Before the Public Utility Commission

Utility Commission

Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System	Rulemaking 8-12-009 (Filed December 18, 2008)

Comments of the Electronic Privacy Information Center (EPIC) on Proposed Policies and Findings Pertaining to the EISA Standard Regarding Smart Grid and Customer Privacy

Lillie Coney, Associate Director, coney@epic.org
Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue, NW, Suite 200
Washington, DC 20009
202-483-1140

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment and constitutional values. EPIC has a long-standing interest in privacy and technology issues.[1] EPIC has a specialized area of expertise regarding digital communication technologies and privacy policy.[2] EPIC has a particular interest in the privacy implications of the Smart Grid standards, as we anticipate that this change in the energy infrastructure will have significant privacy implications for American consumers.[3] In other similar areas, EPIC has consistently urged federal agencies to minimize the collection of personally identifiable information (PII) and to establish privacy obligations when PII is gathered. see http://epic.org/.

EPIC appreciates this opportunity to submit comments before the California Public Utility Commission on the topic of Smart Grid and Privacy.[4] The term "Smart Grid" encompasses a host of inter-related technologies rapidly moving into public use to reduce or better manage electricity consumption. Smart Grid systems may be designed to allow electricity service providers, users, or third-party electricity usage management service providers to monitor and control electricity use.

---

[1] EPIC, Electronic Privacy Information Center, http://www.epic.org (last visited Dec. 1, 2009).
[2] EPIC, Privacy, http://www.epic.org/privacy/default.html (last visited Dec. 1, 2009).
[3] EPIC, The Smart Grid and Privacy, http://epic.org/privacy/smartgrid/smartgrid.html (last visited Dec. 1, 2009).
[4] California Public Utility Commission, Assigned Commissioners and Administrative Law Judge's Joint Ruling Amending Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid, Feb. 8, 2010 http://www.cpuc.ca.gov/EFILE/RULINGS/113482.pdf .

Privacy implications for Smart Grid technology deployment centers on the collection, retention, sharing, or reuse of electricity consumption information on individuals, homes, or offices. Fundamentally, Smart Grid systems will be multi-directional communication and energy transfer networks that enable electricity service providers, consumers, or third-party access to customer information.

Privacy is one of the most fundamental and basic of human rights. Without it, many other rights, such as the freedoms of speech, assembly, religion and the sanctity of the home, would be jeopardized.

SMART GRID DEPLOYMENT PLANS AND PRIVACY

Fundamentally, Smart Grid systems will be multi-directional communications and energy transfer network that enables electricity service providers, consumers, or third-party use of data. The focus for protecting privacy of information stored on computers or exchanged on computing networks is whether data is or is not PII. This is information that can locate or identify a person, or can be used in conjunction with other information to uniquely identify an individual. Historically, PII would include name, Social Security Number, address, phone number, or date of birth. In the Internet Age, the list of PII has grown to include e-mail addresses, IP addresses, social networking pages, search engine requests, log records and passwords.

If privacy is not a core component of Smart Grid and related applications that collect, retain, use, or share PII, then broad adoption of the technology will be at

risk. Smart Grid planning and implementation must take an end-to-end approach to securing PII that enforces privacy rights of energy users.

California has taken steps to establish privacy protections for its residents in a number of areas, but has added the critical component of accountability and oversight.[5] The drafters of the California Constitution state that, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[6]

There is also a well-established federal interest in the right of privacy. The U.S. Supreme Court notes, the constitutional right of privacy protects two distinct interests: "one is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[7] Moreover, public opinion polls consistently find strong support among Americans for privacy rights in law to protect their personal information from government and commercial entities.[8]

More recently, the Supreme Court in *Kyllo v. United States*[9] addressed the privacy implications of the monitoring of electricity use in the home. After reviewing precedent, the Court found that a search warrant must be obtained before the government may use new technology to monitor the use of devices that generate heat in the home:

---

[5] California Office of Privacy Protection, Privacy Laws, http://www.privacy.ca.gov/privacy_laws.htm
[6] California State Constitution, Article1, Section 1, http://www.leginfo.ca.gov/.const/.article_1.
[7] *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977) and *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977).
[8] *See generally* EPIC, Public Opinion on Privacy, http://epic.org/privacy/survey (last visited Dec. 1, 2009).
[9] 533 U.S. 27 (2001).

> [I]n the case of the search of the interior of homes–the prototypical and hence most commonly litigated area of protected privacy–there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.[10]

The Court found that even the minutest details of a home are intimate:

> "[i]n the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes."[11] Thus, the Court held that the police could not use thermal imaging equipment, which was not in general public use, "to explore details of the home that would previously have been unknowable without physical intrusion," without first obtaining a search warrant.[12]

The well-established interest in privacy of power consumption in the home begins the discussion. There are documented instances in this decade where California residents have come under suspicion because of their electricity usage. For example, in 2004 a Carlsbad California family faced police investigation due to higher electricity consumption than their neighbors.[13]

Smart Grid PII data collection should begin with "fair information practices" or FIPs, which set out the essential framework for the collection and use of personal information. FIPs creates the foundation for service provision and is critical to state and federal privacy law. This approach to privacy protection, which places obligations on those entities that collect personal information and provides rights to individuals whose personal data is collected, undergirds most of modern privacy

[10] *Id.* at 34.
[11] *Id.* at 37.
[12] *Id.* at 40.
[13] Privacy.org, "A Suspicious Electric Utility Bill?," March 29, 2004.

law. In fact, it provides the framework for the Privacy Act of 1974[14] and dozens of state and federal laws.[15]

In the area of Smart Grid, the issues will not just arise when utilities are directly involved in the collection, retention, and use of PII, but will extend to whom they share data with and for what purposes. Utilities have used contractors or third-party service providers to manage discrete components of electricity delivery, billing, or service provision. The question before the CPUC ultimately is the legitimacy of using consumer consumption data for marketers to target sales for home improvements or new appliances. Because business models for Smart Grid involve entities that have not engaged electric service relationships with consumers they should be held to a higher standard for data use restrictions and security of consumer data.

TRANSPARENCY

Energy consumers have expectations for privacy regarding their energy usage data that may run counter to data sharing and reuse by non-utility service providers. Some would argue that if consumers sign agreements allowing third parties to get access to their electric utility data that is sufficient. EPIC would strongly recommend that the CPUC not rely on the failed notice and consent models that have proven to be an unreliable means of assuring customer privacy rights.

ABANDON NOTICE AND CONSENT MODELS

[14] Privacy Act of 1974 , 5 U.S.C. § 552a (2008).
[15] *See, e.g.*, Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681u (2008); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-22 (2008); Fair Information Practices Act, Mass Ann. Laws ch. 66A §§ 1-3 (2008); Insurance Information and Privacy Protection Act, Me. Rev. Stat. Ann. tit. 24-A, §§ 2201-20 (2008).

> A clearly-specified notice should exist to describe the purpose for the collection, use, retention, and sharing of PII. Data subjects should be told this information at or before the time of collection. . . . The organization should describe the choices available to individuals and obtain explicit consent if possible, or implied consent when this is not feasible, with respect to the collection, use, and disclosure of their PII.[16]

As a threshold matter, the purposes for which PII can be collected, used, retained, or shared should be outlined by the CPUC. This would accomplish what no ordinary consumer could do for themselves—create the context within which customer data could be collected, retained, used, and shared by non-utility service providers. The purposes for which PII can be collected, used, retained, or shared should be severely restricted. It is insufficient to simply require authorities or organizations to have a nebulous "purpose," as anything from "improved marketing" to "government surveillance" could qualify. CPUC is in the unique position to actualize the privacy rights that utility consumers must continue to have as electric utility modernization moves forward.

The "notice and consent" model is fundamentally flawed and should not be relied upon to excuse or justify any Smart Grid PII activity. As David Vladeck, Director of the Bureau of Consumer Protection at the Federal Trade Commission, recently acknowledged, the model simply does not function as intended:

> [The notice and consent model] may have made sense in the past where it was clear to consumers what they were consenting to, that consent was timely, and where there would be a single use or a clear use of the data. That's not the case today. Disclosures are now as long as treatises, they are written by lawyers - - trained in detail and precision, not clarity - - so they even sound like treatises, and like some treatises, they are difficult to

[16] Cyber Security Strategy, *supra* note at 9.

comprehend, if they are read at all. It is not clear that consent today actually reflects a conscious choice by consumers.

In EPIC's testimony before the United States Senate Committee on Commerce, Science and Transportation, Marc Rotenberg argued that "[s]olutions which rely on simple notice and consent will not adequately protect users." In an analogous context – notice and consent in online agreements - the failures of the model become more obvious. A recent survey of California consumers showed that they fundamentally misunderstand their online privacy rights. In two separate surveys, almost 60% of consumers incorrectly believed that the presence of "privacy policy" meant that their privacy was protected. In a different survey, 55% of participants incorrectly believed that the presence of a privacy policy meant that websites could not sell their address and purchase information.

Another serious challenge to notice and consent is the actions of users routinely click through notices. The Pew Internet and American Life Project found that 73% of users do not always read agreements, privacy statements or other disclaimers before downloading or installing programs. In such an environment, merely giving notice to users before collecting their sensitive information fails to adequately protect privacy in the way consumers expect.

Especially because of the pervasiveness of the proposed nationwide Smart Grid, choice and consent of individuals is severely restricted. In all likelihood, individuals who wish to receive electricity will have little or no choice but to comply with policies that require the disclosure of PII. It is highly likely that situations may arise that the CPUC has not contemplated, such as data collection by a California

utility and information shared with an entity that may not be located within or licensed to do business in the state of California. For authorities or organizations to obtain the consent of individuals would be nearly meaningless, as the power dynamic is fatally skewed. Information should be kept securely, and users should have the ability to know what data about them is being kept, who has it been shared with, and to withdraw consent for the holding of this data. Further, data should only be collected and kept for specified purposes. The data agreements that customers are asked to sign or approve cannot be overly broad in the "fine print," while the representation is that it is to "help customers manage energy usage." Authorities and organizations must limit the collection, use, retention and sharing of PII in the first instance, rather than relying on hollow consents to justify more data collecting activity.

There are lessons to be gathered from the international community regarding privacy protection for digital PII. The International Organization of Economic Cooperation and Development (OECD) codified its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[17] The OECD Privacy Guidelines offer important international consensus on and guidelines for privacy protection and establish eight principles for data protection that are widely used as the benchmark for assessing privacy policies and legislation:

1. Collection Limitation Principle – There should be limits to the collection of personal data; any such data collected should be

[17] *See* OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html [hereinafter OECD Privacy Guidelines], *reprinted in* The Privacy Law Sourcebook 395-423 (Marc Rotenberg ed., 2004).

obtained by lawful means and with the consent of the data subject, where appropriate.

2. Data Quality Principle – Collected data should be relevant to a specific purpose, and be accurate, complete, and up-to-date.

3. Purpose Specification Principle – The purpose for collecting data should be settled at the outset.

4. Use Limitation Principle - The use of personal data ought to be limited to specified purposes, and that data acquired for one purpose ought not be used for others.

5. Security Safeguards Principle – Data must be collected and stored in a way reasonably calculated to prevent its loss, theft, or modification.

6. Openness Principle – There should be a general position of transparency with respect to the practices of handling data.

7. Individual Participation Principle – Individuals should have the right to access, confirm, and demand correction of their personal data.

8. Accountability Principle - Those in charge of handling data should be responsible for complying with the principles of the privacy guidelines.[18]

The OECD Privacy Guidelines reflect a broad consensus about how to safeguard the control and use of personal information. Therefore, they provide a well thought-out solution to challenging questions about international consensus on privacy and data protection that directly implicate Smart Grid policies and practices.

[18] *Id.* at 398-99.

Smart Grid Fair Information Practices Principle
Smart Grid service providers should limit collection of consumers' personal data; any such data collected should be obtained by lawful means and with the consent of the consumer, where appropriate.[19]
Data collected by Smart Grid service providers should be relevant to a specific purpose, and be accurate, complete, and up-to-date.
The purpose for collecting Smart Grid data should be settled at the outset.
The use of Smart Grid personal data ought to be limited to specified purposes, and data acquired for one purpose ought not be used for others.
Smart Grid data must be collected and stored in a way reasonably calculated to prevent its loss, theft, or modification.
There should be a general position of transparency with respect to the practices of handling Smart Grid data.
Smart Grid consumers should have the right to access, confirm, and demand correction of their personal data.
Those in charge of handling Smart Grid data should be responsible for complying with the principles of the privacy guidelines.

ASSESSING SMART GRIDS AND PRIVACY

The Smart Grid implicates privacy at a fundamental level because it will be a powerful digital communication network. Cisco, a communication giant, foresees the Smart Grid network being "100 or 1,000 times larger than the Internet."[20] The Smart Grid would allow the unprecedented flow of information between power providers and power consumers, and its potential benefits to energy efficiency, granular control over power usage, and the environment are immense. However, like any analogous communications network, such as the Internet, the Smart Grid also

[19] "Consent" is widely understood as "any freely given specific and informed indication of a data subject's wishes by which the data subject signifies his agreement to personal data relating to him being processed." European Union Data Protection Directive, *reprinted in* The Privacy Law Sourcebook 450 (Marc Rotenberg ed., 2004).

[20] Martin LaMonica, *Cisco: Smart Grid Will Eclipse Size of Internet*, CNET, May 18, 2009, http://news.cnet.com/8301-11128_3-10241102-54.html.

admits the possibility of new and problematic threats to privacy in the form of increased data collection, retention, sharing and use.[21]

The basic architecture of the Smart Grid may present several thorny privacy issues. The first widely distributed Smart Grid application is the smart meter.[22] Smart meters monitor and report on customer electricity consumption to the utility service provider. Experts estimate that U.S. investment in smart meters could total $40 to $50 billion, and roughly 100 million smart meters could be installed over the next five years.[23] Smart meters, like traditional meters, will be associated with a unique address, which makes it PII.[24] The meter serial number, as well as the electronic information associated with the device would comprise PII for those associated with the address. Smart meters will increase the frequency of communication from the home to the utility service provider or the third-party application user. Traditional meter reading took place once a month, by the visit of a person who was affiliated with the electricity service provider or billing company, whereas smart meters will increase the frequency and access to the data collected.

---

[21] *See* Ann Cavoukian, Jules Polonetsky & Christopher Wolf, Privacy by Design, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation* 8 (Nov. 2009), http://www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf ("Modernization of the current electrical grid will involve end-user components and activities that will tend to increase the collection, use and disclosure of personal information by utility providers, as well as, perhaps, third parties.") [hereinafter *Privacy by Design*].

[22] *See* Stan Mark Kaplan, Congressional Research Service, *Electric Power Transmission: Background and Policy Issues* 23 (2009), *available at* http://opencrs.com/document/R40511/2009-04-14/download/1013 (discussing basic functions of smart meters); U.S. Dep't of Energy, *Smart Grid System Report* 38 (July 2009) [hereinafter "*Smart Grid System Report*] ("The use of smart meters, a driving force behind being able to evaluate grid load and support pricing conditions, has been increasing significantly, almost tripling between 2006 and 2008 to 19 million meters. . . .").

[23] National Institute for Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft) 84 (2009) [hereinafter Draft Framework], http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf.

[24] *See* Cyber Security Strategy, *supra* note at 33 (flow chart detailing Smart Grid communication links between consumers and providers).

Proposals for smart meters discuss "real-time" reporting of usage data.[25] The design specification is not for electricity consumption information to remain in the home or meter location, which could only be accessed easily by the utility user. Rather, the plan as suggested in the Cyber Security Strategy is to share the information with the utility company, who would then share it with others. If the reported goal of Smart Meters is to allow customers to make better energy consumption decisions, then only the customer should have access to that information. This is one of many instances in which the design of a Smart Grid application can favor privacy or ignore it.

Another proposed architectural point that raises privacy implications is the use of wireless communications to transmit Smart Grid data.[26] Any wireless technology used to transmit user PII must protect personal privacy. Wireless sensors and networks are susceptible to security breaches unless properly secured,[27] and breaches of wireless technology could expose users' personal data.[28] Similarly, the potential transmission of Smart Grid data through "broadband over power line" (BPL) implicates users' privacy:

> A BPL node could communicate with any device plugged into an electrical socket. Capture of a substation node would provide control over messages going to smart appliances or computing systems in

---

[25] *See, e.g.*, Draft Framework, *supra* note 23.
[26] *See* Draft Framework, *supra* note, at 23.
[27] *See, e.g.*, Mark F. Foley, Data Privacy and Security Issues for Advanced Metering Systems (Part 2), *available at* http://www.smartgridnews.com/artman/publish/industry/Data_Privacy_and_Security_Issues_for_Advanced_Metering_Systems_Part_2.html ("Wireless sensor networks, for example, are subject to the general security problems of computer networks, ordinary wireless networks, and ad-hoc networks).
[28] *See id.* (breaches could "result in denial of service to customers or utilities (e.g., access to billing information or energy usage), payment avoidance, system overload, reduced quality of service, and violation of power control protocols").

> homes and offices. A utility may also offer customers BPL as a separate revenue stream. This creates risks that [advanced meter] data could be read or modified over the internet or that common internet attacks could be brought against the electrical grid or individual customers.[29]

Moreover, wireless communication is especially problematic in light of the past exploitation of wireless systems by thieves who use techniques known as "war driving" to seek out unprotected or insufficiently protected wireless communication portals.[30] Signals from wireless devices are detectable by others using easily acquired materials with little expertise to pick-up valuable information on systems using wireless technology.

Wireless would not only provide a significant challenge to privacy of users, but may also pose economic as well as security threats. Identity theft, third-party monitoring of utility use, home invasions, domestic abuse and predatory use of home electricity consumption information strips home owners of the protection from prying eyes provided by the walls of their home.

A final architectural problem with the proposed Smart Grid is the interaction between the Smart Grid and with plug-in electric vehicles (PEV). It is possible that the Smart Grid would permit utility companies to use PEVs and other sources of stored energy "as a grid-integrated operational asset,"[31] *i.e.,* drain the energy stored in the PEVs when needed to supply other users. This application of the Smart Grid is particularly troubling. If privacy is, as the Supreme Court has said, the "interest in

---

[29] *Id.*
[30] *See, e.g.*, Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 Va. J.L. & Tech. 7 (2004).
[31] Draft Framework, *supra* note at 23.

independence in making certain kinds of important decisions,"[32] then this proposed application could severely damages both privacy interests and consumer rights.

PRIVACY THREATS

In addition to the architectural weaknesses of the proposed Smart Grid, the application and use of the Grid threatens privacy in many different ways. Robust protection of privacy rights comes with building the system to assure protection of personal information coupled with regulatory protections that establish accountability and oversight. The following paragraphs identify many of the privacy interests threatened by the Smart Grid.

IDENTITY THEFT

Identity theft victimizes millions of people each year.[33] The FTC estimated that 8.3 million people discovered that they were victims of identity theft in 2005, with total reported losses exceeding $15 billion.[34] According to the Privacy Rights Clearinghouse, more than 340 million records containing sensitive personal information have been involved in security breaches since January 2005.[35]

Peter Neumann, an expert on privacy and security (and a member of the EPIC Advisory Board), testified to Congress in 2007 about security and privacy, and concluded that the design of information systems are subject to many pitfalls, and

---

[32] *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977).
[33] *See generally* EPIC, Identity Theft, http://epic.org/privacy/idtheft (last visited Dec. 1, 2009).
[34] Fed. Trade Comm'n, *2006 Identity Theft Survey Report* 4, 9 (2007) [hereinafter "*FTC Survey Report*"].
[35] Privacy Rights Clearinghouse, *Chronology of Data Breaches*, Nov. 23, 2009, http://www.privacyrights.org/ar/ChronDataBreaches.htm.

that there is "[a] common tendency to place excessive faith in the infallibility of identification, authentication, and access controls to ensure security and privacy."[36]

The faith placed in the capacity of the Smart Grid to safeguard sensitive personal information is similarly unfounded. As an employee for Itron, a manufacturer of automated meters, admitted, "Any network can be hacked."[37] Similarly, some experts argue that "an attacker with $500 of equipment and materials and a background in electronics and software engineering could 'take command and control of the [advanced meter infrastructure] allowing for the en masse manipulation of service to homes and businesses.'"[38] Thus, it is possible that "just as identities, credit and debit card numbers, and other financial information are routinely harvested and put up for sale on the Internet, so will be Smart Grid identifiers and related information."[39] Alternatively, identity thieves could use PII obtained elsewhere to impersonate utility customers, which poses the risk of fraudulent utility use and potential impact on credit reports.[40] Further, the exploits of identity thieves should be explored by a "white hat hacker" review of the security vulnerability of Smart Meter devices.

PERSONAL SURVEILLANCE

---

[36] *Security and Privacy in the Employment Eligibility Verification System (EEVS) and Related Systems: Hearing Before the H. Comm. On Ways and Means Subcomm. On Social Security*, 110th Cong. 9 (2007) (statement of Peter G. Neumann, Principal Scientist, Computer Science Lab, SRI International).
[37] Jeanne Meserve, *'Smart Grid' May Be Vulnerable To Hackers*, CNN, March 21, 2009, http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability.
[38] *Id.*
[39] Eric Breisach & H. Russell Frisby, *Energy Identity Theft: We're Way Beyond Plugging in the Meter Upside Down*, Smartgridnews.com, April 9, 2008, http://www.smartgridnews.com/artman/publish/article_425.html.
[40] *See* Rebecca Herold, *SmartGrid Privacy Concerns*, *available at* http://www.privacyguidance.com/files/SmartGridPrivacyConcernsTableHeroldSept_2009.pdf [hereinafter *Privacy Concerns*].

The Smart Grid could also reveal sensitive personal behavior patterns. The proposed Smart Grid will be able to coordinate power supply in real time, based on the power needs of users and the availability of power.[41] For instance,"[e]nergy use in buildings can be reduced if building-system operations are coordinated with the schedules of the occupants."[42] However, coordinating schedules in this manner poses serious privacy risks to consumers. Information about a power consumer's schedule can reveal intimate, personal details about their lives, such as their medical needs, interactions with others and personal habits: "highly detailed information about activities carried on *within the four walls of the home* will soon be readily available for millions of households nationwide."[43] "For example, research has delineated the differences in availability at home for various social types of electricity consumers including working adults, senior citizens, house wives and children of school age." [44] Similarly, the data could reveal the type of activity that the consumer is engaging in, differentiating between, for example, housework and personal hygiene, or even revealing that a consumer has a serious medical condition and uses medical equipment every night, or that he lives alone and leaves the house vacant all day.[45]

---

[41] Draft Framework, *supra* note at 23.
[42] *Id.* at 23.
[43] Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 28 (2009), *available at* http://ssrn.com/abstract=1370731 (emphasis in original) [hereinafter *Privacy and the New Energy Infrastructure*]; *see Privacy Concerns*, *supra* note 40.
[44] *Privacy and the New Energy Infrastructure* at 26-27; *see* A. Capasso et al., *Probabilistic Processing of Survey Collected Data in a Residential Load Area for Hourly Demand Profile Estimation*, 2 Athens Power Tech 866, 868 (1993).
[45] *Privacy and the New Energy Infrastructure*, supra note 43, at 27 ("differences in consumption vary with the type of activity, and profiles of energy uses that differentiate between activities can be constructed for things like leisure time, housework, cooking, personal hygiene"); *see* Capasso, *supra* note 44, at 869.

ENERGY USE SURVEILLANCE

Smart Grid meter data may also be able to track the use of specific appliances within users' homes.[46] These "smart appliances" would be able to communicate with the Smart Grid, transmitting detailed energy-use information and responding dynamically to price fluctuations and power availability. A smart water heater, for example, could engage in "dynamic pricing" by equipping it with "a device that coordinates with a facility's energy-management system to adjust temperature controls, within specified limits, based on energy prices."[47] As other devices become commercially available that are designed to send consumption data over the Smart Grid, the collection of personal data could increase. For example, the monitoring of electricity consumption may require the registration of items within a home for monitoring by the utility company or a third-party service provider. Smart Grid enabled appliances such as washers, dryers, air conditioners, central heating systems, water heaters, stoves, refrigerator, freezers, swimming pools and Jacuzzis consume large amounts of electricity, and may be associated with a fixed address such as a home. Each of these items may have a unique product manufacturer designation (e.g. Whirlpool, General Electric, etc.), and product serial number, and the purchase history of the item would include the purchaser's name. Monitoring the function and operation of these items would be physically associated with an address, which constitutes PII for those occupying the residence.

---

[46] *See, e.g.*, *Privacy by Design*, *supra* note 21, at 8-9.
[47] *Smart Grid System Report*, *supra* note 22, at 34.

Further, it can be anticipated that the Smart Grid could track even smaller electricity usage. Smart plugs or outlets might report in real-time when a lighting fixture, lamp, computer, television, gaming system, music device, or exercise machine is operating and for how long.

One scholar forcefully argues that the ability to monitor electricity use at such a granular level poses a serious threat to privacy:

> This, more than any other part of the smart meter story, parallels Shelley's fable of Frankenstein: while researchers do not currently have the ability to identify every appliance event from within an individual's electricity profile, the direction of the research as a whole and the surrounding context and motivations for such research point directly to developing more and more sophisticated tools for resolving the picture of home life that can be gleaned from an individual's electricity profile. Before the switch is thrown and the information unleashed upon the world for whatever uses willed, it may be prudent to look into data protections lest the unforeseen consequences come back to haunt us.[48]

Indeed, the potential amount of personal information that could be gleaned from smart appliances is colossal:

> For example, it is suggested that the following information could be gleaned with the introduction of end-user components . . . : Whether individuals tend to cook microwavable meals or meals on the stove; whether they have breakfast; the time at which individuals are at home; whether a house has an alarm system and how often it is activated; when occupants usually shower; when the TV and/or computer is on; whether appliances are in good condition; the number of gadgets in the home; if the home has a washer and dryer and how often they are used; whether lights and appliances are used at odd hours, such as in the middle of the night; whether and how often exercise equipment such as a treadmill is used.[49]

---

[48] *Privacy and the New Energy Infrastructure*, *supra* note 43, at 28.
[49] *Privacy by Design*, *supra* note 21, at 11.

Perhaps more problematic, much of the personal information that could be gleaned from smart appliances would not otherwise be available to outsider observers: "With the whole of a person's home activities laid to bare, [appliance-usage tracking] provides a better look into home activities than would peering through the blinds at that house."[50]

Not only could that information be used to extract even more intimate information from the usage data, but that information could also be used in ways that impact the user in tangential areas of their lives.[51] For instance, appliance usage data could be transferred to appliance manufacturers to respond to warranty claims. Or, the data could be transferred to insurance companies that may want the information as part of an investigation into an insurance claim. [52] Landlords could track the energy use and behavior patterns of renters/leasers. The data could even be used to impinge on civil liberties by facilitating censorship or limitation of activities based on energy consumption patterns.[53] For instance, "meter data could reveal resident activities or uses that utility companies may then subsequently decide are inappropriate or should not be allowed."[54] Or more generally, energy service providers in possession of consumer data may simply choose to use the data for marketing purposes or to sell it on the open market.

---

[50] *Id.* at 25.
[51] *See Privacy Concerns*, *supra* note 40; Mark F. Foley, *The Dangers of Meter Data (Part 1)*, *available at* http://www.smartgridnews.com/artman/publish/industry/The_Dangers_of_Meter_Data_Part_1.html [hereinafter "*Dangers (Part I)*"].
[52] *See Dangers (Part I)*, *supra* note 51.
[53] *See Privacy Concerns*, *supra* note 40.
[54] *Id.*

The possibility that the appliances could interface with the Smart Grid through IP-based networks further exacerbates the privacy issues. The Draft Framework raises indirectly the privacy risk that would arise in an IP-based power network: "An analysis needs to be performed for each set of Smart Grid requirements to determine whether IP is appropriate and whether cyber security can be assured."[55] The effect of IP-based networks on privacy must be part of that analysis, as IPv6 and the "Internet of Things" raise new privacy considerations. For instance, the IP addresses associated with appliances or other devices "could be used to track activities of a device (and an associated individual)," thereby revealing an individual's health condition, daily activities, and other sensitive and private information.[56] Moreover, allowing the devices access to the Internet will make them more vulnerable, increasing the likelihood of security breaches and loss of personal privacy: "All of these [Smart Grid] communication links introduce vulnerabilities, especially if they can be accessed over the Internet."[57] The invasiveness of extracting appliance usage data from Smart Grid data, particularly from IP-enabled appliances, cannot be overstated as IP addressing in an IPv6 environment will make possible the unique identification of every single device in the home that receives electric power.

---

[55] See, e.g., Draft Framework, supra note 23.

[56] SANS Institute, The Next Internet Privacy in Internet Protocol 5 (2004); *see* Commission To the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Internet of Things — An Action Plan for Europe 5-6 (2009) ("Social acceptance of [Internet of Things] will be strongly intertwined with respect for privacy and the protection of personal data, two fundamental rights of the EU.").

[57] *See* M. Granger Morgan, et. al., Carnegie Mellon University Department of Engineering and Public Policy, The Many Meanings of "Smart Grid" 5 (2009), *available at* http://www.epp.cmu.edu/Publications/Policy_Brief_Smart_Grid_July_09.pdf.

PHYSICAL DANGERS

Data could be used by criminals, such as burglars or vandals, who could monitor real-time data in order to determine when the house is vacant.[58] As one Carnegie Mellon University researcher argued, "[w]e should not build a power system in which a hacker working for a burglar can tell when you are home by monitoring your control systems. . . ."[59]

Similarly, the Smart Grid affects the interaction between privacy and domestic violence/stalkers.[60] Stalking, domestic violence and intimate partner abuse are also the targets of evolving state and federal policy.[61] Over the years this policy has increasingly included the protection of the privacy of stalking and domestic violence survivors.[62] As EPIC has repeatedly argued, domestic violence victims often have urgent needs for privacy, as they may need to keep data from their abusers. This abuse can also involve privacy violations such as surveillance, monitoring, or other stalking. For a domestic violence victim, the need for privacy is a need for physical safety. However, the Smart Grid could provide abusers with another method for tracking and monitoring their victims. For instance, an abuser could track his victim's daily activities in order to exercise greater control over her ability to contact the authorities or other aid. Similarly, the capabilities of the Smart Grid could affect even emancipated domestic abuse victims, as their former abusers

[58] *See Privacy and the New Energy Infrastructure*, *supra* note 43, at 30; *Privacy Concerns*, *supra* note 40; *Dangers (Part I)*, *supra* note 51.
[59] Morgan, et. al, *supra* note 57, at 5.
[60] *See generally* EPIC, Domestic Violence and Privacy, http://epic.org/privacy/dv (last visited Dec. 1, 2009).
[61] *See, e.g.*, Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960 (2005).
[62] *See* EPIC, Violence Against Women Act and Privacy, http://epic.org/privacy/dv/vawa.html (last visited Dec. 1, 2009).

may be able to relocate the victims using personal information transmitted through the Smart Grid or shared with third-party service providers.

MISUSE OF DATA

The massive amounts of data produced by the Smart Grid can potentially be misused by a number of parties intentionally or unintentionally—power utilities, authorized third parties such as marketing firms, Smart Grid service providers or employees, or unauthorized third parties such as thieves.

Power utilities themselves will likely be interested in conducting complex data mining analysis of Smart Grid data in order to make power distribution decisions. This activity falls within the scope of Smart Grid implementation, what may prove to be difficult for utilities is managing internal use of the resources and knowledge produced by detailed energy consumption analysis for approved purposes. For instance, at the Tennessee Valley Authority (TVA), administrators estimate that they will have 40 terabytes of data by the end of 2010, and that 5 years of data will amount to roughly half a petabyte.[63] The TVA administrators are actively working to improve their ability to analyze the data, including through "complex data mining techniques."[64] Data mining of sensitive personal information raises serious privacy concerns.[65]

Authorized third-parties may also be interested in using data collected

---

[63] Josh Patterson, Cloudera, *The Smart Grid and Big Data: Hadoop at the Tennessee Valley Authority (TVA)*, June 2, 2009, http://www.cloudera.com/blog/2009/06/02/smart-grid-big-data-hadoop-tennessee-valley-authority-tva.

[64] *Id.*

[65] *See* EPIC, Terrorism (Total) Information Awareness, http://epic.org/privacy/profiling/tia (discussing government data mining of citizens' personal information) (last visited Dec. 1, 2009).

through the Smart Grid. The real-time data streaming capabilities of the Smart Grid, in particular, implicate a separate group of privacy risks. Just as appliance manufacturers and insurance companies may want access to appliance usage data, marketing and advertising firms may want access to the data—particularly real-time data—in order to target marketing more precisely.[66] However, power usage data, as discussed, can reveal intimate behavioral information; providing that information to third-party marketing and advertising firms surreptitiously would be a repugnant invasion of privacy.

The misuse of Smart Grid data is further exacerbated by the possibility of combining Smart Grid data with other data sources. For example, Google PowerMeter collects data on home energy consumption.[67] This technology raises the obvious possibility that Google will combine consumer information about power consumption with Google's preexisting ability to record, analyze, track and profile the activities of Internet users.[68] Such new business models also raise significant antitrust concerns.[69] For example, knowing that a consumer's hot water heater has failed, and that the consumer is also searching for "hot water heater" using Google's search application, which serves ads to consumers as part of this service can put consumers at a disadvantage.

---

[66] *See Privacy and the New Energy Infrastructure*, *supra* note 43, at 43; *Privacy Concerns*, *supra* note 40; *Dangers (Part I)*, *supra* note 51.
[67] Google PowerMeter, http://www.google.org/powermeter (last visited Dec. 1, 2009).
[68] *See generally* EPIC, Privacy? Proposed Google/DoubleClick Merger, http://epic.org/privacy/ftc/google (last visited Dec. 1, 2009).
[69] *Cf.* Statement of Interest of the United States of America Regarding Proposed Class Settlement, *The Author's Guild, Inc., et al. v. Google, Inc.*, No. 05 Civ. 8136 (DC), at 16-26 (S.D.N.Y. Sep. 28, 2009) (Department of Justice arguing that the proposed settlement regarding Google Books "may be inconsistent with antitrust law"). *See generally* EPIC, Google Books Settlement and Privacy, http://epic.org/privacy/googlebooks (last visited Dec. 1, 2009).

Unauthorized third-parties will likely also be interested in misusing Smart Grid data, for many of reasons already discussed, such as identity theft or burglary. Indeed, those risks remain if even residual data is stored on Smart Grid meters. If data on Smart Grid meters are not properly removed, residual data could reveal information regarding the activities of the previous users of the meter. [70] Thus, the Smart Grid technology and regulatory objectives should be to avoid the unnecessary retention of PII. Moreover, the prospect of remote access to Smart Grid data could lead to unauthorized access and misuse of the data. Many companies and government agencies provide employees and contractors with remote access to their networks through organization-issued computing devices. Remote access to Smart Grid customer information or utility usage data should be prohibited except for service provision and maintenance. The misuse of Smart Grid data could also harm consumers' reputations in many different ways. The collection and sharing of Smart Grid data could cause unwanted publicity and/or embarrassment. Moreover, public aggregated searches of Smart Grid data could reveal individual behaviors. Finally, the aforementioned data aggregation and data mining activity could permit publicized privacy invasions.

SMART GRID AND OTHER PRIVACY CHALLENGES

The privacy risks associated with the use and retention of "anonymized data" are significant because such data may not be truly anonymous. Quasi-identifiers can be used for re-identification because they can be linked to external databases that contain identifying variables. This method, record linkage, occurs when two or more

[70] *See Privacy Concerns*, *supra* note 40.

databases are joined. Such information can be obtained through public records, such as birth and death certificates.[71] Using record linkage, de-identified data can also be easily re-identified. For example, by utilizing date of birth, gender and zip code information for members of the public, a researcher was able to uniquely identify 87% of the US population.[72]

In a study published in July 2009, two researchers at Carnegie Mellon University found that an individual's entire SSN often could be predicted from publicly available birth information.[73] Moreover, the first five digits of an individual's SSN could be predicted with an even greater degree of accuracy. The accuracy of the researchers' predictions was even greater when predicting the numbers of individuals born in sparsely-populated states like Montana, and the researchers anticipate that their predictions will become increasingly accurate over time. This research demonstrates the ineffectiveness of attempting to protect privacy by "anonymyzing" or "de-identifying" data.

Techniques for anonymizing data should be pursued, but it is vitally important to ensure that such methods are robust, provable and transparent, Any technique proposed to anonymize data should be made public and available to researchers to examine and evaluate. Under no circumstance should a company be able to represent, without independent verification, that it had anonymized data.

---

[71] *See* Salvador Ochoa et al., *Re-identification of Individuals in Chicago's Homicide Database: A Technical and Legal Study*, Massachusetts Institute of Technology (2001) (utilizing the Social Security Death Index and de-identified information about Chicago homicide victims, the researchers were able to re-identify 35% of the victims).

[72] Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J. Law, Med., & Ethics 98, 98–99 (1997).

[73] *See* Alessandro Acquisiti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 Proceedings of the National Academy of Sciences 10975.

Until such techniques are established and safeguards are put in place, the primary objective should be to minimize the collection of PII in the first instance.

ESTABLISH ROBUST CRYPTOGRAPHIC STANDARDS

Strong cryptography should be applied to secure all electronic communications from a Smart Grid application or device. Threats to address include: injection of false information; deletion of information, denial of service attacks, billing identity theft, service identity theft, malicious software, cyber attacks, pranks and various types of surveillance.[74]

"**The Billion-Dollar Bug** Smart meters are extremely attractive targets for malicious hackers, largely because vulnerabilities can easily be monetized. Hackers who compromise a meter can immediately manipulate their energy costs or fabricate generated energy meter readings."[75] For this reason, there should be an open call for designs that seek to maximize both data security and privacy of the home as well as of enterprises. It is well known in the cryptographic community, for instance, that so-called "blind signatures" can allow ultra-secure reporting of energy usage statistics without revealing the precise appliance and timings involved.[76]

Sound cryptographic techniques do not rely upon hiding the cryptographic process, often referred to as an algorithm, from public review. Sound cryptographic processes are made so by the rigors imposed by public disclosure and testing of

---

[74] Patrick McDaniel & Stephen McLaughlin, Security and Privacy Challenges in the Smart Grid, IEEE Security and Privacy, May/June 2009, 75-77.
[75] *id*
[76] David Chaum, *Achieving Electronic Privacy*, Scientific America, Aug. 1992, at 96-101, *available at* http://chaum.com/articles/Achieving_Electronic_Privacy.htm.

algorithms, and perhaps even more significantly, by the environment in which the cryptography is implemented.[77] Placing the strongest cryptography in an operating system or application that can easily be subverted by insiders, or compromised externally by penetration and malware can render the cryptography ineffective.[78] For this reason, it is imperative that all cryptographic algorithms used to secure Smart Grid technology and electronic technology used to facilitate Smart Grid optimization and operations be open for public inspection and testing and that the findings be made public, including the entire systems in which the cryptography is used. Further, encryption and decryption keys that are used to secure information stored or transmitted on the Smart Grid should be of sufficient complexity that they cannot be easily deduced or broken.

Privacy protection is essential to the successful implementation of the Smart Grid, and failure to develop a robust policy framework to safeguard consumer privacy could have dire consequences. EPIC urges CPUC to consider these recommendations in deciding regulatory framework of service providers for the Smart Grid. EPIC is willing and able to contribute to the further development of Smart Grid policy that would help encourage robust privacy protection while allowing the Smart Grid to accomplish important policy objectives.

EPIC appreciates this opportunity to contribute the deliberations of the California Public Utility Commission on the subject of Smart Grid implementation. The objectives of Smart Grid are lofty and offer the state of California and the nation

---

[77] Bruce Schneier, *Applied Cryptography* 21-46 (2d ed. 1996).
[78] Peter Neumann, *Computer Related Risks* 132-180 (1995).

the unique opportunity to introduce a major technological advancement that include the necessary privacy protections to assure consumer privacy rights from the onset. Often innovation, new business practices, or public policy that excludes the important protection of personal information creates resistance to change. The CPUC is leading the way on promoting the dialogue on regulatory policy, and we encourage you to adopt the nation's first smart grid privacy consumer policy.

Sincerely,

/s/

Lillie Coney, Associate Director
EPIC