

## **Taking the “long view” on the Fourth Amendment: Stored Records and the Sanctity of the Home**

*Deirdre K. Mulligan and Jack Lerner*

In the wake of the California energy crisis of 2000-2001, the California Energy Commission (CEC) and California Public Utilities Commission (CPUC) are aggressively pursuing “demand response” (DR) energy programs aimed at reducing peak energy demand. Demand response systems convey information about market conditions through pricing or reliability signals to customers, who in turn, hopefully, alter their electricity consumption choices.<sup>1</sup> In particular DR programs are aimed at shifting the time at which customers use energy through the implementation of time-varying<sup>2</sup> tariffs. Armed with information about the time-varying cost of electricity residential and commercial customers are expected to reduce energy usage and/or shift their usage to non-peak, less costly, hours. Such shifts, even absent reductions in overall consumption, will reduce the likelihood of energy brown and black outs and provide direct savings to consumers.<sup>3</sup> Technologies to enable the demand response system, including advanced metering research and development [OpenAMI] and sensor and control technologies development [DRETD], are under development. These technologies will be coupled with a communication and network infrastructure that supports the multicast of real-time pricing information, and the aggregation of energy usage and billing information.<sup>4</sup>

Demand response energy infrastructure is a policy imperative. The federal Energy Policy Act of 2005<sup>5</sup> directs the Department of Energy to identify target levels of demand response benefits that can be achieved by January of 2007.<sup>6</sup> The statute directs electric utilities to begin offering time-varying energy rates, and meters capable of supporting those rates, to consumers within 18 months of August 8, 2005.<sup>7</sup> The Department of Energy is charged with educating consumers about the benefits of the systems; both state and federal agencies are charged with investigating the potential of, and making plans for, demand response adoption.<sup>8</sup> It is expected that various demand response programs

---

<sup>1</sup> David Cay Johnston, “Taking Control of the Electric Bill, Hour by Hour,” NYT, January 8, 2007 A1.

<sup>2</sup> Energy prices vary in predetermined blocks throughout the day, or vary in real-time based on market conditions.

<sup>3</sup> “Taking Control” (discussing savings of participants in a Chicago DR pilot and Central Park NY co-op that earned \$3,000 selling unused energy capacity back to the utilities during a blackout in July 2006.) A14

<sup>4</sup> It is intended that the associated infrastructure support other operations, such as diagnosis and maintenance, but a discussion of this is beyond the scope of this paper.

<sup>5</sup> Energy Policy Act of 2005, Pub. L. 109-58, § 1252, 119 Stat 594, (2005), which amended § 111(d) of the Public Utility Regulatory Policies Act of 1978 (16 U.S.C. § 2621(d)).

<sup>6</sup> Id. § 1252(d).

<sup>7</sup> Id. § 1252(a).

<sup>8</sup> Id. § 1252(a)-(g). The language of the statute appears to say that states may perform a complete analysis in 18 months – 2 years and then come to the conclusion that implementing advanced metering and demand response at that time is “inappropriate,” § 1252(a), but the statute clearly encourages adoption of demand

will be adopted throughout the country. Similar infrastructures are being put in place in other countries, some more advanced than in the U.S.<sup>9</sup>

A core component of the demand response system is the collection of information about energy consumption from residential and commercial buildings at frequent intervals. The analog electric meters prevalent today are unsophisticated instruments that allow a meter reader to assess electricity use during the time interval between meter readings. The meters found in basements and on exterior walls, are typically read once a month by an employee of the utility who visits on foot.

Over the next two to five years these meters will be replaced by digital meters that collect data at frequent intervals, store it for many days, and transmit it wirelessly to the utility. Meters likely to be installed during 2006 are expected to contain a data collection module that will enable hourly readings and wireless transmittal of these readings to the utilities. Advanced metering installations projected to begin in 2007 will be capable of greater internal processing and have enhanced data storage capability. These meters are expected to collect data on electricity consumption at intervals ranging from one hour down to fifteen minutes. There is little agreement on how often meter readings will be sent to the utility or the intermediate nodes (concentrators) within the neighborhood, and the period for which readings will be retained in the meter, the nodes or the utility. The meters will collect and send a data set including a unique meter identifier, timestamp, usage data and some form of time synchronization information.<sup>10</sup> The data is expected to be in a proprietary format unique to the individual manufacturer or utility<sup>11</sup>, although some participants are looking forward to the availability of open standards and architecture for meters.<sup>12</sup>

---

response programs, and pledges Department of Energy assistance to help states develop their programs. § 1252(e).

<sup>9</sup> Data about pilot DR programs around the country and initiatives in other countries.

<sup>10</sup> Define. Additional information, including outage information, voltage, phase, and frequency data, would be useful for load management, but its collection or transmission is not envisioned until later phases of implementation.

<sup>11</sup> At this point manufacturers and utilities are not intending to use encryption to secure the data and will only use it on select portions of the communications channels.

<sup>12</sup> The OpenAMI project is one entity pursuing open standards and architectures for meters. The American National Standards Institute (ANSI) also provides some standards for electric and other meters. ANSI C12.19 standardizes data formats for the storage, alteration, and transmission of metering information. This includes a language used to dynamically resize data tables to include and exclude certain categories of information for transmission. It also includes standard formats for the users to define their own tables for reading, their own audit logs of metering events such as communications, executions of procedures, and alterations to data or the system clock. C12.19 includes requirements for authentication using a non-hierarchical password (one password for open access) scheme and encryption with meter reading. It provides a read interval (the period of time in between automatic reads) in the range of 1 minute to every 45 days. It includes space for up to 15 distinct seasonal settings (categories of pricing). It is not clear what proportion of meters being considered for widespread deployment actually meet this standard.

Current utility practices include saving many years worth of customer usage data to facilitate customer dispute resolution as well as load and other research. These data retention practices are expected to persist.<sup>13</sup> If all the readings are maintained, a customer's yearly record will shift from a record of one data point per month reflecting average daily usage to a record of 750- 3000 distinct and time-stamped data points per month that reflect actual energy use. The information itself is distinct from the averages found in today's bills. More significantly, the information one can glean or infer from this more accurate and detailed data set is radically different. Electricity consumption patterns in the coming DR system will reveal variations in power consumption that in turn can be associated with various household activities. Over time, power consumption can reveal personal sleep and work habits<sup>14</sup>, the presence of certain medical equipment and other specialized devices<sup>15</sup>, and of course signal the illegal behavior which today prompts law enforcement to seek them in certain drug production cases.

The changes in the frequency, format, contents, storage and transmission of data about electricity consumption that are integral to the planned demand response infrastructure raise interesting questions about the ongoing viability of maintaining, as a technical, practical and legal matter, the privacy of activities occurring within the home. How will the system architecture and business models address the increased sensitivity of meter readings? For example, imagine a future "wardriving"<sup>16</sup> incident where wardrivers detect and monitor the unencrypted traffic between household meters and neighborhood level concentrators that relay energy usage information to the utilities. Monitoring such communications could provide information about occupancy on a per house, block, or neighborhood level. Armed with such information a criminal could relatively easily assess the best time to burglarize homes or engage in other property crimes in a neighborhood.<sup>17</sup> How will the business models of utilities evolve to take advantage of the more detailed information that can be gleaned from energy consumption data taken at fifteen-minute intervals? Most significantly for the purposes of this paper, how will the increased information about in-home activities generated, transmitted and stored in DR systems be dealt with under the Fourth Amendment?

Existing legal precedent addressing the privacy of in-home activities, the energy they require, and the heat signatures they emit point in different directions. On the one

---

<sup>13</sup> One interviewee explained that data is stored for 7 years. Customers can dispute a bill for 3 years, and if they do so, may dispute another 4 years previous. See *Utility Audit Co. v. Southern Calif. Gas Co.*, Decision 98-09-061, Case 97-02-015, 1998 Cal. PUC LEXIS 1097 (Cal. Pub. Util. Comm'n 1998).

<sup>14</sup> Cite to Steve Wicker

<sup>15</sup> Wicker

<sup>16</sup> "Wardriving is the act of searching for Wi-Fi wireless networks by moving vehicle. It involves using a car or truck and a Wi-Fi-equipped computer, such as a laptop or a PDA, to detect the networks. Wikipedia

<sup>17</sup> Crime fighting organizations often tell individuals not to put a vacation stop on their newspaper because the centralization of such information about multiple households with the newspaper creates an attractive data pool to would be thieves. Similarly, the ability to monitor energy consumption data as it feeds into the neighborhood concentrator provides an attractive place for thieves to gather information on multiple households at once and requires less resources than staking out individual houses or neighborhoods to visually assess the daily patterns of residents.

hand the Supreme Court relatively recently affirmed the primacy of privacy in the home by prohibiting the use of a thermal imager to gather details about the home previously inaccessible without a physical trespass—at least until such time as the technology to do so becomes widely available to the general public. On the other hand, the Court has an entrenched position that where the government obtains personal details from third-party business records the Fourth Amendment is not implicated. In the first instance the Court has resisted limitations on Fourth Amendment protections for the home premised on the quality or quantity of the data that can be known.<sup>18</sup> In contrast, the quality and quantity of the data in third party records clearly animates the existing Fourth Amendment case law finding no protection for personal details found in business records and has played a strong role in State Court decisions about the privacy protections provided by Fourth Amendment corollaries in state constitutions.<sup>19</sup> While eschewing an examination of the quality and quantity of information that devices reveal about the inside of the home, the Supreme Court has allowed the *location* of that information—in business records—to be completely determinative of the scope of Fourth Amendment protection.<sup>20</sup>

Under the Court’s jurisprudence it is quite plausible that information about energy consumption inside the home contained in the records of a public utility—regardless of how sophisticated and detailed it becomes or how much it can reveal about the residents—will be found unprotected by the Fourth Amendment while the use of a relatively unsophisticated “device” that enhances law enforcement officers’ senses, allowing them to retrieve far less detailed information about in-home energy consumption, will require a warrant. At least until these devices become widely available to the public—as we would suggest they are today.

We are interested in exploring the Court’s divergent Fourth Amendment analyses when considering technological advancements that directly enhance the ability of law enforcement to gather information, and data collection and retention advancements in the private sector that similarly enhance the ability of law enforcement to gather information. In the leading case examining the law enforcement use of a thermal imager to gather information about the heat signatures of a home the Court refused to consider the privacy issues about the “waste heat” emanating from the home as driven by the notions of voluntarily disclosure, assumption of the risk, or abandonment. These concepts are the animating force behind the business records decisions. But as a logical matter these concepts are a far better fit for the “waste heat” which is freely available for anyone with the right technology to “see” from a public vantage point than they are for the utility

---

<sup>18</sup> See *Karo* (beeper); *Hicks* (reg number on stereo); *Kyllo* (mj rejecting suggestion to base 4thA protection on whether the data revealed “intimate” activity)

<sup>19</sup> see *Miller* and *Smith*; cite state cases discussing capacity of business records to provide a “virtual biography”

<sup>20</sup> Thus, financial information in the home cannot be seized without a warrant, but the same financial information—revealing political contributions, memberships, purchasing patterns and personal and business relationships—held in bank records are completely unprotected by the U.S. Constitution. The importance of the location of information is striking in light of the Court’s stated disavowal of its earlier place-based conception of privacy protections in *Katz*.

records that are a necessary derivative of heating a home and are provided solely to the utility for the purpose of that service.

As more and more information about individuals' activities is collected and archived by the private sector the Court's disparate approach to considering the Fourth Amendment implications of direct collection of information by the government versus indirect collection from private sector entities (even where the data collection may be mandated by law) forces us to confront the possibility of a world with virtually no constitutional protection constraining government prying into citizen's private acts whenever those acts are recorded or can be inferred from data collected in the private sector. If details of individuals' in-home activities are directly recorded in or easily inferred from business records does the Fourth Amendment simply have nothing to say about the governments access and use of this information? Given that individuals are increasingly dependent on businesses to help them continually and in real-time manage activities and events in the home including the television they view, the nanny they hired, and the energy they use, will there be any private activities that remain outside the Fourth Amendment free-zone created by the business records case law?

This article considers the Fourth Amendment issues raised by the changes in the quantity and quality of the data that soon will be routinely available in utility records in California and eventually across the nation.<sup>21</sup> We begin our exploration of these questions in Part II by exploring the Court's Fourth Amendment analysis of law enforcement use of technologies that directly enhance their senses. We compare and contrast this with the Supreme Court's Fourth Amendment analysis and state courts' analysis of comparable state constitutional privacy protections in the context of business records that yield information similar to that available through technological devices. We consider the *Kyllo*, *Smith* and *Miller* cases and state constitutional decisions considering the privacy expectations in utility records. The comparisons highlight the inability of the Supreme Court's current Fourth Amendment jurisprudence to provide a rational and satisfying description of the privacy interests the constitution protects in a world of networks, devices, and personal services that by design collect and retain personal information on private acts. They also illustrate the flimsy protection likely found in the *Kyllo* cases narrow limitation on "government-only" technology.

As the information in utility records becomes more detailed the Court's disparate analysis of these two techniques for collecting information about activities taking place in the home leads to increasingly unsatisfying results from a normative perspective. The continued conclusion that personal information contained in third party business records is outside the Fourth Amendment is poised to obliterate the "firm line [the Fourth Amendment draws] at the entrance to the house."<sup>22</sup> We provide details of the DR

---

<sup>21</sup> This paper builds upon an ongoing collaborative effort at the University of California at Berkeley to study the security and privacy consequences of the overall demand response system, and work with policymakers, technologists and industry to identify and implement technical, policy and practices that can address them. Cec report

<sup>22</sup> *Payton* 445 US at 590

architecture in Section III and explore the ramifications of the business records case law in this context in Section IV.

In Part V, we conclude that the economics of information processing are changing in a manner that is shifting the scope and effect of the Court's business records doctrine. Technology that makes it cheaper and easier to collect and maintain information about customers, aligned with a service economy aimed at assisting individuals in managing their every need, activity and interaction, are diminishing the need for law enforcement to engage in the gumshoe surveillance activities of yesteryear or even the high-tech surveillance activities of yesterday. The private sector is subsidizing, at times displacing, the activities of law enforcement (and intelligence). The ability of law enforcement to cheaply and relatively easily access detailed profiles of individual household energy consumption or individual cell phone users' locations, or access and combine billions of records from a multitude of private sector sources containing personal information as was planned in the Total Information Assessment project will make the Fourth Amendment less and less useful as a tool for prescribing limits on what the government can know and in what circumstances about its citizens.

The evolution of the DR architecture provides a particularly stark example of the capacity of the business records case law to erode the core of Fourth Amendment protections. The cultural dependence on private sector services that generate records containing personal information about activities occurring within the home are blurring the "firm line" around the home that the founders sought to protect. But it is just one example in a growing list. The Court's disjointed approach to dataveillance<sup>23</sup> and surveillance cannot sustain the privacy of the home as the framers' or the current court envisioned it. By placing personal information contained in business records outside the scope of Fourth Amendment protection the Supreme Court has consigned us to a future without privacy.

---

---

<sup>23</sup> Roger Clarke