2008

Taking the Long View on the Fourth Amendment: Stored Records and the Sanctity of the Home

Jack I. Lerner

Deirdre K. Mulligan
Berkeley Law

Stanford Technology Law Review

Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home

JACK I. LERNER* AND DEIRDRE K. MULLIGAN**

CITE AS: 2008 STAN. TECH. L. REV. 3

> "[The] genius of our Constitution resides not in any static meaning that it had in a world that is dead and gone, but in the adaptability of its great principles to cope with the problems of a developing America. A principle to be vital must be of wider application than the mischief that gave it birth. Constitutions are not ephemeral documents, designed to meet passing occasions. The future is in their care, and therefore, in their application, our contemplation cannot be only of what has been but of what may be."
>
> William J Brennan, Jr., *State Constitutions and the Protection of Individual Rights*, 90 HARV. L. REV. 489, 495 (1977).

I. INTRODUCTION

In the wake of the California energy crisis of 2000-2001, the California Energy Commission (CEC) and California Public Utilities Commission (CPUC) began to pursue "demand response" energy programs in order to reduce peak energy demand. Demand response systems use pricing schemes such as tiered pricing or critical-peak pricing to influence customers to exert choice regarding when they use electricity, in the process reducing energy usage and shifting usage to non-peak hours.[1] Armed with information about the time-varying cost of electricity, residential and

* © 2008, Jack I. Lerner, Visiting Clinical Assistant Professor of Law and Acting Director of the USC Intellectual Property and Technology Law Clinic at USC Gould School of Law and Non-Resident Clinic Fellow, Samuelson Law, Technology & Public Policy Clinic, University of California—Berkeley School of Law (Boalt Hall)

** © 2008, Deirdre K. Mulligan, Clinical Professor of Law, Director, Samuelson Law, Technology & Public Policy Clinic, Director, Center for Clinical Education, University of California—Berkeley School of Law (Boalt Hall). The authors wish to thank: Gaymond Yee, Ron Hoffman, P.A. Subrahmanyam, David Wagner, Umesh Shankar, Erin Jones, Paul K. Wright, Nathan Ota, Steve Wicker, Arthur Rosenfeld, Kristy Chew, and the individuals from Charles River Associates International, Cornell Law School, eMeter Corporation, Levy Associates, Pacific Gas & Electric Company, San Diego Gas & Electric Company, Southern California Edison, the United States Department of Justice, and Utility Integration Solutions, Inc. who greatly assisted the authors in preparation of a report prepared for the Network Security Architecture for Demand Response/Sensor Networks project of the California Institute for Energy and Environment, see *infra* note 1; and Jennifer Granick, Matthew Lamberti, Maryanne McCormick, Robert Weisberg, Jeremy Brown, Jeremy Price, and the participants of the "Beyond a Physical Conception of the 4th Amendment: Search & Seizure in the Digital Age" Symposium at Stanford Law School.

[1] P.A. SUBRAHMANYAM, DAVID WAGNER, DEIRDRE MULLIGAN, ERIN JONES, UMESH SHANKAR & JACK LERNER, NETWORK SECURITY ARCHITECTURE FOR DEMAND RESPONSE/SENSOR NETWORKS 14 (2005, rev. 2006), *available at* http://www.ucop.edu/ciee/dretd/ (follow "Draft Final Report (pdf)" hyperlink) (report for the Network Security Architecture for Demand Response/Sensor Networks project, CIEE Award No. DR-04-03A, B, WA No. DR-005, under CEC/CII Prime Contract No. 300-01-043, conducted by CyberKnowledge and the University of California at Berkeley) [hereinafter NETWORK SECURITY ARCHITECTURE].

commercial customers are expected to reduce energy usage and/or shift their usage to non-peak, less costly hours. Such shifts, even if they do not create reductions in overall consumption, are expected to reduce the likelihood of energy brownouts and blackouts and provide direct savings to consumers.[2] Technologies to enable the demand response system, including advanced metering and in-home sensor and control technologies,[3] are now under development, and advanced meters are now being installed in the homes of Pacific Gas & Electric customers throughout Northern California.[4]

The collection of information about energy consumption from residential and commercial buildings at frequent intervals is a core component of the demand response system. 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, or less frequently. Over the next two to five years, however, 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.

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.[5] If all the data generated by demand response systems is retained, a customer's monthly record will shift from a record of one data point reflecting average monthly usage to a record of 750 to 3,000 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, but 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 demand response system will reveal variations in power consumption that, in turn, can be associated with various household activities. Over time, power consumption information can reveal personal sleep and work habits, the presence of certain medical equipment and other specialized devices, and, of course, signal the illegal behavior which today prompts law enforcement to seek it 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 if future "wardrivers"[6] detect and monitor the unencrypted traffic between household meters and neighborhood-level concentrators that relay energy usage information to the utilities. If a criminal were to monitor such communications to obtain information about occupancy on a per house, block, or neighborhood level, he or she could relatively easily assess the best time to burglarize homes or engage in other property crimes in a neighborhood.[7] How will the business models of utilities evolve

---

[2] David Cay Johnston, *Taking Control of Electric Bill, Hour by Hour*, N.Y. TIMES, Jan. 8, 2007, at A14, *available at* http://www.sfpower.org/pdf/nyt_energy_use_article.pdf (discussing savings of participants in a Chicago demand response pilot and Central Park New York City co-op that earned $3,000 selling unused energy capacity back to the utilities during a blackout in July 2006).

[3] *See, e.g.*, Scott Neumann et al., *The Missing Link*, PUBLIC UTILITIES FORTNIGHTLY, March 2007, at 52, *available at* http://www.ucop.edu/ciee/dretd/documents/Fortnightly%20Article%20Mar%2007.pdf.

[4] *See* NETWORK SECURITY ARCHITECTURE, *supra* note 1, at 22. 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. It is intended that the associated infrastructure support other operations, such as diagnosis and maintenance, but a discussion of such operations is beyond the scope of this paper. *Id.* at note a.

[5] *See infra* Part III.

[6] "Wardriving is the act of moving around a specific area and mapping the population of wireless access points for statistical purposes. These statistics are then used to raise awareness of the security problems associated with these types of networks (typically wireless)." JEFF MOSS, WARDRIVING: DRIVE, DETECT, DEFEND: A GUIDE TO WIRELESS SECURITY 3 (2004).

[7] Crime-fighting organizations often advise 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. *Cf.* Chronicle Staff Report, *Chronicle subscriber*

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 demand response systems be dealt with under the Fourth Amendment?

Existing legal precedents addressing the privacy of in-home activities, the energy they require, and the heat signatures they emit, point in different directions. On the one hand, in 2001 the Supreme Court affirmed the primacy of privacy in the home by prohibiting the use of a thermal imager to gather details about the home that would have been previously inaccessible without a physical trespass—at least until such time as the technology to do so becomes widely available to the general public.[8] This decision built upon previous judgments in which the Court maintained robust Fourth Amendment protections for the home based on the quality or quantity of the data that can be known.[9] On the other hand, firmly entrenched federal jurisprudence provides that where the government obtains personal details from third-party business records, the Fourth Amendment is not implicated.[10] Essentially, 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. 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 Fourth Amendment. At the same time, the Court's jurisprudence demonstrates continued respect for the sanctity of the home and for the expectation of privacy that attaches to activities taking place inside the physical boundaries of the home.

Under the Court's jurisprudence, it is 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—could be found to be unprotected by the Fourth Amendment. Meanwhile, 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).

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.[11] We begin our exploration of these questions in Part II by exploring the Court's Fourth Amendment analysis of law enforcement officers' 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, among others, and state constitutional decisions considering the privacy expectations with respect to 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

---

vacation information allegedly stolen, SAN FRANCISCO CHRONICLE, Nov. 10, 2007, at B3, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/11/10/BA4ET9PGL.DTL.

[8] Kyllo v. United States, 533 U.S. 27 (2001) (discussed *infra* Part II).

[9] *See* United States v. Karo, 468 U.S. 705, 716 (1984) (prohibiting government use of a beeper to determine without warrant whether a particular article or person is in a home at a particular time); Arizona v. Hicks, 480 U.S. 321, 327-28 (1987) (holding that moving stereo equipment in order to locate serial numbers constituted search and had to be supported by probable cause).

[10] *See* United States v. Miller, 425 U.S. 435 (1976) (*see infra* Part II); Smith v. Maryland, 442 U.S. 735 (1979) (*see infra* Part II).

[11] This article 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. In particular, this article relies on information gathered for NETWORK SECURITY ARCHITECTURE, *supra* note 1.

personal information on private acts. They also illustrate the flimsy protection likely found in *Kyllo*'s 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 what the Supreme Court has identified as the "firm line [the Fourth Amendment draws] at the entrance to the house."[12] We provide details of the likely demand response architecture in Part III.

In Part IV, we explore the ramifications of the business records case law in this context, and argue 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. The evolution of the demand response architecture provides a particularly stark example of the capacity of the business records case law to erode the core of Fourth Amendment protections, but it should be viewed in the context of a larger societal shift towards a heavily networked existence. In light of our growing cultural dependence on private sector services that generate records containing personal information about activities occurring within the home, by placing personal information contained in business records outside the scope of Fourth Amendment protection, the Supreme Court has effectively consigned us to a future without privacy. We therefore propose that the Court adopt a *Kyllo*-like test that asks whether the technology reveals information that otherwise would not be available absent a trespass into the home into its consideration of business records. In that decision, Justice Scalia, writing for five members of the Court, advocated taking "a long view" on the Fourth Amendment,[13] examining the future potential to intrude on the home rather than the limited heat pattern revealed by the thermal imager at issue.[14] It is time for the Court to take a "long view" on the capacity of business records to intrude on reasonable expectations of privacy in the home.

II. INFORMATION ABOUT ELECTRICITY CONSUMPTION: BUSINESS RECORD OR "VIRTUAL CURRENT BIOGRAPHY"?

The issue of whether the Fourth Amendment protects information about the in-home use of electricity has arisen in two distinct contexts: access to residential records held by utilities and police use of thermal imaging devices to detect heat loss of a residence. In drug investigations, police use both techniques to identify abnormal energy consumption patterns that may indicate in-home marijuana production.

Under existing Supreme Court precedent, these two methods of obtaining information about in-home energy consumption could result in very different outcomes under the Fourth Amendment. Based on the Supreme Court's jurisprudence regarding third-party business records, the first, accessing utility records, would likely not be found to violate the reasonable expectation of privacy protected by the Fourth Amendment.[15] The latter, use of a thermal imaging device, has been held by the Court to invade the reasonable expectation of privacy the Fourth Amendment protects and therefore to require a warrant prior to police use.[16] The disparity in Fourth Amendment protection

---

[12] Payton v. New York, 445 U.S. 573, 590 (1980).

[13] *Kyllo*, 533 U.S. at 103, 106.

[14] *Kyllo*, 533 U.S. at 103.

[15] While the Court has not ruled on utility records directly, it has found no Fourth Amendment interest in a range of records that reveal information about individuals. *See infra* Part II. Several state courts have decided that utility records fall outside the privacy protection afforded by state constitutional equivalents of the Fourth Amendment based largely on the federal business records doctrine. In an earlier article, one of the authors argues against an expansive reading of the business records case law, concluding that the cases limited Fourth Amendment protection only where the business has an independent interest in the records, the records are disclosed to the business for its use, and the substance of the record is not expressive. *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004).

[16] *Kyllo*, 533 U.S. at 27.

hinges largely on a line of 1970s cases finding that individuals have no reasonable expectation of privacy in business records containing their personal information.[17]

State case law finding utility records to be outside the protection afforded by state constitutional equivalents of the Fourth Amendment can be divided into two categories. The bulk of state courts that have ruled on the issue have interpreted state law privacy provisions in a manner consistent with the Supreme Court's business records reasoning, holding that the records voluntarily disclosed to the utilities are afforded no protection. A small number of state courts have found that the records are protected under state constitutional provisions, but have nevertheless found lower levels of procedural protection sufficient upon concluding that only limited privacy interests were at stake.

A. Kyllo v. United States

The Fourth Amendment of the U.S. Constitution and the California Constitution both provide protections against unreasonable government intrusions into the home.[18] Supreme Court jurisprudence under the Fourth Amendment has long held that activities within the four walls of the home, even illicit activities, warrant special protection from intrusion by law enforcement. In 2001, the United States Supreme Court decided in *Kyllo v. United States* that law enforcement agents may not use sense-enhancing technology that is capable of revealing both illegal and legal activity that is not readily available to the public to reveal activity within the home, regardless of whether the information discovered is incriminating.[19] It is a decision that exemplifies the high level of privacy and freedom from surveillance that people can reasonably expect in their homes.

In 1992, federal agents, suspecting that marijuana was being grown in Danny Kyllo's Florence, Oregon triplex, used an Agema Thermovision 210 thermal imager to scan the property for infrared radiation created by high-intensity lamps.[20] The imager "converts radiation into images based on relative warmth—black is cool, white is hot, shades of gray connote relative differences."[21] The scan showed patches of relative heat on a side wall and the roof over the garage. Based on this information and other evidence such as tips from informants and utility bills, a federal magistrate judge issued a warrant authorizing a search of Kyllo's home; in the subsequent search, federal agents found over 100 plants. Kyllo challenged the warrant. On remand from the Ninth Circuit, the district court found that the Agema is a "non-intrusive device which . . shows a crude visual image of the heat being radiated from the outside of the house" that did not reveal people, activities, or conversations inside the home and upheld the warrant. The Ninth Circuit affirmed the district court's decision.

The Supreme Court reversed. Justice Scalia, writing for a 5-4 majority, declared that while visual surveillance had always been lawful, "[t]he present case involves officers on a public street engaged in more than naked-eye surveillance of a home . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[22] The Supreme Court focused its analysis of that question on two details of the sense-enhancing technology employed. First, the Court asked, was the technology in common use at the time, such that residents of the house might have expected the technology to be used against them? The thermal-imaging device in this case was uncommon and not publicly available, so the surveillance was improper without a warrant. Second, would the information gathered be otherwise accessible without entering the home? The information gained by the imaging device in this case would not otherwise be available from outside, and so again, the surveillance was improper.[23]

---

[17] *See infra* Part II.B.

[18] U.S. CONST. amend. IV; CAL. CONST. art. I, § 13.

[19] *Kyllo*, 533 U.S. 27.

[20] *Id.* at 29.

[21] *Id.* at 29-30.

[22] *Id.* at 33-34.

[23] *Id.* at 34-40.

In *Kyllo*, the Court rejected the notion that there is a difference between "off-the-wall" surveillance and "through-the-wall" surveillance in light of the steady advance of technology. To draw such a distinction without regard to the power of the technology "would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home."[24] Besides, noted the Court, "[i]n the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes,"[25] and in any event, thermal-imaging might disclose "at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate' "[26] As a result, "we must take the long view, from the original meaning of the Fourth Amendment forward."[27]

It is useful to think about privacy in a demand response setting by considering the two key questions from *Kyllo*. First, will new technologies that make information on in-home activity available to other persons outside the home—information such as occupancy, movement, or any other behavior that otherwise would not be visible from outside—cross the line set by the Supreme Court and violate a person's rightful expectation of privacy inside his home? It is possible that by mining energy data in a relatively straightforward way, one might be able to discover enough about in-home behavior to cross this line. Second, might the test set forth in *Kyllo*, in which the expectation of privacy is dynamic—tied to the novelty of the technology used to invade it—mean that the expectation of privacy could be eroded over time, as demand response technologies become commonplace?[28] We think not. *Kyllo* soundly reaffirmed the sanctity of the home and the Court's view that an expectation of privacy in activities taking place inside the home is presumptively reasonable. Thus, courts should "take the long view on the Fourth Amendment" and maintain this presumption despite the fact that technology may become increasingly invasive.

B. Federal Business Records Jurisprudence[29]

The Supreme Court has not ruled on utility records directly, but it has held that no Fourth Amendment interest exists in a range of records kept by third parties that reveal information about individuals.

In *Couch v. United States*,[30] the Court held that the Fourth Amendment did not apply to records that a business had voluntarily provided to an independently employed accountant.[31] The Court reasoned that business owners cannot legitimately expect the records they give to outside accountants—with whom there is no recognized confidential privilege—to be private.[32]

The business records doctrine was further developed in *United States v. Miller*.[33] In that case, a defendant in a criminal trial had moved to suppress copies of financial records that federal agents had obtained from a bank.[34] The Court held that under the Bank Secrecy Act of 1970, such documents were not private papers but rather business records belonging to the bank.[35] The Court did not rule

---

[24] *Id.* at 35-36.

[25] *Id.* at 37.

[26] *Id.* at 38.

[27] *Id.* at 40.

[28] Other commentators have discussed the dynamism and circularity of the reasonable expectation of privacy test. *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case For Caution*, 102 MICH. L. REV. 801, 808 (2004); Susan Friewald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 39 & n.205 (2004).

[29] Congress has enacted statutory protections of electronic communications and other information held by third parties, most notably in the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in various sections of 18 U.S.C.). This statute provides some protection, although the protection can be uneven. *See generally* Mulligan, *supra* note 15. A discussion of federal and state statutory protections and their applicability to information held by third parties is outside the scope of this article.

[30] Couch v. United States, 409 U.S. 322 (1973).

[31] *Id.* at 325, 336.

[32] *Id.* at 335-36.

[33] *Miller*, 425 U.S. 435.

[34] *Id.* at 436-37.

[35] *Id.* at 440-41.

on any other types of records, but noted that it would have to "examine the nature of particular documents . . . in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[36]

Finally, in *Smith v. Maryland*,[37] the Court held that law enforcement officers did not need a warrant, or even a court order, to ask a telephone company to monitor the numbers a particular customer dialed.[38] The Court concluded that telephone users could not reasonably expect the numbers they dial to be private because, through the act of dialing, they voluntarily shared the numbers they were dialing with the telephone company.[39]

Although the business records doctrine has been widely criticized,[40] it is firmly established, and the lower federal courts have repeatedly applied it to new types of information held by third parties, including utility records information.[41] In the 1992 case *United States v. Starkweather*,[42] for example, the United States Court of Appeals for the Ninth Circuit applied Supreme Court jurisprudence on third-party information to electric utility records. Citing *Smith* and *Miller*, the court noted that it had previously rejected the argument that telephone company billing records are protected by the Fourth Amendment, since the "public awareness that such records are routinely maintained . . . negate[s] any constitutionally sufficient expectation of privacy regarding the records."[43] Without further discussion, the court concluded, "[w]e see no principled reason to accord electric utility records any different status under the Fourth Amendment than that accorded bank or telephone records."[44] Similarly, in *United States v. Hamilton*, the United States District Court for the District of Oregon held that no warrant was required to obtain power consumption records for the defendant's home.[45] Relying on *Smith v. Maryland*, the court distinguished utility records from the thermal imaging device at issue in *Kyllo*. "[W]hen Mr. Hamilton used power in his home," the court reasoned, "he voluntarily conveyed that information to PGE, his electric company. As a result, he had no reasonable expectation of privacy in his power records."[46]

It is useful to examine why the Court in *Kyllo* did not find an abandonment rationale persuasive. The Court could have concluded, as Justice Stevens urged in his dissenting opinion, that Kyllo had abandoned the heat radiating from his house in the same way that the defendants in *California v. Greenwood*[47] abandoned their garbage.[48] The animating concepts behind the business records doctrine are abandonment, voluntary disclosure, and assumption of risk. These seem like a good fit for the "waste heat" which is freely available for anyone with the right technology to "see" from a public vantage point when compared to utility records which are a necessary derivative of heating or powering a home and are provided solely to the utility for the purpose of that service. We think the Court did not adopt this rationale in part because heat or radiation emanating from a home is not released voluntarily, and more importantly because this technology can be used to observe activities taking place inside the home.[49] In short, by taking a "long view" on the Fourth Amendment, the

---

[36] *Id.* at 442.

[37] *Smith*, 442 U.S. 735.

[38] *Id.* at 745-46.

[39] *Id.* at 743-44.

[40] *See* WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.7(c), at 511-17 (2d ed. 1987); Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 n.7 (2006).

[41] *See, e.g.*, United States v. Hambrick, No. 99-4793, 2000 WL 1062039 (4th Cir. Aug. 3, 2000) (unpublished disposition) (internet service provider information).

[42] United States v. Starkweather, No. 91-30354, 1992 WL 204005 (9th Cir. 1992) (table) (unpublished disposition).

[43] *Id.*

[44] *Id.*

[45] United States v. Hamilton, 434 F. Supp. 2d 974, 980 (D. Or. 2006).

[46] *Id.*

[47] California v. Greenwood, 486 U.S. 35 (1988).

[48] *Kyllo*, 533 U.S. at 41 (Stevens, J., dissenting).

[49] *Cf.* United States v. Sharpe, 470 U.S. 675, 700 (1985) (Marshall, J., concurring) (quoting Johnson v. United States, 333 U.S. 10, 13 (1948) for the proposition that "[O]dors alone do not authorize a search without warrant").

Court reaffirmed the sanctity of the home and the expectation of privacy regarding activities in the home.[50]

C. Federal Business Records Under State Constitutional Law

A plurality of states that have addressed business records in the context of their state constitutional law have followed the Supreme Court's lead and held that such records fall outside the privacy protection afforded by state constitutional equivalents of the Fourth Amendment. This jurisprudence is based for the most part on the business records doctrine set forth in *Smith* and *Miller*.[51] For example, in 1993 the Supreme Court of Kansas adopted the rationale of *Miller* in holding that Kansas citizens have no right to privacy in their bank records under § 15 of the Bill of Rights to the Kansas Constitution.[52]

Other states reject the third-party doctrine in certain instances. California is the most notable of these; in *Burrows v. Superior Court*,[53] the California Supreme Court found a reasonable expectation of privacy in bank records. Brennan based his dissent in *Miller* on Justice Mosk's reasoning in *Burrows*: [54]

> For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography.[55]

A small number of states have found that business records are protected under state constitutional provisions, but also concluded that only a limited privacy interest is at stake and, as a result, have found lower levels of procedural protection sufficient.[56]

Still other states diverge from the federal Fourth Amendment jurisprudence but have not repudiated the third-party doctrine, and some of these have held that no constitutional protection exists for utility records. For example, Alaska's constitution has a privacy amendment,[57] but in 1996 the Court of Appeals of Alaska decided that "utility records . . do not constitute information in which society is prepared to recognize a reasonable expectation of privacy."[58] It is worth noting, however, that this opinion and similar opinions in other states base their holdings on the coarse nature of the discoverable data and the fact that such data cannot identify any activities taking place

---

[50] Several commentators have noted the continuing importance of physical location in Fourth Amendment jurisprudence. *See, e.g.*, Melissa Arbus, *A Legal U-Turn: The Rehnquist Court Changes Direction and Steers Back to the Privacy Norms of the Warren Era*, 89 VA. L. REV. 1729, 1735-43 (2003) (discussing importance of private property and trespass doctrine in post-*Katz* cases despite the Court's rejection of the primacy of trespass analysis in *Katz*); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 125-32 (2004) (identifying principles that dominate public discourse and judicial decisions about privacy, including curtailing intrusions into places deemed private or personal).

[51] *See generally* Henderson, *Learning from All Fifty States*, *supra* note 40 (surveying state law jurisprudence on third party business records); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. (forthcoming 2007). Henderson's research indicates that eighteen states have not diverged from the substantive Fourth Amendment, eleven states have rejected the federal third-party doctrine, eleven states might reject the federal third party doctrine, and ten states sometimes diverge from the Fourth Amendment but have given no reason to believe that they will reject the federal third-party doctrine. Henderson, *Learning from All Fifty States*, *supra* note 40, at 395.

[52] State v. Schultz, 850 P.2d 818 (Kan. 1993).

[53] Burrows v. Superior Court, 529 P.2d 590 (Cal. 1974).

[54] California courts have also held that consumers do have a reasonable expectation of privacy in some records held by telecommunications public utilities. *See* People v. Chapman, 679 P.2d 62 (Cal. 1984) (holding that a customer who paid to keep her name, phone number, and address unlisted in telephone directories had a reasonable expectation of privacy in that data, and so a warrant was required to obtain that data from the telephone company); *see also In re* Pacific Bell, 44 C.P.U.C.2d 694 (Cal. Publ. Util. Comm'n 1992).

[55] *Burrows*, 529 P.2d at 596.

[56] *See, e.g.*, *In re* Maxfield, 945 P.2d 196 (Wash. 1997); State v. Maxwell, 791 P.2d 223 (Wash. 1990); *In re* Rosier, 717 P.2d 1353 (Wash. 1986), *superseded by statute*, Freedom of Information Act Amendments of 1987, ch. 403, 1987 Wash. Laws, § 1, 1546 (recodified at WASH. REV. CODE ANN. § 42.56.050 (West 2007)).

[57] ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.").

[58] Samson v. Alaska, 919 P.2d 171, 173 (Alaska Ct. App. 1996).

inside the home. Thus, reasoned the Alaska court, the billing data does not require a warrant because it "do[es] not identify any activities" of the suspect, nor does it "provide any intimate details of [the suspect's] life, identify his friends or political and business associates, nor does it provide or complete a 'virtual current biography.' The power records, unlike telephone or bank records, do not reveal discrete information about [the suspect's] activities."[59]

Like the Alaska court, both state and federal courts have repeatedly cited the coarse nature of electricity usage data as justification for holding that there is no reasonable expectation of privacy in power consumption information. For example, in a case where police used data collected from a specially installed surveillance electricity meter to obtain a search warrant to look for marijuana plants, the California Court of Appeal reasoned that because the metering information does not reveal information about activities within the home, there is no constitutional protection:

> The surveillance meter neither measures nor reveals anything about the intimate details of activities within the house. The technology employed does not tell those monitoring it what electrical devices are inside the house or what activities the power supports. The meter does not discriminate between electricity used to fire pottery and power used to grow orchids, tomatoes or marijuana. It only tells officers how much electricity is being delivered by the utility and, by comparison to billing records, whether it is being diverted or stolen.[60]

Similar conclusions denying reasonable expectations of privacy in utility records based on how little the data reveals have been drawn in other state and federal courts.[61] This reasoning suggests that metering information that discloses fine-grained usage information may be more likely to be held to fall within a reasonable expectation of privacy than traditional monthly collection of aggregate utility data.

III. DEMAND RESPONSE IMPLEMENTATION

A. Utility Records in the Era Before Demand Response

Energy bills differ from one provider to another, but until recently, they all contained relatively coarse readings of energy consumption. For example, a bill from San Diego Gas and Electric provides information about average daily consumption of kilowatts during the billing period, overall usage data, and comparative information about energy use the preceding month and the same month in the last calendar year.[62] The information available in utility bills is retrospective and does not reveal daily patterns of energy consumption, nor does it reveal information about where within the home energy is used or the purpose for which the energy is used. Importantly, it is difficult to infer information about activities taking place within the home from the data available. For example, greater than normal energy consumption can be due to excessive (as compared to average) laundry washing patterns, halide lighting, or another source.[63] The records at the energy company would not provide insight into which activity was draining the power.

Infrared sensing devices are used by law enforcement to detect heat loss from a residence. Information derived from the use of thermal imagers is used to support an application for a warrant to search the home. The infrared sensing devices detect relative patterns of heat, allowing law enforcement to compare the heat emanating from various parts of a residence and to compare the heat patterns of neighboring homes to the residence at issue. A large amount of heat loss is typical of the halide lights common in indoor marijuana-growing operations.

---

[59] *Id.* at 173 (quoting State v. Kluss, 867 P.2d 247, 254 (Idaho Ct. App. 1993)).

[60] People v. Stanley, 86 Cal. Rptr. 2d 89, 94 (Cal. Ct. App. 1999).

[61] *See* People v. Dunkin, 888 P.2d 305 (Colo. App. 1994); *Kluss*, 867 P.2d 247. *See also* United States v. Delgado, 121 F. Supp. 2d 631 (E.D. Mich. 2000); United States v. Boger, 755 F. Supp. 333 (E.D. Wash. 1990).

[62] *See, e.g.*, San Diego Gas & Electric Company, Understanding Your Gas And Electric Bill, http://www.sdge.com/customer/aboutyourbill.shtml (last visited Oct. 1, 2007) (follow "Sample SDG&E Bill" hyperlink).

[63] *Kluss*, 867 P.2d at 254 ("High power usage may be caused by any one of numerous factors: hot tubs, arc welders, poor insulation, ceramic or pottery kilns, or indoor gardening under artificial lights.").

The most common use of energy records in a criminal case is to establish or confirm residency at an address. Using the records as evidence that a residence is using extraordinary amounts of energy, thus corroborating evidence of a home marijuana-growing operation, is the next most likely use, but is relatively rare. Records may be sought at many stages of a case. Usage records may be sought early in a marijuana home-growth case to support a tip or preliminary evidence, and build a case for a search warrant. Records of usage and billing may alternatively be sought later, when more evidence is in hand, to show that the person paying the energy bill must have had knowledge of the illegal activity.[64]

In non-emergency situations, records are typically sought using a grand jury subpoena,[65] as utilities in California usually do not exercise their option to release customer data to law enforcement voluntarily. It is also believed that subpoenaed records appear stronger in court, which encourages law enforcement to use subpoenas. Obtaining a grand jury subpoena is simple—in some cases, it takes as little as ten minutes. The records sought are typically copies of energy bills, records of payment, and internal records identifying the subscriber.[66]

Current utility practices include saving many years' worth of customer usage data to enable customer disputes, and these data storage practices are expected to continue.[67]

B. Implementation of Demand Response and Advanced Metering

In response to the blackouts of 2000-2001, the California Public Utilities Commission and the California Energy Commission commenced a joint rulemaking "to develop demand response as a resource to enhance electric system reliability, reduce power purchase and individual consumer costs, and protect the environment."[68] The term "demand response" refers to a means by which pricing information or other signals are used to influence customers to exert choice regarding when they use electricity, in the process reducing energy usage or shifting usage to non-peak hours.[69] Various technologies may be used to achieve these results, including advanced metering research and development, in-home sensor and control technologies development, a robust communication network that will use both wired and radio signals to transmit usage and other data, and the aggregation of energy usage and billing information. In 2003-2004, a pricing pilot program in California explored the feasibility of several time-varying rates, ways to communicate those rates, and customers' reactions to them.

California's major investor-owned utilities have submitted various proposals to the CPUC for extensive deployment of advanced meters and related infrastructure, as well as "dynamic pricing tariffs."[70] Investor-owned utilities Pacific Gas & Electric and San Diego Gas & Electric have requested permission to begin pre-deployment and deployment of advanced metering infrastructures, and Southern California Edison has requested permission to develop an advanced integrated meter

---

[64] The fact that a suspect pays the electric bill at an address may be used to infer that he has some knowledge or control of events that take place at or contraband that is found in the residence.

[65] Some agencies have their own administrative subpoena power and obtain records through a different process.

[66] Although there is no clear rule prohibiting law enforcement from requesting customer data for a neighborhood or larger area (and either sifting through it looking for a suspiciously high usage to target a suspect in a neighborhood where marijuana growth is suspected, or using the neighborhood data to show that a suspect's usage is high compared to neighbors'), in most cases the only records requested are those of the suspect's individual residence.

[67] Data is typically stored for seven years. *See* Cal. Pub. Util. Code § 736; Utility Audit Co. v. Southern Cal. Gas Co., Decision 98-09-061, Case 97-02-015, 1998 Cal. P.U.C. LEXIS 1097 (Cal. Pub. Util. Comm'n Sept. 17, 1998). *See also* Network Security Architecture at 38, *supra* note 1, at 87.

[68] Pacific Gas & Electric Co., Decision 06-07-027, Application 05-06-028, 2006 Cal. P.U.C. LEXIS 274, at *3 (Cal. Pub. Util. Comm'n July 20, 2006) (final opinion). *See also* California Energy Commission, Demand Response Proceeding Instituting Rulemaking, http://energy.ca.gov/demandresponse/index.html (last visited Oct. 24, 2007); California Public Utilities Commission, Demand Response and Advanced Metering, http://www.cpuc.ca.gov/static/hottopics/1energy/r0206001.htm (last visited Oct. 24, 2007).

[69] NETWORK SECURITY ARCHITECTURE, *supra* note 1, at 14.

[70] *Id.* The pilot study was enacted in CAL. PUB. UTIL. CODE § 393 (West 2007) (effective Jan. 1, 2001). For reports on the study, *see* California Energy Commission, Documents Related to the Demand Response Proceeding, http://energy.ca.gov/demandresponse/documents/index.html (last visited Oct. 24, 2007).

to support a future deployment.[71] In July 2006, the CPUC authorized PG&E to spend (and bill ratepayers) $1.7 billion to deploy advanced meters throughout its territory, which would involve upgrading five million electric meters and four million gas meters over the following five years.[72] These meters are expected to allow PG&E to "monitor its electrical load on an hourly basis," "conduct remote meter reading, pinpoint outages, [provide] remote turn off/turn on capability, [e]nable two-way communication to each customer's meter[,] [and] offer time varying rates to all of its customers," among other capabilities.[73] The CPUC has also approved funding for SDG&E pre-deployment activities.[74]

Advanced metering capabilities that are now being implemented will employ refurbished meters having a data collection module with hourly readings and transmission of raw data to the utility.[75] Later meters may contain more internal processing and data storage capability. The data set the meter will send to the utility is expected to contain a unique meter identifier, a timestamp, hourly usage data, and some kind of time synchronization information.[76]

The availability of hourly usage data will be a major change for utilities, and it is not yet clear how this data will be used and distributed to utility subsystems, although they do anticipate using raw usage data for customer service, billing, and automatic meter activation. Customer service departments may use usage data and profiles to provide counseling to customers on how to reduce their bill, and they may also wish to query the meter in real time. In addition, as demand response pricing systems become more complex and the billing rate changes with time, utility billing departments may need more detailed data to be able to calculate the bill.[77]

Although there has been some discussion of a meter that would have sufficient processing and storage capability to compute a customer's bill on the customer's premises, such meters are thought to be prohibitively expensive and are not currently being planned.[78] In the long term, however, technology is being developed that would place numerous sensors in the home that communicate wirelessly with a more sophisticated meter. The meter would learn the customer's preferences and habits by monitoring and receiving information from sensors dispersed throughout the home, including occupancy sensors and sensors on power outlets, power cords, or appliances.[79] Such in-home systems are being studied by researchers at the University of California-Berkeley.[80]

In short, rather than containing one data point reflecting average monthly use, customers' utility records may soon contain 750 to 3,000 distinct and time-stamped data points per month that reflect actual energy use. The information about in-home activity that can be determined from this data is

---

[71] The advanced metering pre-deployment and deployment cases filed with the CPUC include: A. 05-03-016 and A. 05-06-028 (PG&E), A. 05-03-015 and A. 05-06-017 (SDG&E), and A. 05-03-026 (SCE).

[72] California Public Utilities Commission, *PUC Approves SmartMeters for PG&E Customers*, CALIFORNIA PUBLIC UTILITIES COMMISSION NEWS RELEASE, July 20, 2006, at 1, http://www.cpuc.ca.gov/word_pdf/NEWS_RELEASE/58233.pdf; *see also* Pacific Gas & Electric Co., 2006 Cal. P.U.C. LEXIS 274, at *4 n.2, *96.

[73] *PUC Approves SmartMeters for PG&E Customers*, *supra* note 72, at 1.

[74] A decision in the PG&E rate setting case was issued September 22, 2005. Pacific Gas & Electric Co., Decision 05-09-044, Application 05-03-16, 2005 Cal. P.U.C. LEXIS 438 (Cal. Pub. Util. Comm'n Sept. 22, 2005). A decision on the SDG&E pre-deployment filing was issued August 25, 2005. San Diego Gas & Electric Co., Decision 05-08-018, Application 05-03-015, 2005 Cal. P.U.C. LEXIS 567 (Cal. Pub. Util. Comm'n Aug. 25, 2005).

[75] NETWORK SECURITY ARCHITECTURE, *supra* note 1, at 36; PG&E Smart Meter, http://www.pge.com/smartmeter/ (last visited Dec. 14, 2007).

[76] *Id.* at 37.

[77] The utilities also anticipate that advanced metering data will be available for monitoring demand load or voltage variation at transformers, thus allowing customization of transformer size, detection of load imbalance, rerouting, and rebalancing. Utilities look forward to using advanced metering data for research tasks like load profiling, rate design, and program evaluation, but these systems will likely not have access to real-time usage data. Some utilities expect to be able to accomplish research tasks using only subsets or samples of the usage data. Others look forward to data mining the entire set. Since data is not routed to researchers in real time, there is the ability to preprocess the data that is released.

[78] NETWORK SECURITY ARCHITECTURE, *supra* note 1, at 39; Pacific Gas and Electric Company, PG&E SmartMeter, http://www.pge.com/smartmeter/ (last visited Dec. 11, 2007).

[79] *Id.* at 40-41; *see, e.g.*, PIER Demand Response Research Center, A National Town Meeting & Symposium on Demand Response, June 26-27, 2008, http://drrc.lbl.gov/drrc-DRtownmtg-ppt.html.

[80] *Id.*

radically different from the traditional model. Electricity consumption patterns generated from advanced metering infrastructure will reveal variations in power consumption that can be associated with various household activities; detailed power consumption information can reveal personal sleep, work, and travel habits, and likely identify the use of medical equipment and other specialized devices (if not ordinary appliances). No longer can utility records be said not to "identify any activities" of a resident or "provide . . intimate details of [the suspect's] life."[81] Unlike in *Samson v. Alaska*, these records could likely be used to "reveal discrete information about [the suspect's] activities."[82]

In effect, the data generated by demand response technology is more like infrared sensing devices than traditional utility records. Like the data provided by the Agema Thermovision 210 at issue in *Kyllo*, such data might reveal "at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate'; and a much more sophisticated system might detect nothing more intimate than the fact that someone left a closet light on."[83] This will be much more likely, of course, if the sensor-based systems now in development see widespread implementation. Because the information is held by a private third party, however, and because the consumer has a contractual relationship with the utility, such information might be considered by some courts to be nothing more than business records that fall outside the purview of the Fourth Amendment.

IV. THE FOURTH AMENDMENT, DEMAND RESPONSE, AND THE NEW POWER OF REMOTE INFORMATION PROCESSING AND STORAGE

As more and more information about individuals' activities is collected and archived by the private sector, the Court's disparate treatment of direct collection of information by the government versus indirect collection by 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 investigation into citizens' 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 government's access and use of this information? Given that individuals are increasingly dependent on businesses to help them manage activities and events in the home—including the television they view, the nanny they hire, 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?

To obtain information lawfully about activity inside a home, law enforcement agents generally must obtain a warrant or receive permission to "enter" the home, even if "entry" does not entail setting foot inside the threshold. Private parties wishing to access and use information stored in the home must subpoena it and obtain a court order requiring production; otherwise, they must trespass upon private property to obtain it. In all instances, the law provides strong protections against access to personal information and other items maintained in the home. Any data on personal behavior, habits, or energy usage that is maintained inside the home is customarily afforded the same high level of privacy protection against both private party and government intrusions. The individual is able to exercise the highest level of control over the reuse and disclosure of personal information maintained inside the home.

In recent years, however, consumer technologies and the networks that connect them have become more pervasive, sophisticated, and intrusive. Increasingly, such technologies and networks are making the boundaries of the home porous, as evidenced by devices such as cable set-top boxes and internet connections, both of which are routinely monitored outside the home by the service provider. Unlike these services, however, electricity is a necessary component of modern life, and the

---

[81] *Samson*, 919 P.2d at 173 (quoting *Kluss*, 867 P.2d 247).

[82] *Id.*

[83] *Kyllo*, 533 U.S. at 38.

disclosure of power consumption to a utility company for billing or other limited business purposes should not relinquish the entirety of an individual's interest in the privacy of those records, especially where they contain information that is 750 to 3,000 times more detailed than the data now being collected. Unlike traditional usage information stored by the utility, this much data allows one to determine when a person is customarily home and when he or she is away, when a person sleeps, when a person bathes, the relative number of people in a home, and possibly even which appliances a person is using—no less than a "virtual current biography" of in-home activity.[84]

In light of our growing cultural and practical dependence on private sector services that generate records containing personal information about activities occurring within the home—and particularly in light of the impending collection of incredibly detailed electricity usage information—by placing personal information contained in business records outside the scope of Fourth Amendment protection, the Supreme Court has effectively consigned us to a future without privacy. In *Kyllo*, the Court advocated taking "a long view" on the Fourth Amendment,[85] finding relevance in the future potential to intrude on the home rather than the limited heat pattern revealed by the thermal imager at issue.[86] As technology begins to collapse these two doctrines, we propose that the Court take *Kyllo*'s "long view" with respect to business records. When confronted with a business record or other information held by a third party, the Court should ask whether the record, or the technology used to create the record, reveals information about activities taking place inside the home that otherwise would not be available absent a trespass into the home. The Court should further inquire as to whether the consumer has been able to exercise any real choice about whether to create such records, or whether to maintain such records in the home.[87] Because consumers have a reasonable expectation of privacy in activities that take place inside the home, if the answer to both questions is yes, then the information should be deemed to fall within the purview of the Fourth Amendment, and law enforcement officials should be required to obtain a warrant before being given access to those records. Under this test, information about in-home activities generated by advanced meters or sensors in a demand response system would be protected by the Fourth Amendment. In contrast, information gleaned from garbage placed on the curb, for example, would not receive such protection because the user voluntarily released the garbage outside the home.

Unlike *Kyllo*, we do not recommend that the test depend on whether the government uses the technology at issue, nor on whether the technology is widely available to the public. The animating principle in *Kyllo* is the preservation of privacy in the home in the face of invasive technologies, and in light of that principle, the increasingly digitized and networked nature of our existence[88] should not vitiate the sanctity of the home and the expectation of privacy that individuals and society continue to maintain about activities taking place in the home. It is high time for the Court to take a "long view" on the capacity of business records to intrude on reasonable expectations of privacy in the home.

---

[84] *Burrows*, 529 P.2d at 596.

[85] *Kyllo*, 533 U.S. at 40; *see also id.* at 36 ("[T]he rule we adopt must take account of more sophisticated systems that are already in use or in development.").

[86] *Id.* at 35-36 (rejecting the government's and dissent's argument that thermal imagining should be upheld because it detected only heat radiating from the external surface of the house, instead asserting that "[r]eversing [the approach in *Katz*] would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home . . . the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

[87] From a practical standpoint, such an outcome is likely not possible. Instead, we have proposed a rule that would appeal to a wide set of stakeholders while protecting particularly problematic records, such as the demand response-generated records, and placing reasonable limits on the business records doctrine.

[88] *See generally* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005); Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83 (2006).