

# Chapter 14

## Broadband Networks and Smart Grid: How Do We Build a Better Tomorrow?

Lillie Coney

Broadband and smart grid deployment are leading the digital wave that is sweeping the world. Along with these changes are others that are just as significant. For example, how people share information, learn, work, and are entertained has drastically changed over the last decade because of wireless broadband communication networks and consumers' embrace of portable digital communication devices. Today, people are not limited to just one-to-one communication, but can engage in one-to-many communication. Although changes are happening on the micro- and macro-level, often the most visible are the micro-changes in the form of new personal computing devices such as iPads, e-books, digital phones or faster and broadly available communication networks. These changes are re-inventing how people experience work, leisure, and engage in civic affairs. The challenge for innovators, policy makers and consumers is determining how best to use resources made available through a broadband connected world. There are significant differences in the pre-and post- broadband Digital Information Age:

- Information is not recorded in physical form
- Digital communication systems are used for essential commercial, and government service provision
- Consumers have fewer choices for initiating, accessing, and receiving services by first engaging in face-to-face communications with other people

Today, human capacity for creativity, innovation and information exchange relies on a digital infrastructure created during the 1960s with a modest goal of networking a few high-level federal government research institutions separated by a few thousand miles. The capacity for economies or rankings of national progress among nations will rest on their capacity for information management. A potential downside to the digital information age is to what extent information warehouses will be able to collect, retain, protect, share or restrict access to knowledge. The invention of written language

---

L. Coney (✉)  
Electronic Privacy Information Center (EPIC),  
1718 Connecticut Avenue NW Suite 200, Washington, DC 20009, USA  
e-mail: coney@epic.org

as a means of collecting, retaining, sharing or restricting access to information worked because literacy rates were initially very low. However, as literacy ceased to be a barrier to written information other means were deployed to prevent access to knowledge. The digital information age may re-introduce much more effective means for controlling access to information than was possible for written communications. This may be a challenge for government transparency and provision of services as well as undermining certitude regarding communications should conflicts arise.

In the midst of this digital information shift is the matter of personal information—its value; who controls it; does it merit ownership and if so why; and ultimately the importance of privacy as a right. For some time, privacy policy experts and legal scholars have ignored calls that announced the death of privacy because privacy is indeed alive. The question was always about its condition and future well-being.

There is a distinct set of conditions that give rise to modern discussions around the topic of privacy:

- Technology innovations that collect, records, retains, or shares personal information.
- A perceived, or real, lack of control by individuals over their personal information.
- Absence of customs, laws, or regulations to govern the collection, retention, use, or sharing of personal information.

Electronic Privacy Information Center (EPIC) has long been involved in the debate over whether digital information users can freely use strong encryption to secure information in transit on computer disk, or over the Internet or subnets. The key issue for broadband deployment and the Smart Grid are consumer control of their personal identifiable information in its many forms. The debate is with the many purposes to which that personal information may be used to enhance its value to collectors and to benefit consumers. The struggle for consumer privacy from an advocate's perspective is assuring that consumers are allowed to define what is or is not beneficial to them. To illustrate the points raised thus far, the Smart Grid will be a good model for the questions that will face policymakers, decision makers, consumers, researchers, innovators, and advocates as the new ways of the digital information economy replaces the old economy.

## **Privacy and Smart Grid**

Privacy is not a matter of ownership, but rather of control over personal information: how information is collected, if it is retained, how it may be used, what rights belong to the data subject, data holder oversight, and accountability obligations. It is interesting that the word "ownership" is cropping up in the context of the Smart Grid. Many residential, and some commercial energy consumers will likely not realize the value of energy usage data until instances of data abuse or misuse make that value evident. It is likely that, as a result of abuses or misuses of energy consumption data, the model of customer control will dominate the collection, retention, and use of Smart Grid data.

Ownership has well-defined meanings in commercial exchanges. Ownership means that one party conferred to another party through a mutual agreement the right of property ownership. Property can also mean that the right of ownership can be challenged by court proceedings and potential removed and assigned to another.

The condition of ownership in its purest form offers challenges to privacy—there may be means of conferring limited rights of personal data use but to forever relinquish the right to control who may use energy consumption information would be too great a cost—especially if the bargain rested on the provision of electricity service.

*Privacy protection has five key areas:*

- Physical privacy
- Informational privacy
- Decisional privacy
- Proprietary privacy
- Associational privacy

Privacy implications for Smart Grid technology deployment can touch on each of these five privacy areas.

For example, Smart Grid electricity consumption patterns may reveal when someone is home and when they are not, when a business is open and when employees are off the premises. The electricity data transferred by the Smart Grid presents information privacy questions. The need for electricity could create false choices that threaten decisional privacy regarding personal information. A requirements that customers must relinquish data privacy rights as a condition of receiving electricity service would effectively remove decisional privacy rights. As devices and appliances develop Smart Grid enabled energy consumption monitoring. There are already instances of proprietary privacy instances when consumer electricity consumption information is used in promotion material and reports to consumers reflecting their energy usage as compared with their neighbors. Finally, associational privacy may be an issue should electric vehicle recharge outlets collect data about then automobile such as VIN numbers or owner information.

Privacy is one of the most fundamental and basic of human rights. Without it, many other rights, such as freedom of speech, assembly, religion, the sanctity of the home, and/or business would be void. The route this nation took to the grand view of what ought to constitute a free people began with the Declaration of Independence, which spoke of very serious matters regarding the need of people to be free.

We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.<sup>1</sup>

The pursuit of happiness sounds whimsical, but it is the right to pursue the trade of your choice, to own a business, write a novel, or retire at the age of 35. The Constitution and its Amendments exist to protect us (the people) from a powerful government. An essential protection from powerful interests is our right to privacy. Thinking and acting as individuals empowered to govern ourselves requires that we can speak and think freely about whatever we want whenever we please. However, the right to privacy does not guarantee that we can express our thoughts or views in ways that diminish the rights or security of others, which is why definitions of what is and is not lawful are critical.

---

<sup>1</sup> Declaration of Independence, Continental Congress, July 4, 1776, [http://archives.gov/exhibits/charters/declaration\\_transcript.html](http://archives.gov/exhibits/charters/declaration_transcript.html).

## Privacy Fundamentals

The right of privacy is as old as human civilization. There is acknowledgement and recognition of the right of privacy in the sacred writings of many of the world's great religions—Jewish Law, The Bible, and the Qur'an. Privacy protection also existed in classical Greece and ancient China.

Privacy rights that are protected by criminal statutes existed in the West for centuries. However, in 1890, the proposition that tort law should protect privacy rights was outlined in a Harvard Law Journal article "The Right to Privacy," authored by Samuel Warren and Louis Brandeis, most famous for the phrase—"the right to be left alone." This article launched privacy violations into a whole new category, taking them out of the realm of mere criminal acts (e.g. eavesdropping prohibitions, or trespass laws), and into the category of human rights violations. Human rights are inalienable; such rights cannot be denied or abridged without sacrificing liberty and freedom.

There is no explicit right of privacy mentioned in the text of the Constitution or its Amendments. Supreme Court Associate Justice Louis Brandeis, co-author of the Harvard Law Journal Article, became a leading voice for the proposition that the Constitution of the United States did provide for a right to privacy. Brandeis served on the Supreme Court from 1916 until 1939, and his most widely quoted opinion was a dissent in the *Olmstead* case, regarding telecommunication privacy from government eavesdropping.<sup>2</sup>

Following the abuses of human rights and dignity proceeding and during World War II, steps were taken by a collective of nations to protect themselves from aggressor nations and to uphold a set of basic values regarding human rights.<sup>3</sup> The United Nations was formed through the adoption of its charter by those nations who would make up its ranks. The member nations were also asked to sign-on to the Declaration of Human Rights—an equivalent document in importance to the United States Bill of Rights.<sup>4</sup> The Declaration of Human Rights contains much of the imagery and the tone of both the United States Constitution and its subsequent Bill of Rights concerning the rights of individuals to be secure from certain abuses and threats.

Article 12, Declaration of Human Rights, December 10, 1948

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

For the next 30 years, much of the work to establish privacy law in the United States fell to judicial decisions, state constitutions, and a few laws dealing with discrete problems.

*Griswold v. Connecticut*, 318 U.S. 478 (1965)

The Court declared that individuals have a constitutional right to privacy found in the "penumbras" or "zones" of freedom created by an expansive interpretation of the Bill of Rights

<sup>2</sup><http://epic.org/privacy/wiretap/>.

<sup>3</sup><http://www.un.org/en/documents/charter/preamble.shtml>.

<sup>4</sup><http://www.un.org/en/documents/udhr/index.shtml#ap>.

Katz v. United States, 389 U.S. 347 (1967)

- The 4th Amendment protects people and not places
- Police must obtain warrants when searches take place in public locations like a phone booth

Our legal system has long recognized and protected the right of personal privacy in personally identifiable information (PII). 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. 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.” Moreover, public opinion polls consistently find strong support among Americans for privacy laws to protect their personal information from government and commercial entities.

In an analogous context, the Supreme Court in *Kyllo v. United States* addressed the interaction between the Fourth Amendment and the monitoring of electrical use. After reviewing precedent, the Court found that individuals have strong privacy rights within their homes:

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.” Thus, the Court held that the police could not use thermal imaging equipment, which was not in general public use, “to explore details of the home that would previously have been unknowable without physical intrusion,” without first obtaining a search warrant.

In 1973, the Department of Health Education and Welfare commissioned a report on records, computers, and the rights of citizens.<sup>5</sup> Shortly after the report was published, revelations from the scandals of the Nixon White House captured the public’s attention and ushered in a wave of laws intended to protect individuals from the potential abuse of government records. The committee set out recommendations that established a “Code of Fair Information Practices,” which became the foundation of privacy protections in the United States and in many nations around the world.<sup>6</sup>

*The Code of Fair Information Practices (FIPs) states that:*

- There must be no personal data record keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.

<sup>5</sup> <http://epic.org/privacy/hew1973report/default.html>.

<sup>6</sup> <http://epic.org/privacy/hew1973report/Summary.htm>.

- 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 misuse of the data.

## **Federal Privacy Act of 1974**

The Federal Privacy Act of 1974 established rules for government agency collection, retention, and use of information on citizens. The law also restricted how and when federal government agencies could share information about individuals. The Federal Privacy Act was added as an amendment to the Freedom of Information Act (FOIA), which originally became law in 1968. FOIA is a critical compliment to the Federal Privacy Act because it assures the right of citizens to have access to information on what government agencies might know about them.

## **Transparency Is Key to Privacy**

*Sunlight is said to be the best of disinfectants; electric light the most efficient policeman* (Louis Brandeis, Harper's Weekly, Dec 20 1913)<sup>7</sup>

The FOIA is in its fourth decade and remains a powerful tool for shining light on the activities of government and institutions. Transparency is a means for electric energy consumers to understand how their information is being collected, retained, used, or shared by Smart Grid service providers. Transparency is critical to assuring that personal information managed on the Smart Grid and its related applications are consistent with FIPs.

The principles outlined in FIPs have been adopted and expounded upon by other nations, such as the Organization of Economic Cooperation and Development's Committee (OECD) for Information, Computer and Communication Policy's Working Party on Information Security and Privacy's Privacy Guidelines on global networks eight principles.

*OECD basic privacy principles:*

- Collection limitations: there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- Data quality: personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.
- Purpose specification the purposes for which personal data are collected should be specified not later than at the time of the data collection and the subsequent use

---

<sup>7</sup>[http://www.schneier.com/blog/archives/2005/04/brandeis\\_quote.html](http://www.schneier.com/blog/archives/2005/04/brandeis_quote.html).

limited to the fulfillment of those purposes or such other purposes that are not incompatible with those expressed prior to data collection.

- Use limitations: personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the “purpose specification” except: (a) with the consent of the data subject or (b) by the authority of law.
- Security safeguards: personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.
- Openness: there should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller.
- Individual participation: an individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him [or her]; (b) to have communicated to him [or her], data relating to him [or her]: within a reasonable time... in a reasonable manner; and in a form that is readily intelligible to him [or her]; (c) to be given reasons if a request [related to this principle] is denied, and to be able to challenge such a denial; and, (d) to challenge data relating to him [or her] and, if the challenge is successful to have the data erased, rectified completed, or amended.
- Accountability: a data controller should be accountable for complying with measures, which give effect to the principles state above.

Canada has two privacy laws that protect personal information and require data holders to adhere to federal laws. The first is the Privacy Act, which governs how government agencies must protect personal information.<sup>8</sup> Each of the 13 Canadian Provinces has some type of public sector law. The second Canadian privacy law is the Personal Information Protection and Electronic Documents Act (PIPEDA) passed in 2000, and it governs how private sector companies must protect personal information.<sup>9</sup> Only the Provinces of Alberta, Quebec, and British Columbia have their own private sector law, which usurps the federal PIPEDA law on private sector privacy regulation. Smart Grid would likely be under the 13 different Provincial government authorities, which will rely on PIPEDA unless they have their own law in place.

## Smart Grid and Privacy

The challenge for privacy and the Smart Grid is that the flow of information is not apparent or transparent to data subjects. Making the right of privacy real in this technological context is building it from the start and creating control by focusing data access at the consumer level.

---

<sup>8</sup> <http://laws.justice.gc.ca/en/P-21/FullText.html>.

<sup>9</sup> <http://laws.justice.gc.ca/en/ShowDoc/cs/P-8.6//20090818/en?page=1>.

There are several potential threats to customers of Smart Grid use that should be explored and addressed through architecture or protocols that control access to data.

### ***Disclosure of Private Facts or the Details of Activities within Homes or Businesses***

Smart Grid's design at present seeks to report on electricity usage in intervals that may be as short as 15 min or less time frames. It may also allow the drawing off of stored electricity from reserves on batteries (electric vehicles, large appliances, backup generators, etc.) owned by customers. The monitoring of electricity consumption in near real time, the ability to drain stores of power held by e-appliances, e-vehicles, or e-manufacturing components presents interesting challenges for privacy and autonomy.

Consumer energy signatures monitored and collected over a period of time may allow a new kind of surveillance, criminal or competitor exploits, and corruption of the customer utility relationship that test the resources of individuals and institutions. What could be learned from the energy consumption patterns of comparable structures with similar energy usage needs? Energy-use profiles could be helpful to utilities in determining what energy will be needed over time and for what period of time down to the minute. However, this same information in the hands of a thief, marketer, competitor, loan officer, stockholder, or others could pose significant problems for the energy consumer.

### ***Identity Theft***

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

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

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.” Similarly, some experts argue, “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.’” 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.” 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.

### *Personal Surveillance*

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. For instance, “[e]nergy use in buildings can be reduced if building-system operations are coordinated with the schedules of the occupants.” 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.” “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.” 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.

### *Energy Use Surveillance*

Smart Grid meter data may also be able to track the use of specific appliances within users’ homes or industrial equipment used by a commercial entity. These “smart appliances” or “smart devices” 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 specif[ic] limits, based on energy prices.”

As other devices become commercially available that are designed to send consumption data over the Smart Grid, the definition of PII will evolve as well. 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 model designation (Whirlpool, General Electric, etc.), product serial number, and the purchase history of the item may note the purchaser's name. Monitoring the function and operation of these items would be physically associated with an address, which is PII for those occupying the residence.

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.

In addition, application development has become a separate business from the development and sale of personal digital devices or social network services. There are thousands of trained and skilled software developers who are willing and able to create applications that perform useful tasks or entertain the user. Not long after the first Smart Meters or appliances are installed new Web applications may be available to collect, retain, and share energy usage information.<sup>10</sup>

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."

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. 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. Landlords could track the energy use and behavior patterns of renters/leasees. The data could even be used to impinge on civil liberties by facilitating censorship or limitation of activities based on energy consumption patterns. 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 possibility that the appliances could interface with the Smart Grid through IP-based networks further exacerbates the privacy issues. The Draft Framework 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

---

<sup>10</sup>[http://developers.facebook.com/get\\_started.php](http://developers.facebook.com/get_started.php).

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. 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.” 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.

### ***Physical Dangers***

Criminals, such as burglars or vandals, who could monitor real-time data in order to determine when the house is vacant, could use data of this knowledge to cause harm. 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...”

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

### ***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. The TVA administrators are actively working to improve their ability to analyze the data, including through “complex data mining techniques.” Data mining of sensitive personal information raises serious privacy concerns.

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 works with utilities to permit users to have home energy consumption data displayed through their Google account. This technology raises the possibility of combining Smart Grid data with Google’s preexisting ability to record, analyze, track, and profile the activities of Internet users with data that are both personally identifiable and data that are not personally identifiable.

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 are 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. Thus, the Smart Grid should be structured in order to avoid the 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. However, even if permitted, appropriate security measures should be implemented. Computing device remote access should limit access to Smart Grid critical infrastructure and PII of customers. Access should include protocols to rapidly terminate access from devices that are lost or stolen, and personal use of the devices should be prohibited in order to help avoid viruses, worms, or malicious applications.

The misuse of Smart Grid data could also harm consumers’ reputations in many different ways. The collection and sharing of Smart Grid data could cause unwanted publicity and/or embarrassment. Moreover, public aggregated searches of Smart Grid data could reveal individual behaviors. Finally, the aforementioned data aggregation and data mining activity could permit publicized privacy invasions.

## **Cyber Security and Privacy**

Cyber Security policy is intended to protect information in databases, communication networks, and access to Internet-based services. Privacy may be threatened when Cyber Security is defined in such a way that increases surveillance of network users in general without the presence of suspicion. President Obama said that Cyber Security would not involve mass collection or monitoring of Internet Communications.

The key for adequate privacy and Cyber Security considerations for Smart Grid and related applications is to recruit the best and brightest minds to share

information and collaborate on building a network that is secure and respectful of FIPs in the management of personal information it collects, retains, transmits, and uses.

## Smart Grid Privacy and Cyber Security

There are two kinds of harm that the Smart Grid might face: intentional and unintentional. Nature or the environment can cause harm, but it will never be based on an underlying intent. Utilities preparedness and response to hurricanes, tornadoes, ice storms, may in many ways resemble their response to man caused events that impact the reliability or availability of electricity.

However, the next greatest threat will be manmade intended or unintended consequences to the Smart Grid. New applications or devices added to a complex system of Smart Grid architecture may offer threats to reliability that might challenge service providers. Further, weaknesses in the underlying architecture; grid software and firmware development could also introduce vulnerabilities to information privacy and security. Further threats are posed by updates, or intentional exploitations of vulnerabilities or weaknesses inherent in the complexity of Smart Grid systems. Additionally, the applications introduced by third-party service providers may also pose risk to consumers.

For example<sup>11</sup>:

- Bypassing or overriding Smart Grid security protocols intended to protect personal or electricity usage data in transit or other critical functions by insiders. Errors in software design or intentional development of trapdoors during development or specifically for maintenance purposes that are exploited for unapproved or impermissible purposes.
- Inadequate identification, authentication, and authorization of users, tasks, and systems, which may result in system spoofing attacks when one component masquerades as another. In addition, incomplete or inconsistent authentication and validation problems can lead to breaches of personal information or exploits against critical Smart Grid infrastructure.
- Other problems can include improper installation of technology, improper finalization of Smart Grid infrastructure and applications.
- Improper encapsulation where internal Smart Grid system or subsystem are made in accessible from the outside.
- Reliance upon clocks, internal sequential processes that must occur before other critical functions can occur that can lead to system failures for securing of personal information or critical systems.
- Individuals who design and field Smart Grid energy management equipment independent of standards or oversight can pose risks to consumers. Customers of

---

<sup>11</sup> Peter G. Neumann, *Computer Related Risk*, pp. 105–108, 1995.

an energy usage management company in the United Kingdom were adversely affected when the system failed. As they occurred, problems with the energy manage company's service were fixed on the fly and eventually the system became so complicated that they attempted to redesign it. The underlying problem that created an inherent vulnerability was how electricity managed by the energy usage management company on its customers' behalf did not address backups should the system fail. Power supplied to the company's outstation fell below capacity and it tripped off heating systems. It was a very cold winter and after hours of waiting the power was restored. The failure resulted in the hospitalization of an elderly woman for hypothermia.<sup>12</sup>

Finally, the implications for protecting privacy of information stored on computers or exchanged on Smart Grid networks is whether data are or are not PII. This is information that can locate or identify a person, or can be used in conjunction with other information to uniquely identify an individual. Historically, PII would include name, social security number, address, phone number, or date of birth. In the Internet Age, the list of PII has grown to include e-mail addresses, IP addresses, social networking pages, search engine requests, logons, or passwords.

Privacy violations can lead to threats to individuals in a number of instances. For example,<sup>13</sup>

- A stalker killed Rebecca Schaeffer, a television actress after he used publically available California Division of Motor Vehicle (DMV) records to locate her home address.
- A former Arizona law enforcement officer collected information from three different sources to track down his estranged girl friend and murdered her.
- An Anaheim Police Department employee used access to DMV records to identify the home of a person targeted by anti-abortion group, which led to the Tustin, California, home being picketed in February 1993.

### ***Possibility of Significant Privacy Harms Posed by Wireless Smart Grid Applications***

Wireless Smart Grid technology used to transmit user electricity consumption data must protect privacy. Wireless sensors and networks are susceptible to security breaches unless properly secured, and breaches of wireless technology could expose users' personal data. This is more evident each day with disclosures that "Street View" collected vast amounts of granular usage data on home computer networks; cell phones, and other WI-FI enabled technology.<sup>14</sup>

---

<sup>12</sup> <http://catless.ncl.ac.uk/Risks/5.67.html#subj7.1>.

<sup>13</sup> *il*, footnote 10.

<sup>14</sup> [http://news.cnet.com/8301-31921\\_3-20082777-281/street-view-cars-grabbed-locations-of-phones-pcs/](http://news.cnet.com/8301-31921_3-20082777-281/street-view-cars-grabbed-locations-of-phones-pcs/).

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. 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 not only would provide a significant challenge to privacy of users, but may also pose economic as well as cyber security threats. Identity theft, third-party monitoring of utility use, cloning of key Smart Grid devices, manipulation of key functions that manage electricity reliability, facilitate 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.

“War Driving” thieves search for open unprotected wireless communication devices for the purpose of using it for communication purposes, or to steal data being transmitted over the device.

For example:

“War driving” hackers will search for unprotected wireless devices at shopping centers and strip malls. If the security of the device used by shopping centers or malls has weak wireless security, hackers will exploit it for the data they can obtain remotely. They can be stationed in a car parking lot outside of the structure where the wireless device is located.<sup>15</sup> The largest known security breach due to “War Driving” involved the theft of 45 million credit cards from the TJ Max and Marshalls’s chain of stores when hackers found vulnerability in the wireless technology used by the retailers.<sup>16</sup>

The degree to which Smart Grid systems and related applications would recalculate the formulation of what is knowable about the intimate details of home life by adding to the list of PII, or expanding on the collection, retention, use, and sharing of PII pose significant risk to consumers of electricity.

The conservative view of data security is to stop any possible bad thing by keeping knowledge bottled up. The converse view is to know everything knowable about everyone who might have some input or influence over a protected system. The first approach faces challenges in the “Digital Information Age” because anything that is knowable is learnable and therefore sharable. The Second approach poses serious problems for a free and democratic society.

## Recommendations

### 1. Adopt Smart Grid Fair Information Practices

---

<sup>15</sup> [http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/the\\_web/article4470120.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4470120.ece).

<sup>16</sup> <http://www.informationweek.com/news/mobility/showArticle.jhtml?articleID=199500385>.

---

**Smart grid fair information practices principle**


---

Smart Grid service providers should limit collection of consumers' personal data; any such data collected should be obtained by lawful means and with the consent of the consumer, where appropriate<sup>17</sup>

Data collected by Smart Grid service providers should be relevant to a specific purpose, and be accurate, complete, and up to date

The purpose for collecting Smart Grid data should be settled at the outset

The use of Smart Grid personal data ought to be limited to specified purposes, and data acquired for one purpose ought not be used for others

Smart Grid data must be collected and stored in a way reasonably calculated to prevent its loss, theft, or modification

There should be a general position of transparency with respect to the practices of handling Smart Grid data

Smart Grid consumers should have the right to access, confirm, and demand correction of their personal data

Those in charge of handling Smart Grid data should be responsible for complying with the principles of the privacy guidelines

---

2. Adopt Privacy Impact Assessment Models for evaluation of privacy and Smart Grid applications and systems.<sup>18</sup>
3. Establish Independent Privacy Oversight—organizations and institutions responsible for providing Smart Grid services to consumers or oversight of companies engaged in providing services to consumers should establish independent privacy oversight within their organizations. Regulatory authorities should establish independent privacy oversight of companies engaged in Smart Grid service provision.
  - Privacy Officer should have experience in privacy law as well as policy.
  - Privacy Office should be independent.
  - Privacy oversight should be based on FIPs compliance.
  - Privacy Office should have the resources to engage in Privacy Impact Assessments on uses of personal information or new forms of PII.
4. Abandon the Notice and Consent Model of privacy protection. Notice and choice has failed because of over reliance on it alone instead of all of the principles of FIPs. Notice in exchanges where the customer has not alternatives, such as in the case of electricity service does not work.
5. Institute restrictions on data retention and use to only those necessary to provide a benefit or service related to Smart Grid.
6. Institute end-to-end security requirements for Smart Grid systems, eliminate the use of wireless technology, and establish strong security standards for all applications that will communicate with or receive communication from the Smart Grid network.

---

<sup>17</sup>“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).

<sup>18</sup>[http://www.cio.gov/documents/pia\\_for\\_it\\_irs\\_model.pdf](http://www.cio.gov/documents/pia_for_it_irs_model.pdf).



7. Verify techniques that are intended to anonymize data be sure that they are effective and evaluate the potential for re-identification of individuals based on the anonymization process used.
8. Establish robust cryptographic standards to protect Smart Grid electricity usage data collection, retention, transfer, and use. Further evaluation and appropriate measures should be taken to protect other forms of personal information retained by service providers.<sup>19</sup>
9. Adopt standards and certification requirements that match or exceed those for aviation or medical technology.
10. Define due process rights of individuals when law enforcement seeks Smart Grid information or access to network communications.
11. Prohibit participation in Fusion Centers or Federal or state information sharing environment programs.
12. Consider the relevance of residential and commercial electricity backup capacity in the event of Smart Grid or related system failures.
13. Reject the data model of ownership and adopt a model based on customer control over data about energy usage.

## Conclusion

Privacy protection is essential to the successful implementation of the Smart Grid and failure to develop robust and implement privacy policy will hinder adoption of applications and services. Progress is marked by broad adoption as well as acceptance of innovation. Innovation without consideration of consumer privacy in a digital information economy is a system that will have many dead ends before it can find a smooth path to success.

---

<sup>19</sup><http://www.securecomputing.net.au/Feature/150901,hacking-the-smart-grid.aspx>.