55]

Researchers Deirdre K. Mulligan and Jack I. Lerner reviewed Fourth Amendment and state constitutional jurisprudence, and found that monthly aggregated data was often found to have little or no constitutional protection; court decisions repeatedly connected these conclusions to the courts' understandings that traditional aggregrated data was essentially unrevealing.[56] In contrast, the greater specificity of smart-grid data may raise constitutional concerns, particularly in regard to surveillance of homes. As Justice Scalia noted in *Kyllo v. United States*[57], which found that police may not peer into a house via thermal imaging technology without a warrant, '[i]n the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes'.[58] As such, the new forms of energy usage data created by smart meters are at odds with previous courts' reasoning in holding that monthly aggregated consumption data does not require constitutional protection and at odds with the incomplete statutory protection in place today.

Since 2008, a number of government actors have begun to address smart grid privacy issues in depth. State and Federal agencies in the US, as well as European states and the EU, have opened discussions of privacy issues. Some agencies have moved beyond discussion to policy development; a few state leaders—notably, California, Colorado, Ohio, and Texas—have either implemented policies or begun detailed discussions. In 2011, California became the first state to implement a comprehensive privacy rule for household energy consumption data,[59] and Colorado followed in early 2012.[60] Most states, however, have not yet developed complete approaches.

In 2010, California enacted Sections 8380-8381 of the California Public Utilities Code, governing utilities' use and disclosure of energy usage data. In parallel with the legislature's efforts, the California Public Utilities Commission (CPUC) began reviewing privacy and security issues in early 2010 as part of a comprehensive proceeding to regulate smart meter deployment and to mandate customer access to usage data. The CPUC specifically focused on privacy issues later that year, and commenced a year-long evaluation of likely uses of smart grid energy data and appropriate protections for it. In July 2011, the CPUC issued a rule (California Rule) implementing Sections 8380-8381, which required regulated entities to implement a robust version of the Fair Information Practice Principles (FIPPs) in handling energy consumption data.[61] Because of California's status as a national leader in smart grid deployment, and because it was the first state to consider comprehensive data privacy rules for smart grid data, the proceeding received significant attention. The California Rule has since influenced other state and federal efforts to address smart grid privacy issues. For example, in 2014 the DOE issued for public comment a draft 'voluntary code of conduct', intended to apply to smart grid data privacy practices by both utilities and third parties, that reflects many features of the California Rule.[62]

The California Rule followed a broad consensus, based on a full implementation of FIPPs developed in 1973 by the US Department of Health, Education and Welfare (HEW). The HEW FIPPs have since become the basis for privacy regulations in the US, Canada, and EU, and the basis for the privacy guidelines promulgated by the Organization for Economic Co-operation and Development (OECD). In translating the principles into regulatory language, the CPUC followed calls to apply the HEW FIPPs by DOC,[63] the Obama Administration's National Science and Technology Council (NSTC),[64] and NIST in its Guidelines 1,[65] and by others.

It remains to be seen whether the present regulatory discussions will be adequate to protect smart grid data, or whether they will require adjustment in the future. Even California's relatively comprehensive approach leaves questions unanswered. As the CPUC moved to release data for government, business, environmental, and research uses, it began to confront difficult privacy and security issues such as data breaches and re-identification threats. And importantly, third parties (outside of the customer-utility relationship) that receive data directly from a customer's smart meter or from another customer device (so-called 'below the meter' devices) are not necessarily covered by the California Rule. The CPUC found its jurisdiction clearly to extend to regulated utilities and to entities that receive information from the utilities, but left open the question of whether it may regulate energy data that flows directly from the customer.[66] Traditionally US public utility commissions regulate only to the 'demarcation point' of the meter and do not extend their regulations inside houses. This leaves a large piece of the overall smart grid data ecosystem under the auspices of the ill-fitting and piecemeal pre-smart-grid regime. As such, pressure remains on federal and state legislatures to consider broader protections.

Overall, the policy landscape around smart grid data is changing rapidly, and a number of regulatory efforts to address both privacy and security issues are underway in both the US and EU. In such a highly dynamic environment, the governmental reports cited earlier can provide a foundational background, and the California Rule and ensuing CPUC efforts can provide a detailed exemplar of regulation. But whether privacy issues will be adequately addressed across jurisdictions—and whether they will be addressed in a manner that supports innovation while building protections into system design—is a question that remains to be answered.

Note on cyber-security issues: a pressing issue

In keeping with the information-policy focus of this book, this Chapter mainly concerns itself with privacy. It is important to note, however, that the privacy and confidentiality issues presented by granular usage data make up a subset of the serious technical security issues presented by the shift to a smarter grid. As grids become "smarter," they are becoming both much more *complex* than before, incorporating far more devices and involving far more actors, and much more *interconnected*, incorporating several network layers and many communication protocols, including increasing connections to the Internet and other open networks.[67] Indeed, the smart grid will connect millions of local area networks, which each contain a variety of sensors, meters, or other devices.[68] In addition, the smart grid is planned to be highly *automated*, increasing the number of electronic controls.[69] Each of these changes introduce multiple entry points for attack and other vulnerabilities, some of which are exacerbated by widespread use of wireless data transmission. For example, home energy devices and smart meters nearly all communicate within Home Area Networks and with utility systems wirelessly. The introduction to the NIST Guidelines 2 notes that risks associated with the evolution of the Smart Grid 'include:

- Increasing the complexity of the grid could introduce vulnerabilities and increase
- exposure to potential attackers and unintentional errors;
- Interconnected networks can introduce common vulnerabilities;
- Increasing vulnerabilities to communication disruptions and the introduction of malicious software/firmware or compromised hardware could result in denial of service (DoS) or other malicious attacks;
- Interconnected systems can increase the amount of private information exposed and
- increase the risk when data is aggregated;

- Increased use of new technologies can introduce new vulnerabilities; and
- Expansion of the amount of data that will be collected that can lead to the potential for compromise of data confidentiality, including the breach of customer privacy.'[70]

The Guidelines further explain that this increased interconnectedness increasing the risk of 'cascading failures' that compromise multiple systems.

These technical vulnerabilities are coupled with a high practical risk of attack and very serious potential consequences if cyber-security measures fail. As critical infrastructure, any country's grid is attractive to the full gamut of attackers, from cyber-criminals to state actors. Smart grid infrastructures in the United States and in other countries have repeatedly been attacked both by criminals demanding extortion payments after cutting power and by state actors. This attractiveness, and the potential negative consequences of a successful attack, increases with the smart grid's increasing flows of valuable and sensitive data, increased physical vulnerabilities, and increased opportunities for creating cascading failures.[71] The smart grid's complexity and interconnection also makes it vulnerable to mistakes or malicious behavior by insiders.[72] Finally, utilities are not well versed in cyber-security, and as such, must catch up. Accordingly, smart grid cyber-security is recognized as a crucial concern by governments, leading to efforts such as the NIST Guidelines.

A more complete discussion is beyond the scope of this Chapter. However, key resources include the NIST Guidelines 2 and a second PIER report, 'Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks.'[73]

Conclusion

The value of smarter electricity delivery and use, along with the substantial investments already made in both EU and US jurisdictions, make it highly likely that smart grid deployment will continue and accelerate. In light of this rapid shift, George Hart's 1989 questions about NALM and its privacy implications look prescient today.

The rapid deployment of smart grid technologies, if not carefully executed, has the potential to introduce serious security and privacy flaws to the grid. These flaws may then become 'baked in' to technical designs and business practices. Fixing such problems later will be a costly and difficult enterprise. In contrast, the relatively nascent state of the technology and the fact that industry and policymakers anticipate a fundamental grid system overhaul provides a real opportunity to simultaneously address threats up front, through 'privacy by design' principles and careful security practices. If we manage the transition poorly, however, we risk introducing serious privacy and security threats that have the potential to profoundly challenge our assumptions about privacy in the home and the security of grid infrastructure.

[1] Hart, George W. (1989), 'Residential energy monitoring and computerized surveillance via utility power flows', *IEEE Tech. & Soc'y Mag.,* **8** (2), 12-16.

[2] *Ibid.*

[3] *See*, *e.g.*, United States Government Accountability Office (2011), 'Electricity grid modernization: progress being made on cybersecurity guidelines, but key challenges remain to be addressed', p. 4-5, http://www.gao.gov/new.items/d11117.pdf, accessed 2 April 2012 [hereinafter GAO, 'Electricity Grid Modernization Report'].

[4] *See* GAO, 'Electricity grid modernization', at 4-5.

[5] *Ibid.*, at 5.

[6] Mulligan, D., L. Wang, and A. Burstein (2010), 'Privacy in the smart grid: an information flow analysis', California Energy Commission, p. 5.

[7] Giordano, V., F. Gangale, G. Fulli, and M. Jiménez, (2011), 'Smart grid projects in Europe: lessons learned and current developments', *JRC-IE Reference Reports*, p. 10 [hereinafter Giordano, 'Smart grid projects in Europe'].

[8] GAO, 'Electricity Grid Modernization Report', at 6.

[9] Energy Independence and Security Act, Title VIII, Sec. 1301, Pub.L 110-140, 121 Stat. 1783 (2007) (codified at 42 U.S.C. § 17381).

[10] American Recovery and Reinvestment Act of 2009, Pub.L. 111-5, 123 Stat. 115 (2009).

[11] US Department of Energy (2009), 'Smart grid system report', http://www.smartgrid.gov/sites/default/files/pdfs/sgsr_main.pdf, accessed 2 April 2012; U.S. Department of Energy (2009), 'Guidebook for ARRA: smart grid program metrics and benefits', http://www.smartgrid.gov/sites/default/files/doc/files/metrics_guidebook.pdf, accessed 2 April 2012.

[12] Federal Energy Regulatory Commission (Sept. 2009) 'Assessment of demand response and advanced metering', Staff report, p. 2, http://www.ferc.gov/legal/staff-reports/sep-09-demand-response.pdf, accessed 4 August 2011 [hereinafter FERC, 'Demand Response'].

[13] Department of Commerce (2010), 'Commercial data privacy and innovation in the internet economy: a dynamic policy framework', http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf, accessed 2 April 2012 [hereinafter DOC, 'Commercial Data Privacy'].

[14] Federal Communications Commission (2009), 'Bringing broadband to rural America: report on a rural broadband strategy', p. 16, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-291012A1.pdf, accessed 2 April 2012.

[15] National Science and Technology Counsel (2011), 'A policy framework for the 21st century grid: enabling our secure energy future', pp. 3-6, http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf, accessed 2 April 2012 [hereinafter NSTC, 'Policy Framework].

[16] FERC, 'Demand Response', at 2.

[17] Giordano, 'Smart grid projects in Europe', at 15.

[18] *Ibid.*, at 19 (Box 1).

[19] *Ibid.*, at 13.

[20] *Ibid.*

[21] *Ibid.,* at 13-14.

[22] *See*, *e.g.*, Energy, Inc. (2010) 'About: the energy detective'*,* http://www.theenergydetective.com/about-ted, accessed 4 August 2011 (personal metering devices and energy efficiency data analysis) [hereinafter Energy, Inc.]; Control4, 'Brochure', http://www.control4.com/files/Control4-Brochure.pdf, accessed 5 August 2011 [hereinafter Control4].

[23] Mulligan, Wang and Burstein, at 6.

[24] *See* Energy, Inc.

[25] Consumer Reports (2010) 'General Electric's smart appliances', http://www.consumerreports.org/cro/video-hub/appliances/other-appliances/general-electrics-smart-appliances/16548701001/62916551001, accessed 5 August 2011.

[26] *See* Quinn, Elias L. (2009) 'Privacy and the new energy infrastructure', *Center for Energy & Envtl. Security,* **09**, 1-43, p. 21, n. 118.

[27] Hart, at 13; Sultanem, F. (1991), 'Using appliance signatures for monitoring residential loads at meter panel level', *IEEE Transactions on Power Delivery,* **6** (4), 1380, 1381, col. 2 (showing load graphs of various appliances and a fluorescent light). *See generally* Quinn, at 21-25.

[28] Mulligan, Wang and Burstein, at 29.

[29] Hart, at 12-16.

[30] *See*, *e.g.*, Electronic Frontier Foundation and Samuelson Law, Technology & Public Policy Clinic, (2013), 'Memorandum from Electronic Frontier Foundation and the Samuelson Law, Technology & Public Policy Clinic regarding technical Issues with anonymization and aggregation of detailed energy usage data as methods for protecting customer privacy', http://www.law.berkeley.edu/17342.htm, accessed 28 September 2014.

[31] NSTC, 'Policy Framework', at 52, 63.

[32] *See*, *e.g.*, Department of Energy Electricity Advisory Committee (December 2008), 'Smart grid: enabler of the new energy economy', p. 9, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/final-smart-grid-report.pdf, accessed 15 October 2014.

[33] *See* Utility Week (2011) 'Not everyone will be a winner', http://www.utilityweek.co.uk/news/news_story.asp?id=195686&title=Smart+meters%3A+not+everyone+will+be+a+winner, accessed 5 August 2011*;* Sonksen, Tyler and Golden State Alliance for Liberty (2011) 'Smart meter rollout', http://gsalca.com/2011/03/22/smart-meter-rollout-4, accessed 5 August 2011.

[34] *Ibid.*

[35] *See*, *e.g.*, DistribuTECH (2011) 'Silver spring expands partnership with OG&E on customer engagement and demand response', http://www.silverspringnet.com/newsevents/pr-020211.html, accessed 4 August 2011; Energy, Inc.

[36] PG&E, 'SmartAC frequently asked questions: what are the SmartAC technology options?'*,* http://www.pge.com/myhome/saveenergymoney/energysavingprograms/smartac/faq, accessed 4 August 2011.

[37] PG&E, 'Honeywell thermostat operating manual', http://www.pge.com/includes/docs/pdfs/shared/smartac/thermostatuserguide.pdf, accessed 4 August 2011.

[38] PG&E, 'SmartAC thermostat programming website guide', http://www.pge.com/includes/docs/pdfs/shared/smartac/pg-wc-7e_webguide_tstat[f]-screen.pdf, accessed 4 August 2011.

[39] PG&E, 'On call savings program', http://www.fpl.com/business/energy_saving/programs/oncall.shtml, accessed 4 August 11.

[40] *See*, *e.g.*, Mulligan, Wang and Burstein, at 50-51.

[41] Control4, 'Home automation', http://www.control4.com, accessed 15 October, 2014; Tendril, 'Energy Efficiency', http://www.tendrilinc.com/solving-your-needs/energy-efficiency, accessed 15 October 2014; Silver Spring Networks, 'The unified smart energy platform is here', http://www.silverspringnet.com/products, accessed 5 August 2011; Opower, 'What is Opower', http://opower.com/what-is-opower, accessed 5 August 2011.

[42] Southern California Edison (SCE), SmartConnect use case: C7 – utility uses SmartConnect data for targeted marketing campaigns, http://www.sce.com/NR/rdonlyres/E2927535-15B3-41F3-AE88-B06CE760225F/0/C7_Use_Case_081229.pdf; Mulligan, Wang and Burstein, at 8, n. 15-16.

[43] National Institute of Standards and Technology (August 2010), 'Guidelines for smart grid cyber security: vol. 2, privacy and the smart grid', *NISTIR 7628* [hereinafter NIST, 'Guidelines 1'].

[44] NIST, 'Guidelines 1', at 31, Tbl. 5-3.

[45] National Institute of Standards and Technology (September 2014), 'Guidelines for smart grid cyber security: vol. 2, privacy and the smart grid', *NISTIR 7628 Revision 1* [hereinafter NIST, 'Guidelines 2'].

[46] NIST, 'Guidelines 2', appendix d, p. 68-75.

[47] NIST, 'Guidelines 2', appendix c, p. 63-67.

[48] NIST, 'Guidelines 2', appendix e, p. 76-167.

[49] *See*, *e.g.*, Lerner, J. and D. Mulligan (2008), 'Taking the 'Long View' on the Fourth Amendment: stored records and the sanctity of the home', *Stan. Tech. L. Rev.*, 2008, p. 3, http://stlr.stanford.edu/pdf/lerner-mulligan-long-view.pdf, 4, accessed 5 August 2011; Narciso, Dean (28 February 2011), 'Police seek utility data for homes of marijuana-growing suspects', *The Columbus Dispatch*, http://www.dispatch.com/live/content/local_news/stories/2011/02/28/police-suspecting-home-pot-growing-get-power-use-data.html?sid=101, accessed 2 April 2012.

[50] Mulligan, Wang and Burstein.

[51] *Ibid.,* at 57-58.

[52] *Ibid.*

[53] Hart, at 12-16.

[54] Mulligan, Wang and Burstein, p. 24; California Public Utilities Commission (2011), ‘Decision 11-07-056’, p. 127 [hereinafter CPUC, ‘Decision’].

[55] Mulligan, Wang and Burstein, at 57.

[56] Lerner & Mulligan, § II.C, ¶¶ 25-30.

[57] *See Kyllo v. United States*, 533 U.S. 27 (2001).

[58] *Ibid.* at 37.

[59] CPUC, ‘Decision’.

[60] NIST, ‘Guidelines 2’, appendix c, p. 65.

[61] *Ibid*.

[62] United States Department of Energy Electricity Advisory Committee, ‘Data privacy and the smart grid: a voluntary code of conduct’, http://energy.gov/sites/prod/files/2014/09/f18/VCC_principles_2014_08_12_final_draft.pdf, accessed 28 September 2014.

[63] DOC, ‘Commercial data privacy’, at 22-29.

[64] NSTC, ‘Policy framework’, at 7, n. 12.

[65] NIST, ‘Guidelines 1’, at 7.

[66] CPUC, ‘Decision’, at 31.

[67] *See*, *e.g.*, Ghansah, I. (2012), ‘Smart grid cyber security potential threats, vulnerabilities and risks’, California Energy Commission, p. 8.

[68] Wang, W. and Z. Lu (2013), ‘Cyber security in the Smart Grid: survey and challenges’, *Computer Networks,* **57**, 1345.

[69] *See*, *e.g.*, Ghansah, at 8.

[70] National Institute of Standards and Technology (September 2014), ‘Guidelines for smart grid cyber security: vol. 1, smart grid cybersecurity strategy, architecture, and high-level requirements’, *NISTIR 7628 Revision 1* [hereinafter NIST, ‘Guidelines 2 introduction’], p. 1-2.

[71] Ghansah, at 19-11.

[72] NIST, ‘Guidelines 2 introduction’, at 7.

[73] Ghansah.