COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to
THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
"NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)"
November 9, 2009

By notice published in the Federal Register on October 9, 2009, the National Institute of Standards and Technology (NIST) announced it seeks public comment on the draft framework and roadmap for Smart Grid interoperability standards.[1] NIST seeks

> (1) Comments on the overall document and the contents of all chapters, except Chapter 4, Standards Identified for Implementation; and (2) Comments on . . . ``Standards Identified for Implementation'' (Chapter 4); the NIST-proposed ``Guidance for Identifying Standards for Implementation''; and recommendations for adding or removing standards and specifications on the list of standards identified for implementation (Table 2), referencing relevant guidance criteria. In addition, NIST requests comments on the standards in Table 3--additional standards NIST has identified for further review.[2]

Pursuant to this notice the Electronic Privacy Information Center submits the following comments to NIST regarding the privacy implications of the draft framework and roadmap.

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. 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

---

[1] NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft), 74 Fed. Reg. 52,181-83 (October 9, 2009), *available at* http://edocket.access.gpo.gov/2009/E9-24429.htm.
[2] *Id.*
[3] *Available at* http://www.epic.org/.

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 implication 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.

Background

The Energy Independence and Security Act of 2007 (EISA)[6] directed NIST to take "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems. . . ."[7] Accordingly, NIST published the "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)."[8] The Draft Framework states that it:

> describes a high-level reference model for the Smart Grid, identifies nearly 80 existing standards that can be used now to support Smart Grid development, identifies 14 high priority gaps, plus cyber security, for which new or revised standards are needed, documents action plans with aggressive timelines by which designated Standards Development

[4] *Available at* http://www.epic.org/privacy/default.html.
[5] *Available at* http://epic.org/privacy/smartgrid/smartgrid.html.
[6] *Id.* at 52,182; Pub. L. No. 110-140, 121 Stat. 1492 (codified as amended in scattered sections of 42 U.S.C.).
[7] EISA § 1305.
[8] National Institute for Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft) 5 (2009) [hereinafter Draft Framework].

> Organizations are tasked to fill these gaps, and describes the strategy being pursued to establish standards for ensuring cyber security of the Smart Grid.[9]

The NIST Framework is ambitious scope, covering a wide range of issues, but it mentions privacy only briefly. The first reference to "privacy" comes on page 74 of the 90 page document, after all discussion of standards and "priority action plans."[10]

Once privacy is finally discussed, it is through a fleeting reference to the privacy implications of the Smart Grid under a section titled "Other Issues that Must be Addressed."[11] That section references and summarizes the findings of another report, entitled "Smart Grid Cyber Security Strategy and Requirements."[12]

Privacy cannot effectively be protected when it is an afterthought, and NIST cannot purport to establish a Smart Grid Framework without weaving security and privacy concerns into the framework at a fundamental level. Accordingly, NIST should first review comments regarding the security and privacy of the Smart Grid, and then incorporate those comments into a revised version of the Draft Framework.

EPIC's comments will focus on the significant privacy implications of the Smart Grid proposal and a proposed framework for privacy protection.

---

[9] *Id.*
[10] *Id.* at 74.
[11] *Id.* at 81.
[12] National Institute of Standards and Technology, Smart Grid Cyber Security Strategy and Requirements (2009).

EPIC's Comments and Recommendations

1. The Smart Grid Has Significant Privacy Implications

The collection of personally identifiable information will dramatically transform the ability of providers of power services in the United States to track the activities of American consumers. Some of this tracking will serve the important purpose of reducing energy consumption. But other forms of tracking may be completely unrelated to the stated goal of the Smart Grid program. It is for this reason that comprehensive privacy regulations that limit the collection and use of this data need to be established.

The Smart Grid may threaten privacy in many different ways. First, the Smart Grid could reveal sensitive personal behavior patterns. The Draft Framework proposes to create a "draft specification for facilitating common scheduling operations."[13]That is, coordinate power supply based on the schedules of the power needs of users and the availability of power. For instance, [e]nergy use in buildings can be reduced if building-system operations are coordinated with the schedules of the occupants."[14] 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."[15] "For example, research has delineated the

[13] Draft Framework, *supra* note 8, at 51.
[14] *Id.* at 52.
[15] 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* Rebecca Herold, SmartGrid *Privacy Concerns*, *available at*

differences in availability at home for various social types of electricity consumers including working adults, senior citizens, house wives, and children of school age." [16] 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.[17]

That concern is further exacerbated by the fact that Smart Grid meter data may be able to track the use of specific appliances within users' homes:

> 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.[18]

The ability to track appliance usage data has significant privacy implications: "With the whole of a person's home activities laid to bare, [appliance-usage tracking] provides a

---

http://www.privacyguidance.com/files/SmartGridPrivacyConcernsTableHeroldSept_2009.pdf [hereinafter *Privacy Concerns*].

[16] *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).

[17] *Privacy and the New Energy Infrastructure* 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 at 869.

[18] *Privacy and the New Energy Infrastructure* at 28.

better look into home activities than would peering through the blinds at that house."[19] 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.[20] For instance, appliance usage data could be transferred to appliance manufacturers to respond to warranty claims.[21] Or, the data could be transferred to insurance companies that may want the information as part of an investigation into an insurance claim.[22] 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.

The Draft Framework's discussion of "IP-Based Networks" fails to take those risks into account. The Framework states that protocols for such networks have not yet been identified, and that future rulemakings will permit comments on the protocols selected. However, it does not mention the protection of privacy as one of the attributes that would be needed in an IP-based 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." 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

[19] *Id.* at 25.
[20] *See Privacy Concerns*, *supra* note 15; 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)*"].
[21] *See Dangers (Part I)*, *supra* note 20.
[22] *See id*.

track activities of a device (and an associated individual)," thereby revealing an individual's health condition, daily activities, and other sensitive and private information.[23] Moreover, allowing the devices access to the Internet will make them more vulnerable, increasing the likelihood of security breaches and loss of personal privacy.[24] 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.

One specific use of the Smart Grid that implicates unique privacy concerns is the interaction 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,"[25] *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 kinds of

[23] 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.").

[24] *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 ("All of these communication links introduce vulnerabilities, especially if they can be accessed over the Internet. We 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 or a hacker on the other side of the world can cause system-wide instabilities and blackouts.").

[25] Draft Framework, *supra* note 8, at 67.

important decisions,"[26] then this proposed application severely damages consumers' privacy rights.

Moreover the real-time data streaming capabilities of the Smart Grid 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.[27] Similarly, the 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.[28]

Conversely, the Smart Grid should be structured in order to avoid the *retention* of PII. 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.[29]

The Smart Grid also heightens the risk of identity theft, as PII contained in the data transmitted to and from the consumer and the service providers could be intercepted and misused.[30] 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.[31]

Finally, not only does the content of the data itself pose privacy risks, but the *transmission* of that data raises separate risks. The Draft Framework proposes to assess

---

[26] *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977).
[27] *See Privacy and the New Energy Infrastructure* at 29; *Privacy Concerns*, *supra* note 15; *Dangers (Part I)*, *supra* note 20.
[28] *See Privacy and the New Energy Infrastructure* at 30; *Privacy Concerns*, *supra* note 15; *Dangers (Part I)*, *supra* note 20.
[29] *See Privacy Concerns*, *supra* note 15.
[30] *See id*.
[31] *See id.*

"the capabilities and weaknesses of specific wireless technologies."[32] 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,[33] and breaches of wireless technology could expose users' personal data.[34] 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 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.[35]

In summary, the collection of data through the Smart Grid could dramatically enhance the ability of energy providers, as well as both authorized and un-authorized third parties, to track the activities of energy consumers. Comprehensive privacy regulations limiting the collection and use of this data must therefore be established to ensure that the data collected is used for appropriate purposes.

---

[32] Draft Framework, *supra* note 8, at 65.
[33] *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).
[34] *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").
[35] *Id.*

2. Our Legal System Protects Personal Privacy

Our legal system has long recognized and protected the right of personal privacy. 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.[36] 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."[37] 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.[38]

More specifically, fair information practice principles 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*.[39] In that publication, the HEW Advisory Committee on Automated Personal Data Systems set out a Code of 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

[36] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
[37] *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977).
[38] *See generally* EPIC: Public Opinion on Privacy, *available at* http://epic.org/privacy/survey/.
[39] 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*"].

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. "[40]

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 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." [41]

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

[40] *Id.* at xx-xxi.
[41] *Id.* at xxiii.

Privacy Act of 1974 and dozens of state and federal laws. Fair Information Practices also provide the essential starting point for analyzing the privacy implications of new systems.

However, the Draft Framework fundamentally fails to address privacy issues raised by the Smart Grid. There is simply no effort to articulate a policy framework to address the privacy implications of the proposal.

3. The Smart Grid Must Be Structured to Protect Privacy

The Smart Grid can and should be structured in a way that protects the privacy of utility consumers. As a threshold matter, the Smart Grid should be structured in a way that adheres with the fair information practice principles enunciated in the *HEW Report*.[42] 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. NIST should recommend that authorities 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. Moreover, authorities should distinguish between the different types of PII activity when establishing the permitted purposes. For instance, it may be permissible to collect or use PII for the purpose of conserving energy, but it may be impermissible to retain or share the same PII for that purpose if it would require the PII to be shared with third parties.

[42] *See supra*, notes 36-38.

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, authorities and organizations must not be permitted to "hide" behind notices. Notices should not be used to justify superfluous collection, use, retention, or sharing of PII. Authorities' and organizations' primary objective must be to limit those activities to permissible purposes, not to expand them and justify them after the fact with notices.

Moreover, in order to ensure that the fair information practices are adhered to, NIST should incorporate enforcement mechanisms, such as civil and criminal penalties, injunctions, and private rights of action.[43] An independent privacy agency could also help enforce privacy rules.

More specifically, several of the technical capabilities of the Smart Grid should be structured in ways that protect user privacy. Any coordination of scheduling must be sensitive to privacy rights and ensure that PII is not collected or disseminated during that coordination—including PII arising from appliance usage. It must be structured so that real-time data cannot be used—by authorized or un-authorized parties—in a way that reveals PII about the utility customers. To avoid problems raised by the retention of PII, the meters should be constructed so that they do not retain any PII.

On the issue of PEVs, consumers should have exclusive control over the fact that power is stored in their PEVs and other devices. Consumers should certainly have control over the use of that energy.

[43] *See supra* notes 36-38.

One way in which the Smart Grid can accomplish its policy goals while still protecting privacy is by providing utility customers with usage information and giving them the power to alter their usage accordingly. The Draft Framework recognizes this option by proposing to "define data standards to enable customers and customer-authorized third-party service or software providers to access energy usage information from the Smart Grid, enabling customers to make better decisions about energy use and conservation."[44] Providing consumers with usage information is an effective way to encourage energy reduction while minimizing the collection or use of PII. NIST should emphasize this function of the Smart Grid, and make end-user control of energy use a primary means by which to achieve the goals of the Smart Grid.

Despite these concrete ways in which the Smart Grid could be structured in order to better protect privacy, the Draft Framework largely fails to take any steps towards incorporating more robust protection of privacy into the Smart Grid. It rightfully recognizes that privacy vulnerabilities in the proposed Smart Grid, including the "[p]otential for compromise of data confidentiality, including the breach of customer privacy."[45] It goes on to briefly address some of the privacy issues raised by the Smart Grid:

> Privacy advocates have raised serious concerns about the type and amount of billing and usage information flowing through the various entities of the Smart Grid, the dangers posed by data aggregation of what was considered to be "anonymized" data, and the privacy implications of frequent meter readings that could provide a detailed time-line of activities occurring inside the home. [46]

[44] Draft Framework, *supra* note 8, at 56.
[45] *Id.* at 74.
[46] *Id.* at 84.

However, the Draft Framework fails to propose ***any*** suggestions that would ameliorate those privacy concerns, and does not discuss or respond to many of the other concerns presented in this Comment. The protection of privacy rights must be fundamentally incorporated into the basic structure of the Smart Grid, which the Draft Framework purports to represent.

Finally, the Draft Framework states that:

> Future research is necessary to keep up with the multitude of use cases of the various technologies and business processes created for the Smart Grid. Legal and regulatory frameworks can be further harmonized and updated as the Smart Grid becomes more pervasive. PIAs of data collection, data flows and processing are also crucial for a deeper understanding of the evolutionary and revolutionary changes that are coming about with the rollout of Smart Grid implementations.[47]

By the time "the Smart Grid becomes more pervasive," it will be too late to incorporate effective privacy protection. The revised version of the Draft Framework ***must*** incorporate privacy protection and not merely refer to extrinsic documents or future proposals. The following paragraphs suggest ways in which the existing text of the Draft Framework could be amended to better protect privacy, to the extent that it has not previously been addressed by this Comment.

The Draft Framework, in the "Priority Action Plans" section, proposes to develop a price model that "will define how to exchange data on energy characteristics, availability, and schedules to support efficient communication of information in any market."[48] When developing that model, NIST should recognize that the protection of privacy is a benefit that should reduce prices, not increase them. For instance, one researcher found that

[47] *Id.*
[48] *Id.* at 50.

> Privacy saves money. If privacy rules force record keepers to keep fewer records or to maintain records for a shorter period, the costs of record maintenance will be reduced. If accurate records result in fairer decision making about individuals, savings and benefits will result. If privacy protections encourage more individuals to use the Internet to make purchases and to engage in other activities, the cost of doing business will drop, and many will benefit.[49]

Those findings are easily extended to the context of the Smart Grid. By protecting privacy on the front end, utility companies and other entities will save money. Thus, the price model should reflect the benefits of privacy protection and, as privacy is increased, price should go down.

[49] Robert Gellman, Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete 36 (2002).

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 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