COMMENTS OF THE
ELECTRONIC PRIVACY INFORMATION CENTER
Joined by

PRIVACYACTIVISM
PRIVACY RIGHTS CLEARINGHOUSE
LIBERTY COALITION
ELECTRONIC FRONTIER FOUNDATION
GOVERNMENT ACCOUNTABILITY PROJECT
U.S. BILL OF RIGHTS FOUNDATION
CENTER FOR MEDIA AND DEMOCRACY
CYBER SECURITY PROJECT
THE RUTHERFORD INSTITUTE
WORLD PRIVACY FORUM
CENTER FOR FINANCIAL PRIVACY AND HUMAN RIGHTS
AMERICAN CIVIL LIBERTIES UNION
CONSUMER ACTION
AMERICAN LIBRARY ASSOCIATION

Privacy and Security Experts

Bruce Schneier
Christopher Wolf
Pablo Molina
Prof. Helen Nissenbaum
Deborah Hurley
Philip Friedman
Edward G. Viltz
Chris Larsen
Stefan Brands

to
THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
on
DOCKET NO. 0909301329-91332-01

"Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements; Request for Comments"

December 1, 2009

TABLE OF CONTENTS

I. BACKGROUND AND SIGNATORIES

By notice published in the Federal Register on October 9, 2009, the National Institute of Standards and Technology (NIST) announced[1] it seeks public comment on the Smart Grid Cyber Security Strategy and Requirements document.[2]

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.[3] EPIC has a specialized area of expertise regarding digital communication technologies and privacy policy.[4] 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.[5] 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. http://epic.org/

Privacy Activism is a nonprofit organization whose goal is to enable people to make well-informed decisions about the importance of privacy on both a personal and societal level. A key goal of ours is to inform the public about the importance of privacy rights and

[1] Smart Grid Cyber Security Strategy and Requirements, 74 Fed. Reg. 52,183-84 (October 9, 2009).
[2] National Institute for Standards and Technology, Smart Grid Cyber Security Strategy and Requirements 5 (2009) [hereinafter Cyber Security Strategy].
[3] EPIC, Electronic Privacy Information Center, http://www.epic.org (last visited Dec. 1, 2009).
[4] EPIC, Privacy, http://www.epic.org/privacy/default.html (last visited Dec. 1, 2009).
[5] EPIC, The Smart Grid and Privacy, http://epic.org/privacy/smartgrid/smartgrid.html (last visited Dec. 1, 2009).

the short- and long-term consequences of losing them – either inadvertently, or by explicitly trading them away for perceived or ill-understood notions of security and convenience. http://www.privacyactivism.org.

Privacy Rights Clearinghouse (PRC) is a nonprofit consumer organization with a two-part mission -- consumer information and consumer advocacy. It was established in 1992 and is based in San Diego, California. It is primarily grant-supported and serves individuals nationwide. http://www.privacyrights.org/

The Electronic Frontier Foundation (EFF) is a non-profit, member-supported civil liberties organization based in San Francisco, California, that works to protect rights in the digital world. Because Smart Grid technology can gather detailed information about individual and family activities at home, privacy is a crucial concern; law enforcement today uses utility records, and the expected increase in amount and detail of information available through utilities with the Smart Grid will fuel demand for data about home activities that should only be available to government with a warrant. Privacy of the home can only be adequately protected in the Smart Grid if it is analyzed together with Smart Grid policy and architecture. Clear standards are needed as to what information (and how much and how detailed) is transmitted or available to utilities. System architecture (e.g. centralization vs. decentralization, network nodal structure) may permit significant minimization of data and detail; if homes and neighborhoods have significant computing capacity in local devices and networks, much monitoring, calculation and analysis of energy

usage can be done locally, obviating utility data collection in the first place.

http://www.eff.org/

The Liberty Coalition works to help organize, support and coordinate trans-partisan public policy activities related to civil liberties and basic rights. We work in conjunction with groups of partner organizations that are interested in preserving the Bill of Rights, personal autonomy and individual privacy. http://www.libertycoalition.net/

The U. S. Bill of Rights Foundation is a non-partisan public interest law policy development and advocacy organization seeking remedies at law and public policy improvements on targeted issues that contravene the Bill of Rights and related Constitutional law. The Foundation implements strategies to combat violations of individual rights and civil liberties through Congressional and legal liaisons, coalition building, mission development, project planning & preparation, tactical integration with other supporting entities and the filings of amicus curiae briefs in litigated matters.

http://usbor.netboots.net/

The Cyber Privacy Project (CPP) addresses concerns and issues about privacy raised in today's networked world. In upholding the belief that privacy is essential to democratic government, the Cyber Privacy Project anchors its approach in realizing the beneficial potential of the Constitution, laws and policies of the United States. CPP calls for implementation of privacy protections based on First Amendment rights of privacy and anonymity, Fourth Amendment rights against unreasonable searches and seizures, the

Fifth and Fourteenth Amendment rights to due process and protection of liberty, and Ninth Amendment implied rights to privacy. http://www.cyberprivacyproject.org/

The Rutherford Institute, a nonprofit legal and educational civil liberties organization, provides legal assistance at no charge to individuals whose constitutional rights have been threatened or been violated. The Institute has emerged as one of the nation's leading advocates of civil liberties and human rights, litigating in the courts and educating the public on a wide spectrum of issues affecting individual freedom in the United States and around the world. http://www.rutherford.org/

The World Privacy Forum is a nonprofit, non-partisan 501 (C) (3) public interest research group. The organization is focused on conducting in-depth research, analysis and consumer education in the area of privacy. It is the only privacy-focused public interest research group conducting independent, longitudinal work. The World Privacy Forum has had notable successes with its research, which has been groundbreaking and consistently ahead of trends. World Privacy Forum reports have documented important new areas, including medical identity theft. Areas of focus for the World Privacy Forum include health care, technology and the financial sector. The Forum was founded in 2003 and works both nationally and internationally. http://www.worldprivacyforum.org/

The Center for Financial Privacy and Human Rights was founded in 2005 to defend privacy, civil liberties and market economics and is part of the Liberty and Privacy Network, a Washington, DC-based 501(c)(3) organization. http://financialprivacy.org/

Consumer Action is a non-profit, membership-based organization that was founded in San Francisco in 1971. During its more than three decades, Consumer Action has continued to serve consumers nationwide by advancing consumer rights, referring consumers to complaint-handling agencies through our free hotline, publishing educational materials in Chinese, English, Korean, Spanish, Vietnamese and other languages, advocating for consumers in the media and before lawmakers, and comparing prices on credit cards, bank accounts and long distance services. http://www.consumer-action.org/

The American Civil Liberties Union (ACLU) is our nation's guardian of liberty, working daily in courts, legislatures and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country.

The ACLU also works to extend rights to segments of our population that have traditionally been denied their rights, including people of color; women; lesbians, gay men, bisexuals and transgender people; prisoners; and people with disabilities. http://www.aclu.org/

The American Library Association (ALA) strives to provide leadership for the development, promotion, and improvement of library and information services and the profession of librarianship in order to enhance learning and ensure access to information for all. In 1998 the ALA Council voted commitment to five Key Action Areas as guiding principles for directing the Association's energies and resources: Diversity, Equity of

Access, Education and Continuous Learning, Intellectual Freedom and 21st Century Literacy. http://www.alawash.org/

II. PRIVACY AND THE SMART GRID

a. DEFINING PRIVACY AND THE SMART GRID

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. Although most countries around the world include explicit protection of a right to privacy in their constitutions, it remains one of the more difficult terms to define.

The focus for protecting privacy of information stored on computers or exchanged on computing networks is whether data is or is not personally identifiable information (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 information is PII, our legal system has long recognized and protected the right of personal privacy in that information. The drafters of the Constitution "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be

deemed a violation" of constitutional principles.[6] As the Supreme Court noted, 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 electrical 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:

> [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 most minute 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

---

[6] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
[7] *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).
[10] *Id.* at 34.
[11] *Id.* at 37.

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. More broadly, "fair information practices," which set out the essential framework for the collection and use of personal information for any service provision, have been recognized in our legal system for years, beginning with the magisterial report of the U.S. Dep't. of Health, Education and Welfare (HEW) entitled *Records, Computers, and the Rights of Citizens*.[13] In that publication, the HEW Advisory Committee on Automated Personal Data Systems set out a Code of Fair Information Practices (FIPs), based on five principles:

> (1) There must be no personal data record-keeping systems whose very existence is secret. (2) There must be a way for a person to find out what information about the person is in a record and how it is used. (3) There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent. (4) There must be a way for a person to correct or amend a record of identifiable information about the person. (5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. [14]

The *HEW Report* also recommended enforcement mechanisms to ensure adherence to the principles:

> (1) The Code should define 'fair information practice' as adherence to specified safeguard requirements; (2) The Code should prohibit violation of

[12] *Id.* at 40.
[13] Dep't. of Health, Educ. and Welfare, *Secretary's Advisory Comm. on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens* (Government Printing Office 1973) [hereinafter "*HEW Report*"].
[14] *Id.* at xx-xxi.

> any safeguard requirements as an "unfair information practice"; (3) The Code should provide that an unfair information practice be subject to both civil and criminal penalties; (4) The Code should provide for injunctions to prevent violation of any safeguard requirement; (5) The Code should give individuals the right to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions. It should also provide for recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful suits.[15]

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 law. In fact, it provides the framework for the Privacy Act of 1974[16] and dozens of state and federal laws.[17]

The international community has also recognized the importance of robust fair information practices: in 1980, the International Organization of Economic Cooperation and Development (OECD) codified its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[18] 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:

---

[15] *Id.* at xxiii.
[16] Privacy Act of 1974 , 5 U.S.C. § 552a (2008).
[17] *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).
[18] *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).

1. Collection Limitation Principle – There should be limits to the collection of personal data; any such data collected should be 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 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.[19]

Representatives from North America, Europe and Asia drafted the original OECD Privacy Guidelines. Countries around the world, with varying cultures and systems of governance, have adopted roughly similar approaches to privacy protection with respect to the OECD Privacy Guidelines. 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. Thus,

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

fair information practices, as defined by the HEW Report and the OECD Guidelines, provide the essential starting point for analyzing the privacy implications of the Smart Grid.

b. ASSESSING SMART GRIDS AND PRIVACY

The Smart Grid implicates privacy at a fundamental level, as it can best be understood as a powerful digital communication network. Indeed, communications giant Cisco 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 admits the possibility of new and problematic threats to privacy in the form of increased data collection, retention, sharing and use.[21] As NIST acknowledges, "[t]he major benefit provided by the Smart Grid, i.e. the ability to get richer data to and from customer meters and other electric devices, is also its Achilles' heel from a privacy viewpoint."[22]

---

[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.

[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] National Institute for Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft) 84 (2009) [hereinafter Draft Framework].

The basic architecture of the Smart Grid presents several thorny privacy issues. The first widely distributed smart grid application is the smart meter.[23] 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.[24] Smart meters, like traditional meters, will be associated with a unique address, which makes it PII.[25] 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.

Smart meters could be designed or configured to report electricity consumption once a month, or weekly, or daily. However, proposals for smart meters discuss "real-time" reporting of usage data.[26] The design specification is not for that electricity consumption information to remain in the home or meter location, which could only be accessed easily

[23] *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. . . .").

[24] Draft Framework, *supra* note 22, at 21-22.

[25] *See* Cyber Security Strategy, *supra* note 2, at 33 (flow chart detailing Smart Grid communication links between consumers and providers).

[26] *See, e.g.*, Draft Framework, *supra* note 22, at 56.

by the utility user. Rather, the plan as suggested in the Cyber Security Strategy is to share the information with the utility company or others. If, as the document suggests, the information will 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 architectural point that raises privacy implications is the use of wireless communications to transmit Smart Grid data.[27] The Draft Framework proposed to assess "the capabilities and weaknesses of specific wireless technologies."[28] Although it mentions security as a characteristic of wireless technology that may be relevant to that assessment, it does not mention privacy. Any wireless technology that would be used to transmit user data must protect personal privacy. Wireless sensors and networks are susceptible to security breaches unless properly secured,[29] and breaches of wireless technology could expose users' personal data.[30] 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 homes and offices. A

[27] *See* Draft Framework, *supra* note 22, at 65.
[28] *Id.*
[29] *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).
[30] *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").

> 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.[31]

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.[32] 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,"[33] *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 independence in making certain

---

[31] *Id.*
[32] *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).
[33] Draft Framework, *supra* note 22, at 67.

kinds of important decisions,"[34] then this proposed application could severely damages both privacy interests and consumer rights.

c. 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. NIST should establish comprehensive privacy regulations that limit the collection and use of consumer data. Only by building privacy protection into the Smart Grid from the outset can NIST defend the robust privacy interests long protected by our legal system. The following paragraphs identify many of the privacy interests threatened by the Smart Grid.

i. IDENTITY THEFT

Identity theft victimizes millions of people each year.[35] 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.[36] According to the Privacy Rights Clearinghouse, more than 340 million records containing sensitive personal information have been involved in security breaches since January 2005.[37]

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 that there is "[a]

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

common tendency to place excessive faith in the infallibility of identification, authentication, and access controls to ensure security and privacy."[38]

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."[39] 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.'"[40] 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."[41] 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.[42]

ii. PERSONAL SURVEILLANCE

[38] *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).
[39] Jeanne Meserve, *'Smart Grid' May Be Vulnerable To Hackers*, CNN, March 21, 2009, http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability.
[40] *Id.*
[41] 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.
[42] *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.[43] For instance,"[e]nergy use in buildings can be reduced if building-system operations are coordinated with the schedules of the occupants."[44] 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."[45] "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." [46] 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.[47]

---

[43] Draft Framework, *supra* note 22, at 51.
[44] *Id.* at 52.
[45] 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 42.
[46] *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).
[47] *Privacy and the New Energy Infrastructure*, supra note 45, 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 46, at 869.

iii. ENERGY USE SURVEILLANCE

Smart Grid meter data may also be able to track the use of specific appliances within users' homes.[48] 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."[49] 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.), 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 is personally identifiable information for those occupying the residence.

[48] *See, e.g.*, *Privacy by Design*, *supra* note 21, at 8-9.
[49] *Smart Grid System Report*, *supra* note 23, 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.[50]

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.[51]

[50] *Privacy and the New Energy Infrastructure*, *supra* note 45, at 28.
[51] *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." [52]

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. [53] 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. [54] 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.[55] For instance, "meter data could reveal resident activities or uses that utility companies may then subsequently decide are inappropriate or should not be allowed."[56] 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.

---

[52] *Id.* at 25.
[53] *See Privacy Concerns*, *supra* note 42; 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)*"].
[54] *See Dangers (Part I)*, *supra* note 53.
[55] *See Privacy Concerns*, *supra* note 42.
[56] *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."[57] 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.[58] 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."[59] 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.

---

[57] *Draft Framework*, *supra* note 22, at 29.

[58] 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.").

[59] *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.

iv. 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.[60] 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. . . ."[61]

Similarly, the Smart Grid affects the interaction between privacy and domestic violence/stalkers.[62] Stalking, domestic violence and intimate partner abuse are also the targets of evolving state and federal policy.[63] Over the years this policy has increasingly included the protection of the privacy of stalking and domestic violence survivors.[64] 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

---

[60] *See Privacy and the New Energy Infrastructure*, *supra* note 45, at 30; *Privacy Concerns*, *supra* note 42; *Dangers (Part I)*, *supra* note 53.
[61] Morgan, et. al, *supra* note 59, at 5.
[62] *See generally* EPIC, Domestic Violence and Privacy, http://epic.org/privacy/dv (last visited Dec. 1, 2009).
[63] *See, e.g.*, Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960 (2005).
[64] *See* EPIC, Violence Against Women Act and Privacy, http://epic.org/privacy/dv/vawa.html (last visited Dec. 1, 2009).

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 may be able to relocate the victims using personal information transmitted through the Smart Grid.

v. MISUSE OF DATA

The massive amounts of data produced by the Smart Grid can potentially be misused by a number of parties—the power utilities themselves, authorized third parties such as marketing firms, or unauthorized third-parties such as identity 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. 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.[65] The TVA administrators are actively working to improve their ability to analyze the data, including through "complex data mining techniques."[66] Data mining of sensitive personal information raises serious privacy concerns.[67] For example, Total Information Awareness (TIA), developed by the Defense Advanced Research Projects Agency (DARPA), proposed to data mine wide swaths of information in order to detect

[65] 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.
[66] *Id.*
[67] *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).

terrorists.[68] However, privacy concerns led Congress to eliminate funding for the project, and the Technology and Privacy Advisory Committee of the Department of Defense issued a report[69] recommending that Congress pass laws to protect civil liberties when the government sifts through computer databases containing personal information. The data mining of sensitive personal information transmitted through the Smart Grid raises similar privacy concerns. Moreover, the TVA has explored using cloud computing resources to analyze and data mine the data, which raises a separate set of privacy concerns.[70]

Authorized third-parties may also be interested in using data collected 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.[71] 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

---

[68] *See id.*
[69] Department of Defense, *Safeguarding Privacy in the Fight Against Terrorism* (2004), *available at* http://www.epic.org/privacy/profiling/tia/tapac_report.pdf.
[70] *See* EPIC, Cloud Computing, http://epic.org/privacy/cloudcomputing (last visited Dec. 1, 2009).
[71] *See Privacy and the New Energy Infrastructure*, *supra* note 45, at 45; *Privacy Concerns*, *supra* note 42; *Dangers (Part I)*, *supra* note 53.

home energy consumption.[72] 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.[73] Such new business models also raise significant antitrust concerns.[74]

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. [75] Thus, the Smart Grid should be designed 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

[72] Google PowerMeter, http://www.google.org/powermeter (last visited Dec. 1, 2009).
[73] *See generally* EPIC, Privacy? Proposed Google/DoubleClick Merger, http://epic.org/privacy/ftc/google (last visited Dec. 1, 2009).
[74] *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).
[75] *See Privacy Concerns*, *supra* note 42.

Smart Grid data could reveal individual behaviors. Finally, the aforementioned data aggregation and data mining activity could permit publicized privacy invasions. Thus, NIST must be of the potential reputational harms presented by the Smart Grid.

III. EPIC RECOMMENDATIONS ON HOW TO MAKE THE SMART GRID PRIVACY SMART

a. NIST'S APPROACH IS INSUFFICIENT

NIST's Cyber Security Strategy report properly recognizes that one of the risks posed by the Smart Grid is the "[p]otential for compromise of data confidentiality, include the breach of customer privacy."[76] Within the rubric of potential risks to customer privacy, NIST conducted a Privacy Impact Assessment, examining the "privacy implications and related information security safeguards within the planned U.S. Smart Grid, particularly issues involved with consumer-to-utility data items collected and how they are used."[77]

NIST concluded that "[t]he results of a high-level PIA of the consumer-to-utility metering data sharing portion of the Smart Grid reveal that significant areas of concern must be addressed within each localized region of the Smart Grid."[78] More specifically, NIST found that the "lack of consistent and comprehensive privacy policies, standards and supporting procedures throughout the states, government agencies, utility companies and supporting entities that will be involved with Smart Grid management and information collection and use creates a privacy risk that needs to be addressed."[79]

---

[76] Cyber Security Strategy, *supra* note 2, at 2.
[77] *Id.* at 8.
[78] *Id.*
[79] *Id.*

NIST then identified ten principles "as a starting point for the development of appropriate protections for PII collected and/or used within the Smart Grid."[80] However, several of the principles are flawed, and NIST relies too heavily on the discredited notice and consent model of privacy protection. This comment proposes ways to strengthen NIST's recommendations for privacy protection in the Smart Grid environment.

b. ADOPT FAIR INFORMATION PRACTICES

PII activity should, as mentioned, be limited to a permitted and specified purpose. EPIC agrees that "only the minimum amount of data necessary for the utility companies to use for energy management and billing should be collected."[81] EPIC also agrees that treatment of information must conform to fair information practices. However, NIST should specify that those practices match the practices identified in the *HEW Report*[82] and the OECD Privacy Guidelines.[83] As discussed, the *HEW Report* established fair information practices, based on five principles:

> (1) There must be no personal data record-keeping systems whose very existence is secret. (2) There must be a way for a person to find out what information about the person is in a record and how it is used. (3) There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent. (4) There must be a way for a person to correct or amend a record of identifiable information about the person. (5) Any organization creating, maintaining, using, or disseminating records of

[80] *Id.* at 9.
[81] *Id.* at 12.
[82] *HEW Report*, *supra* note 13.
[83] OECD Privacy Guidelines, *supra* note 18.

identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. [84]

Similarly, the OECD Privacy Guidelines established eight principles for data protection that are widely used as the benchmark for assessing privacy policies and legislation: Collection Limitation; Data Quality; Purpose Specification; Use Limitation; Security Safeguards; Openness; Individual Participation; and Accountability.[85] The treatment of Smart Grid information should conform to those practices in the following manner:

OECD Privacy Principle	Corresponding Smart Grid Principle
Collection Limitation: There should be limits to the collection of personal data; any such data collected should be obtained by lawful means and with the consent of the data subject, where appropriate.	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.[86]
Data Quality: Collected data should be relevant to a specific purpose, and be accurate, complete, and up-to-date.	Data collected by Smart Grid service providers should be relevant to a specific purpose, and be accurate, complete, and up-to-date.
Purpose Specification: The purpose for collecting data should be settled at the outset.	The purpose for collecting Smart Grid data should be settled at the outset.
Use Limitation: The use of personal data ought be limited to specified purposes, and data acquired for one purpose ought not be used for others.	The use of Smart Grid personal data ought be limited to specified purposes, and data acquired for one purpose ought not be used for others.
Security Safeguards:	Smart Grid data must be collected and

[84] *HEW Report*, *supra* note 13, at xx-xxi.
[85] OECD Privacy Guidelines, *supra* note 18.
[86] "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).

Data must be collected and stored in a way reasonably calculated to prevent its loss, theft, or modification.	stored in a way reasonably calculated to prevent its loss, theft, or modification.
Openness: There should be a general position of transparency with respect to the practices of handling data.	There should be a general position of transparency with respect to the practices of handling Smart Grid data.
Individual Participation: Individuals should have the right to access, confirm, and demand correction of their personal data.	Smart Grid consumers should have the right to access, confirm, and demand correction of their personal data.
Accountability: Those in charge of handling data should be responsible for complying with the principles of the privacy guidelines.	Those in charge of handling Smart Grid data should be responsible for complying with the principles of the privacy guidelines.

Moreover, NIST should require enforcement of the guidelines in accordance with the *HEW Report*.[87] NIST should recommend enforcement mechanisms, such as civil and criminal penalties, injunctions and private rights of action. By specifying the parameters and enforcement of the fair information practices, NIST can require actual conformance, rather than loosely requiring treatment to "conform."

Several of the principles proposed by NIST reflect the FIPs contained in the *HEW Report* and the OECD Privacy Guidelines, which is commendable. However, the NIST guidelines also propose other principles that could be strengthened or improved upon.

c. ESTABLISH INDEPENDENT PRIVACY OVERSIGHT

The Cyber Security Strategy proposes that "[a]n organization should formally appoint personnel to ensure that information security and privacy policies and practices exist and are followed. Documented requirements for regular training and ongoing

[87] *HEW Report*, *supra* note 13, at xxiii.

awareness activities should exist and be followed. Audit functions should be present to monitor all data accesses and modifications."[88]

It is essential to ensure that information security and privacy policies and practices exist and are followed. NIST proposes that "[d]ocumented requirements for regular privacy training and ongoing awareness activities for all utilities, vendors and other entities with management responsibilities throughout the Smart Grid should be created implemented, and compliance enforced." However, it may be insufficient for organizations to simply provide privacy training to their employees or even to appoint dedicated privacy officers with audit functions.

For example, in an analogous situation, despite the training and audit authority conferred to the Chief Privacy Office of the Department of Homeland Security, that office has proven to be impotent, powerless to effectively protect privacy. On a range of issues, from whole body imaging to suspicionless electronic border searches, the Chief Privacy Officer for DHS has failed to fulfill her statutory obligations.[89] Accordingly, EPIC and other privacy and civil liberties groups have called for Congress to consider the establishment of alternative oversight mechanisms, including the creation of an independent office.[90] Without such an independent office,[91] it would be impossible to ensure the proper

[88] Cyber Security Strategy, *supra* note 2, at 9.
[89] *See* EPIC, Department of Homeland Security Chief Privacy Office and Privacy, http://epic.org/privacy/dhs-cpo.html (last visited Dec. 1, 2009).
[90] Letter from EPIC, et al., to Representatives Bennie G. Thompson and Peter T. King (Oct. 23, 2009), *available at* http://epic.org/security/DHS_CPO_Priv_Coal_Letter.pdf.
[91] *See*, *e.g.,* European Commission, Data Protection – National Commissioners, http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm (last visited

protection of privacy rights, because the decisions of the Chief Privacy Officer would continue to be subject to the oversight of the Secretary and the rest of the Executive branch.

Similarly, for Smart Grid organizations to appoint privacy personnel or simply train existing personnel would be an ineffective solution that would only serve to preclude the possibility of creating an independent position with actual authority to protect privacy. The better solution is simple – NIST should recommend that an independent Privacy Office, with completely independent authority be established, with power over all entities associated with the Smart Grid.

d. ABANDON THE NOTICE AND CONSENT MODEL

The NIST principles rely heavily on the notice and consent model:

> 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.[92]

As a threshold matter, the purposes for which PII can be collected, used, retained, or shared should be severely restricted. The purposes for which PII can be collected, used, retained, or shared should be severely restricted. It is insufficient to simply require

---

Dec. 1, 2009); Office of the Privacy Commissioner of Canada, http://www.priv.gc.ca/index_e.cfm (last visited Dec. 1, 2009); Office of the Privacy Commissioner for Personal Data, Hong Kong, http://www.pcpd.org.hk (last visited Dec. 1, 2009).

[92] Cyber Security Strategy, *supra* note 2, at 9.

authorities or organizations to have a nebulous "purpose," as anything from "improved marketing" to "government surveillance" could qualify. NIST should recommend that a formal rulemaking be established so that service providers establish a concrete set of approved purposes for which PII activity is permitted. That list of approved purposes should be very limited, and only purposes essential to the functioning of the Smart Grid should be permitted.

Once permissible purposes are established, data subjects should always be informed of the purpose of any collection, use, retention, or sharing of any PII. However, the "notice and consent" model is fundamentally flawed and should not be relied upon to excuse or justify any 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 comprehend, if they are read at all. It is not clear that consent today actually reflects a conscious choice by consumers. It is not clear that consent today actually reflects a conscious choice by consumers.[93]

Indeed, in EPIC's testimony before the United States Senate Committee on Commerce, Science and Transportation, Marc Rotenberg argued that "[s]olutions which

[93] David Vladeck, *Privacy: Where do we go from here?*, Speech to the International Conference of Data Protection and Privacy Commissioners, Nov. 6, 2009, *available at* http://www.ftc.gov/speeches/vladeck/091106dataprotection.pdf.

rely on simple notice and consent will not adequately protect users."[94] 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.[95] In two separate surveys almost 60% of consumers incorrectly believed that the presence of "privacy policy" meant that their privacy was protected.[96] 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.

Users also 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.[97] In such an environment, merely giving notice to users before collecting their sensitive information fails to adequately protect privacy in the way consumers expect.

Consumer data should instead receive substantive and ongoing protection. Especially because of the pervasiveness of the proposed nation-wide Smart Grid, choice and consent of individuals' is severely restricted. In all likelihood, individuals who wish to

---

[94] *Impact and Policy Implications of Spyware on Consumers and Businesses: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 110th Cong. (2008) (statement of Marc Rotenberg, President, EPIC).
[95] Joseph Turow, et al., *Consumers Fundamentally Misunderstand the Online Advertising Marketplace* (Oct. 2007), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf.
[96] *Id.* at 1.
[97] Pew Internet & American Life Project, *Spyware: The Threat of Unwanted Software Programs isChanging the way People use the Internet*, 6 (July 2005), *available at* http://pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf.

receive electricity will have little or no choice but to comply with policies that require the disclosure of PII. 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 it has been shared with, and to withdraw consent for the holding of this data. Further, data should only be collected and kept for specified purposes. 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.

e. IMPOSE MANDATORY RESTRICTIONS ON USE AND RETENTION OF DATA

NIST must ensure that restrictions on the use and retention of data is mandatory, not aspirational. The NIST guidelines propose that: "Information should only be used or disclosed for the purpose for which it was collected, and should only be divulged to those parties authorized to receive it. . . .PII should only be kept as long as is necessary to fulfill the purposes for which it was collected."[98]

It is insufficient to simply say that information *should* be used or disclosed only for a permitted purpose. Instead, NIST must *require* organizations to follow those policies, and must provide the authorities with the power to enforce them.

Furthermore, it is inadequate to permit PII to be retained "as long as is necessary to fulfill the purposes for which it was collected." That standard is entirely too lenient, and it would permit organizations too much leeway to retain information whenever they deem it

[98] Cyber Security Strategy, *supra* note 2, at 12.

necessary. Instead, NIST should set expiration dates on PII so that PII can be retained only for a certain period of time.[99] The length of time could vary based on the type of PII and the purpose for which it was collected. A concrete expiration date would make the system more transparent for consumers, as they would be more aware of the lifespan of their data.

NIST should also implement role-based access control to Smart Grid data. NIST has done significant work on the topic of role-based access control to computer records and systems. In this context, role-based access control protocols should strictly manage when, where, who and how PII in Smart Grid data is accessed. Access to PII, including electricity usage, should be limited to the function of the position an individual fills within the Smart Grid service delivery and billing relationship. Graduated levels of access should be based on responsibilities for providing Smart Grid FIPs and service provision purposes. Access should be monitored by log files and auditing of access use and resolution of issues related to customer service and proper operation of the Smart Grid.

Finally, NIST should explicitly address law enforcement access to Smart Grid data and should ensure that their access complies with the strictures of the Fourth Amendment. As discussed,[100] the Supreme Court in *Kyllo v. United States* addressed the interaction between the Fourth Amendment and the monitoring of electrical use, holding 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

[99] *See* Viktor Mayer-Schönberger, *Delete: the virtue of forgetting in the digital age* (2009) (arguing that digital information should have expiration dates, which will enable people to both control the sharing of information with others, as well as be more aware of the "finiteness of information).

[100] *See supra*, notes 9-12.

intrusion," without first obtaining a search warrant.[101] As the Court recognized, "'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"[102] Similarly, in the Smart Grid context, NIST should make clear that the Fourth Amendment protects the information of Smart Grid consumers, and that law enforcement must first obtain a search warrant before gaining access to the information.

f. VERIFY TECHNIQUES FOR ANONYMIZATION OF DATA

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 databases are joined. Such information can be obtained through public records, such as birth and death certificates.[103] 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.[104]

Similarly, according to the GAO, complete SSNs may be reconstructed from truncated digits by simply comparing truncated SSNs in federally generated public records,

---

[101] 533 U.S. 27, 40 (2001).
[102] *Id.* at 31 (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)).
[103] *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).
[104] Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J. Law, Med., & Ethics 98, 98–99 (1997).

which provide only the final four digits, to truncated SSNs provided by many information resellers, which provide only the first five digits.[105] Thus, by simply comparing the two records, a complete SSN can be reconstructed.[106]

Moreover, 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.[107] 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. 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.

g. ESTABLISH ROBUST CRYPTOGRAPHIC STANDARDS

[105] U.S. Gen. Accounting Office, *Identity Fraud Survey Report: Consumer Version* 2-3 (2009).
[106] *Id.* at 3.
[107] *See* Alessandro Acquisiti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 Proceedings of the National Academy of Sciences 10975.

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.[108]

> "**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."

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.[109]

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 algorithms, and perhaps even more significantly, by the environment in which the cryptography is implemented.[110]

---

[108] Patrick McDaniel & Stephen McLaughlin, Security and Privacy Challenges in the Smart Grid, IEEE Security and Privacy, May/June 2009, 75-77.
[109] David Chaum, *Achieving Electronic Privacy*, Scientific America, Aug. 1992, at 96-101, *available at* http://chaum.com/articles/Achieving_Electronic_Privacy.htm.
[110] Bruce Schneier, *Applied Cryptography* 21-46 (2d ed. 1996).

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.[111] 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.

It is disconcerting that a document prepared by the National Institute of Standards and Technology on what will be the most significant leap forward in digital communication capability in thirty years had so little to say about cryptography. The document mentioned "cryptography" and "encryption" only twice, and both times were in a table on standards and applications.

IV. CONCLUSION

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 NIST to take these recommendations into consideration in deciding the structure and capabilities of the Smart Grid. EPIC is willing and able to contribute to the further development of Smart Grid policy that would help

[111] Peter Neumann, *Computer Related Risks* 132-180 (1995).

encourage robust privacy protection while allowing the Smart Grid to accomplish important policy objectives.

Respectfully submitted,

/s/

Marc Rotenberg
Executive Director
EPIC
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009

Lillie Coney
Associate Director
EPIC

Matthew Phillips
Appellate Privacy Fellow
EPIC

Deborah Pierce
Executive Director
Privacyactivism

Beth Givens, Director
Privacy Rights Clearinghouse

Michael Ostrolenk
Liberty Coalition

Lee Tien
Electronic Frontier Foundation

Mark P. Cohen, Esq.
Executive Director
Government Accountability Project

Dane vonBreichenruchardt,
President

U.S. Bill of Rights Foundation

Lisa Graves
Executive Director
Center for Media and Democracy

Richard Sobel,
Cyber Security Project

John W. Whitehead
President
The Rutherford Institute

Pam Dixon
Executive Director
World Privacy Forum

J. Bradley Jansen
Director
Center for Financial Privacy and
Human Rights

Michael Macleod-Ball
Acting Director
American Civil Liberties Union

Linda Sherry
Director, National Priorities
Consumer Action

Lynne E. Bradley,
Director, Office of Government
Relations
American Library Association