NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid

The Smart Grid Interoperability Panel – Cyber Security Working Group

August 2010

NIST National Institute of Standards and Technology • U.S. Department of Commerce

NISTIR 7628

Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid

The Smart Grid Interoperability Panel–Cyber Security Working Group

August 2010

U. S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology (IT). ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This National Institute of Standards and Technology Interagency Report (NISTIR) discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7628, vol. 2
69 **pages (August 2010)**

ACKNOWLEDGMENTS

This report was developed by members of the Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP-CSWG), formerly the Cyber Security Coordination Task Group (CSCTG), and during its development was chaired by Annabelle Lee of the Federal Energy Regulatory Commission (FERC), formerly of NIST. The CSWG is now chaired by Marianne Swanson (NIST). Alan Greenberg (Boeing), Dave Dalva (CiscoSystems), and Bill Hunteman (Department of Energy) are the vice chairs. Mark Enstrom (Neustar) is the secretary. Tanya Brewer of NIST is the lead editor of this report. The members of the SGIP-CSWG have extensive technical expertise and knowledge to address the cyber security needs of the Smart Grid. The dedication and commitment of all these individuals over the past year and a half is significant. In addition, appreciation is extended to the various organizations that have committed these resources to supporting this endeavor. Members of the SGIP-CSWG and the working groups of the SGIP-CSWG are listed in Appendix J of this report.

In addition, acknowledgement is extended to the NIST Smart Grid Team, consisting of staff in the NIST Smart Grid Office and several of NIST's Laboratories. Under the leadership of Dr. George Arnold, National Coordinator for Smart Grid Interoperability, their ongoing contribution and support of the CSWG efforts have been instrumental to the success of this report.

Additional thanks are extended to Diana Johnson (Boeing) and Liz Lennon (NIST) for their superb technical editing of this report. Their expertise, patience, and dedication were critical in producing a quality report. Thanks are also extended to Victoria Yan (Booz Allen Hamilton). Her enthusiasm and willingness to jump in with both feet are really appreciated.

Finally, acknowledgment is extended to all the other individuals who have contributed their time and knowledge to ensure this report addresses the security needs of the Smart Grid.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

OVERVIEW AND REPORT ORGANIZATION

REPORT OVERVIEW

Version 1.0 (V1.0) of NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, is the Smart Grid Interoperability Panel—Cyber Security Working Group's (SGIP-CSWG's) report for individuals and organizations who will be addressing cyber security for Smart Grid systems. This includes, for example, vendors, manufacturers, utilities, system operators, researchers, and network specialists; and individuals and organizations representing the IT, telecommunications, and electric sectors. This report assumes readers have a functional knowledge of the electric sector and a functional understanding of cyber security.

AUDIENCE

This report is intended for a variety of organizations that may have overlapping and different perspectives and objectives for the Smart Grid. For example—

- *Utilities/asset owners/service providers* may use this report as guidance for a specific Smart Grid information system implementation;
- *Industry/Smart Grid vendors* may base product design and development, and implementation techniques on the guidance included in this report;
- *Academia* may identify research and development topics based on gaps in technical areas related to the functional, reliability, security, and scalability requirements of the Smart Grid; and
- *Regulators/policy makers* may use this report as guidance to inform decisions and positions, ensuring that they are aligned with appropriate power system and cyber security needs.

CONTENT OF THE REPORT

- Volume 1 – Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
  - Chapter 1 – *Cyber Security Strategy* includes background information on the Smart Grid and the importance of cyber security in ensuring the reliability of the grid and the confidentiality of specific information. It also discusses the cyber security strategy for the Smart Grid and the specific tasks within this strategy.
  - Chapter 2 – *Logical Architecture* includes a high level diagram that depicts a composite high level view of the actors within each of the Smart Grid domains and includes an overall logical reference model of the Smart Grid, including all the major domains. The chapter also includes individual diagrams for each of the 22 logical interface categories. This architecture focuses on a short-term view (1–3 years) of the Smart Grid.
  - Chapter 3 – *High Level Security Requirements* specifies the high level security requirements for the Smart Grid for each of the 22 logical interface categories included in Chapter 2.

  - Chapter 4 – *Cryptography and Key Management* identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives.
  - Appendix A – *Crosswalk of Cyber Security Documents*
  - Appendix B – *Example Security Technologies and Procedures to Meet the High Level Security Requirements*
- Volume 2 – Privacy and the Smart Grid
  - Chapter 5 – *Privacy and the Smart Grid* includes a privacy impact assessment for the Smart Grid with a discussion of mitigating factors. The chapter also identifies potential privacy issues that may occur as new capabilities are included in the Smart Grid.
  - Appendix C – *State Laws – Smart Grid and Electricity Delivery*
  - Appendix D – *Privacy Use Cases*
  - Appendix E – *Privacy Related Definitions*
- Volume 3 – Supportive Analyses and References
  - Chapter 6 – *Vulnerability Classes* includes classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.
  - Chapter 7 – *Bottom-Up Security Analysis of the Smart Grid* identifies a number of specific security problems in the Smart Grid. Currently, these security problems do not have specific solutions.
  - Chapter 8 – *Research and Development Themes for Cyber Security in the Smart Grid* includes R&D themes that identify where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the Smart Grid.
  - Chapter 9 – *Overview of the Standards Review* includes an overview of the process that is being used to assess standards against the high level security requirements included in this report.
  - Chapter 10 – *Key Power System Use Cases for Security Requirements* identifies key use cases that are architecturally significant with respect to security requirements for the Smart Grid.
  - Appendix F – *Logical Architecture and Interfaces of the Smart Grid*
  - Appendix G – *Analysis Matrix of Interface Categories*
  - Appendix H – *Mappings to the High Level Security Requirements*
  - Appendix I – *Glossary and Acronyms*
  - Appendix J – *SGIP-CSWG Membership*

CHAPTER FIVE
PRIVACY AND THE SMART GRID

The Smart Grid is an evolving construct of new technologies, services, and entities integrating with legacy solutions and organizations. The SGIP-CSWG privacy subgroup views the privacy chapter as a starting point for continuing the work to improve upon privacy practices as the Smart Grid continues to evolve and as new privacy threats, vulnerabilities and the associated risks emerge. The information in this chapter was developed as a consensus document by a diverse subgroup consisting of representatives from the privacy, electric energy, telecommunications and cyber industry, academia, and government organizations. The chapter does not represent legal opinions, but rather was developed to explore privacy concerns, and provide associated recommendations for addressing them. Privacy impacts and implications may change as the Smart Grid expands and matures. It should be noted that this chapter addresses residential users and their data. The CSWG Privacy Subgroup will begin to explore privacy concerns for commercial, industrial, and institutional energy consumers, and deliver updates to existing work to address any new privacy considerations based on the pace of Smart Grid evolution.

CHAPTER ABSTRACT

The Smart Grid brings with it many new data collection, communication, and information sharing capabilities related to energy usage, and these technologies in turn introduce concerns about privacy. *Privacy* relates to individuals. Four dimensions of privacy are considered: (1) *personal information*— any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, locational or social identity; (2) *personal privacy*—the right to control the integrity of one's own body; (3) *behavioral privacy*—the right of individuals to make their own choices about what they do and to keep certain personal behaviors from being shared with others; and (4) *personal communications privacy*—the right to communicate without undue surveillance, monitoring, or censorship.

Most Smart Grid entities directly address the first dimension, because privacy of personal information is what most data protection laws and regulations cover. However, the other three dimensions are important privacy considerations as well and should be considered by Smart Grid entities.

When considering how existing laws may deal with privacy issues within the Smart Grid, and likewise the potential influence of other laws that explicitly apply to the Smart Grid, it is important to note that while Smart Grid privacy concerns may not be expressly addressed, existing laws and regulations may still be applicable. Nevertheless, the innovative technologies of the Smart Grid pose new issues for protecting consumers' privacy that will have to be tackled by law or by other means.

The Smart Grid will greatly expand the amount of data that can be monitored, collected, aggregated, and analyzed. This expanded information, particularly from energy consumers and other individuals, raises added privacy concerns. For example, specific appliances and generators can be identified from the signatures they exhibit in electric information at the meter when collections occur with great frequency as opposed to through traditional monthly meter readings. This more detailed information expands the possibility of intruding on consumers' and other individuals' privacy expectations.

The research behind the material presented in this chapter focused on privacy within personal dwellings and electric vehicles and did not address business premises and the privacy of individuals within such premises. The researchers' conclusions based upon work in these primary areas are as follows:

- Evolving Smart Grid technologies and associated new types of information related to individuals, groups of individuals, and their behavior within their premises and electric vehicles privacy risks and challenges that have not been tested and may or may not be mitigated by existing laws and regulations.

- New Smart Grid technologies, and particularly smart meters, smart appliances, and similar types of endpoints, create new privacy risks and concerns that may not be addressed adequately by the existing business policies and practices of utilities and third-party Smart Grid providers.

- Utilities and third-party Smart Grid providers need to follow standard privacy and information security practices to effectively and consistently safeguard the privacy of personal information.

- Most consumers probably do not understand their privacy exposures or their options for mitigating those exposures within the Smart Grid.

Based on initial research and the details of the associated findings, a summary listing of all recommendations includes the following points for entities that participate within the Smart Grid:

- Conduct pre-installation processes and activities for using Smart Grid technologies with utmost transparency.
- Conduct an initial privacy impact assessment before making the decision to deploy and/or participate in the Smart Grid. Additional privacy impact assessments should be conducted following significant organizational, systems, applications, or legal changes—and particularly, following privacy breaches and information security incidents involving personal information, as an alternative, or in addition, to an independent audit.

- Develop and document privacy policies and practices that are drawn from the full set of Organisation for Economic Cooperation and Development (OECD) Privacy Principles and other authorities (see 5.4.1 "Consumer-to-Utility PIA Basis and Methodology"). This should include appointing personnel responsible for ensuring

privacy policies and protections are implemented.

- Provide regular privacy training and ongoing awareness communications and activities to all workers who have access to personal information within the Smart Grid.
- Develop privacy use cases that track data flows containing personal information to address and mitigate common privacy risks that exist for business processes within the Smart Grid.
- Educate consumers and other individuals about the privacy risks within the Smart Grid and what they can do to mitigate them.
- Share information with other Smart Grid market participants concerning solutions to common privacy-related risks.

Additionally, manufacturers and vendors of smart meters, smart appliances, and other types of smart devices, should engineer these devices to collect only the data necessary for the purposes of the smart device operations. The defaults for the collected data should be established to use and share the data only as necessary to allow the device to function as advertised and for the purpose(s) agreed to by Smart Grid consumers.

5.1 INTRODUCTION

Modernizing the current electric grid through the computerization and networking of intelligent components holds the promise of a Smart Grid infrastructure that can—

- Deliver electricity more efficiently;
- Provide better power quality;
- Link with a wide array of energy sources in addition to energy produced by power plants (such as renewable energy sources);
- Enable self-healing in cases of disturbance, physical and cyber attack, or natural disaster; and
- Provide consumers, and other individuals[1], with more choices based on how, when, and how much electricity they use.

Communications technology that enables the bidirectional flow of information throughout the infrastructure is at the core of these Smart Grid improvements, which rely upon collated energy usage data provided by smart meters, sensors, computer systems, and many other devices to

[1] Because consumers are often thought of as the individuals who actually pay the energy bills, the SGIP-CSWG privacy group determined it was important to include reference all individuals who would be within a particular dwelling or location since their activities could also be determined in the ways described within this chapter. From this point forward, for brevity, only the term “consumers” will be used, but it will mean all the individuals applicable to the situation being described.

derive understandable and actionable information for consumers and utilities—and it is this same technology that also brings with it an array of privacy challenges. The granularity, or depth and breadth of detail, captured in the information collected and the interconnections created by the Smart Grid are factors that contribute most to these new privacy concerns.

The Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP-CSWG) has worked since June 2009 to research privacy issues within the existing and planned Smart Grid environment. Its research to date has focused on privacy concerns related to consumers' personal dwellings and use of electric vehicles.[2] In July and August of 2009, the privacy subgroup performed a comprehensive privacy impact assessment (PIA) for the consumer-to-utility portion of the Smart Grid, and the results of this study have enabled the group to make the recommendations found in this chapter for managing the identified privacy risks.

The privacy subgroup membership is derived from a wide range of organizations and industries, including utilities, state utility commissions, privacy advocacy groups, academia, Smart Grid appliance and applications vendors, information technology (IT) engineers, and information security (IS) practitioners. This diversity of disciplines and areas of interest among the group's participants helps to ensure all viewpoints are considered when looking at privacy issues, and it brought a breadth of expertise both in recognizing inherent privacy risk areas and in identifying feasible ways in which those risks might be mitigated while at the same time supporting and maintaining the value and benefits of the Smart Grid.

Because this chapter will be read by individuals with a wide range of interests, professional fields, and levels of expertise with respect to Smart Grid privacy issues, careful consideration has been given to the chapter's structure, which is as follows:

1. **Discussion of the concept of privacy**. This establishes our common ground in understanding the notion of "privacy," and defines the notion of privacy, where readers may hold different viewpoints on the subject.
2. **Definitions of privacy terms**. Privacy terms are defined differently among various industries, groups, countries, and even individuals. We define the privacy terms used in this chapter.
3. **Overview of current data protection laws and regulations with respect to privacy**. Even though numerous laws exist to establish a range of privacy protections, it is important to consider how those privacy protections apply to the Smart Grid.
4. **Determination of personal activities within the Smart Grid**. This explains the creation of new data types in the Smart Grid, as well as new uses for data that has formerly only been in the possession of utilities outside of retail access states.[3]

[2] There may also be privacy concerns for individuals within business premises, such as hotels, hospitals, and office buildings, in addition to privacy concerns for transmitting Smart Grid data across country borders. However, because the existing collection of NIST use cases does not cover business locations or cross border data transmission, and in view of its time constraints, the Privacy Group did not research business premises or cross border privacy issues. The Privacy Group recommends these as topics for further investigation.

[3] "Retail access states" refers to those states offering programs whereby energy services companies may supply service to customers at market-based prices.

5. **Summary of the consumer-to-utility PIA**. Identifies key privacy issues identified by the privacy subgroup in performing its PIA for the consumer-to-utility portion of the Smart Grid and provides a guide for subsequent research.
6. **In-depth look at privacy issues and concerns**. Addresses follow-on research based on the PIA findings in which the privacy subgroup explored the broader privacy issues that exist within the entire expanse of the Smart Grid.
7. **Detailed analysis of representative privacy use cases**. Use cases can help Smart Grid architects and engineers build privacy protections into the Smart Grid. Some example privacy use cases were created for specific scenarios within the Smart Grid to identify privacy concerns and demonstrate how to use privacy use cases. Developers of Smart Grid applications, systems, and operational processes can employ a more comprehensive set of privacy use cases to create architectures that build in privacy protections to mitigate identified privacy risks.
8. **Conclusions and recommendations**. This section summarizes the main points and findings on the subject of privacy and collects in one place all of the recommendations found within this Privacy Chapter.
9. **Appendices**. Reference material.

5.2 WHAT IS PRIVACY?

There is no one universal, internationally accepted definition of "privacy," it can mean many things to different individuals. At its most basic, privacy can be seen as the right to be left alone.[4] Privacy is not a plainly delineated concept and is not simply the specifications provided within laws and regulations. Furthermore, privacy should not be confused, as it often is, with being the same as confidentiality; and personal information[5] is not the same as confidential information. Confidential information[6] is information for which access should be limited to only those with a business need to know and that could result in compromise to a system, data, application, or other business function if inappropriately shared.[7]

It is important to understand that privacy considerations with respect to the Smart Grid include examining the rights, values, and interests of *individuals*; it involves the related characteristics, descriptive information and labels, activities, and opinions of individuals, to name just a few applicable considerations.

For example, some have described privacy as consisting of four dimensions:[8]

[4] Warren, Samuel D. and Louis D. Brandeis "The Right to Privacy," Harvard Law Review, Vol. IV December 15, 1890 No. 5

[5] See a full definition and discussion of "personal information" in Appendix C.

[6] The use of the phrase "confidential information" in this document does not refer to National Security/classified information.

[7] For example, market data that does not include customer-specific details is considered confidential. Other chapters within this report address confidentiality in depth.

[8] *See* Roger Clarke, "What's Privacy?" at http://www.rogerclarke.com/DV/Privacy.html. Clarke makes a similar set of distinctions between the privacy of the physical person, the privacy of personal behavior, the privacy of personal

1. **Privacy of personal information**. This is the most commonly thought-of dimension. Personal information is any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, locational or social identity. Privacy of personal information involves the right to control when, where, how, to whom, and to what extent an individual shares their own personal information, as well as the right to access personal information given to others, to correct it, and to ensure it is safeguarded and disposed of appropriately.
2. **Privacy of the person**. This is the right to control the integrity of one's own body. It covers such things as physical requirements, health problems, and required medical devices.
3. **Privacy of personal behavior**. This is the right of individuals to keep any knowledge of their activities, and their choices, from being shared with others.
4. **Privacy of personal communications**. This is the right to communicate without undue surveillance, monitoring, or censorship.

Most Smart Grid entities directly address the first dimension, because most data protection laws and regulations cover privacy of personal information. However, the other three dimensions are important privacy considerations as well; thus dimensions 2, 3, and 4 should also be considered in the Smart Grid context because new types of energy use data can be created and communicated. For instance, we can recognize unique electric signatures for consumer electronics and appliances and develop detailed, time-stamped activity reports within personal dwellings. Charging station information can detail whereabouts of an EV. This data did not exist before the application of Smart Grid technologies.[9]

The privacy subgroup looked at how the Smart Grid, and the data contained therein, could potentially be used to infringe upon or otherwise negatively impact individuals' privacy in the four identified dimensions and then sought ways to assist Smart Grid organizations in identifying and protecting the associated information. While many of the types of data items accessible through the Smart Grid are not new, there is now the possibility that other parties, entities or individuals will have access to those data items; and there are now many new uses for the collected data, which may raise substantial privacy concerns. New energy use data is also created through applications of Smart Grid technologies. As those data items become more specific and are made available to additional individuals, the complexity of the associated privacy issues increases as well.

The mission of the privacy subgroup is to recognize privacy concerns within the Smart Grid and to identify opportunities and recommendations for their mitigation. In addition, the group strives to clarify privacy expectations, practices, and rights with regard to the Smart Grid by—

---

communications, and the privacy of personal data. Roger Clarke is a well-known privacy expert from Australia who has been providing privacy research papers and guidance for the past couple of decades.

[9] For instance, consider the enhanced ability the Smart Grid will give to determining a person's behavior within a home through more granular energy usage data.

- Identifying potential privacy problems and encouraging the use of relevant Fair Information Practice Principles[10]
- Seeking input from representatives of Smart Grid entities and subject matter experts, and then providing guidance to the public on options for protecting the privacy of—and avoiding misuse of—personal information used within the Smart Grid. This guidance is included in this chapter; and
- Making suggestions and providing information to organizations, regulatory agencies, and Smart Grid entities in the process of developing privacy policies and practices that promote and protect the interest of Smart Grid consumers and Smart Grid entities.

To meet this mission, this chapter explores the types of data within the Smart Grid that may place individuals' privacy at risk, and how the privacy risks related to the use, misuse, and abuse of energy data may increase as a result of this new, always-connected type of technology network.

Because "privacy" and associated terms mean many different things to different audiences, definitions for the privacy terms used within this chapter are found in Appendix C, and definitions for energy terms are included in Appendix I.

5.3 LEGAL FRAMEWORKS AND CONSIDERATIONS

5.3.1 Overview

In assessing privacy considerations and related legal impacts within the Smart Grid, it is important to understand existing regulatory and legislative frameworks, concepts, and definitions. This subsection discusses these themes in general terms and then narrows its focus to those deemed most relevant.

5.3.2 Existing Regulatory Frameworks

When considering the possible legal impacts to privacy engendered by the Smart Grid, and likewise the influence of laws that directly apply to the Smart Grid, it is important to note that current privacy laws may not explicitly reference the Smart Grid or associated unique Smart Grid data items. Moreover, existing U.S. state-level Smart Grid and electricity delivery regulations may not explicitly reference privacy protections.[11] However, even though Federal or State laws may not definitively reference the Smart Grid at this time, it is possible that existing laws may be amended to explicitly apply to the Smart Grid as as it is more widely implemented and touches more individuals.

While it is uncertain how privacy laws will apply to Smart Grid data, one thing that is certain is that the Smart Grid brings new challenges and issues with its new types of data, such as detailed personal use patterns of all electrical appliances used by any individual within a premise, usage

[10] Fair Information Practice Principles describe the manner in which entities using automated data systems and networks should collect, use, and safeguard personal information to assure their practice is fair and provides adequate information privacy protection.

[11] The SGIP-CSWG Privacy Group has compiled a list of most state Smart Grid and electricity delivery regulations and provided them in Appendix A as a useful resource for our readers.

patterns of all electrical appliances used in public, commercial and educational facilities, and fingerprint information about new device usage, including medical devices and vehicle charging data. These new data items, and the use of existing data in new ways, will require additional study and public input to adapt current laws or to shape new laws.

To understand the types of data items that may be protected within the Smart Grid by privacy laws and regulations, let us first consider some of the current and most prominent laws that provide for privacy protection. U.S. federal privacy laws cover a wide range of industries and topics, such as:

1. Healthcare: Examples include the Health Insurance Portability and Accountability Act (HIPAA) and the associated Health Information Technology for Economic and Clinical Health (HITECH) Act.
2. Financial: Examples include the Gramm-Leach-Bliley Act (GLBA), the Fair and Accurate Credit Transactions Act (FACTA), and the Red Flags Rule.
3. Education: Examples include the Family Educational Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA).
4. Communications: Examples include the First Amendment to the U.S. Constitution, the Electronic Communications Privacy Act (ECPA), and the Telephone Consumer Protection Act (TCPA).
5. Government: Examples include the Privacy Act of 1974, the Computer Security Act of 1987, and the E-Government Act of 2002.
6. Online Activities: Examples include the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act, commonly known as the "Patriot Act").[12]
7. Privacy in the Home: Examples are the protections provided by the Fourth and Fourteenth Amendments to the U.S. Constitution.
8. Employee and Labor Laws: Examples include the Americans with Disabilities Act (ADA) and the Equal Employment Opportunity (EEO) Act.

It is currently not clear to what extent the above laws providing privacy protections will apply to Smart Grid data. Most state provides additional privacy laws and regulations for a wide range of issues, such as for, but not limited to, the following, which may also apply to the Smart Grid:

- Privacy breach notice;
- Social Security number (SSN) use and protections ; and
- Drivers license use.

There are generally three approaches to protecting privacy by law—

[12] The acronym stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. The statute enacted by the United States Government was signed into law on October 26, 2001.

- **Constitutional protections**. The First, Fourth, and Fourteenth Amendments, covering personal communications and activities.
- **Data-specific protections**. These protect specific information items such as credit card numbers and SSNs, or specific technology such as phones or computers used for data storage or communication.
- **Contractual protections**. These are protections specifically outlined within a wide range of business contracts, such as those between consumers and business.

The application of Fourth Amendment considerations to data collected about appliances and patterns of energy consumption, including the extent that Smart Grid data reveals information about personal activities, such as those described in "Privacy Concerns in the Smart Grid" (subsection 5.6 of this chapter) has not yet been tested.

Even though public utilities commissions (PUCs) have protected energy data in some states such as California, the energy-related data produced by the Smart Grid may not be covered by privacy protection laws that name specific data items. Energy consumption patterns have historically not risen to the level of public concern given to financial or health data because (1) electrical meters had to be physically accessed to obtain usage data directly from buildings, (2) the data showed energy usage over a longer time span such as a month and did not show usage by specific appliance, and (3) the utilities were not sharing this data in the ways that will now be possible with the Smart Grid. Public concerns for the related privacy impacts will likely change with implementation of the Smart Grid, because energy consumption data can reveal personal activities and the use of specific energy using or generating appliances, and because the data may be used or shared in ways that will impact privacy.

While some states have examined the privacy implications of the Smart Grid, most states had little or no documentation available for review by the privacy subgroup. Furthermore, enforcement of state privacy-related laws is often delegated to agencies other than PUCs, who have regulatory responsibility for electric utilities.

5.3.3 Smart Grid Data Ownership

The legal ownership of Smart Grid energy data is the subject of much discussion. Various regulators and jurisdictions have treated the issue of who owns energy data differently. However, regardless of data ownership, the management of energy data that contains or is combined with personal information or otherwise identifies individuals, and the personal information derived from such data, remains subject to the privacy considerations described in this report. The custodian of energy data should consider managing and safeguarding the information in accordance with the recommendations included in this report.

5.3.4 Applicability of Existing Data Protection Laws and Regulations to the Smart Grid

Personally identifiable information (PII) has no single authoritative legal definition. However, as noted in Appendix A, there are a number of laws and regulations, each of which protects different specific types of information. A number of these were previously noted, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which defines individually identifiable health information, arguably the widest definition by many organizations throughout the U.S. of what constitutes PII within the existing U.S. federal regulations. State attorneys general have pointed to HIPAA as providing a standard for defining

personal information, and to cite one case, the State of Texas has adopted the HIPAA requirements for protected health information to be applicable to all types of organizations, including all those based outside of Texas. Many of these organizations could possibly be providing information via the Smart Grid—if not now, then almost certainly at sometime in the future.[13]

The private industry's definition of personal information predates legislation and is generally legally defined in a two-step manner, as *x* data (e.g., SSN) in conjunction with *y* data (e.g., name.) This is the legal concept of "personally identifiable information" or PII.

For example, the Massachusetts breach notice law,[14] in line with some other state breach notice laws, defines the following data items as being personal information:

> First name and last name or first initial and last name in combination with any one or more of the following:
>
> 1. Social Security number;
> 2. Driver's license number or state-issued identification card number; or
> 3. Financial account number.

Utilities often store SSNs and financial account numbers in their payroll or billing systems and have been obligated to follow the associated legal requirements for safeguarding this data for many years. The sharing and storage capabilities that the Smart Grid network brings to bear creates the new need to protect the items specifically named within existing laws, in addition to protecting new types of personal information that is created within the Smart Grid.

There is also the possibility of utilities possessing new types of data as a result of the Smart Grid for which they have not to date been custodians. These new types of data may be protected by regulations from other industries that utilities did not previously have to follow. As is revealed by the privacy impact assessment that is the subject of section 5.4 of this chapter, there is a lack of privacy laws or policies directly applicable to the Smart Grid. Privacy subgroup research indicates that, in general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid.[15] Comprehensive and consistent definitions of privacy-affecting information with respect to the Smart Grid typically do not exist at state or federal regulatory levels, or within the utility industry.[16]

---

[13] For example, the Texas Appellate Court stated that the HIPAA Privacy rule applies to the entire State of Texas. *See* Abbott v. Texas Department of Mental Health and Mental Retardation for details, or refer to the discussion at http://www.hipaasolutions.org/white_papers/HIPAA%20Solutions,%20LC%20White%20Paper%20-Texas%20AG%20Opinion%20On%20Privacy%20And%20HIPAA.pdf.

[14] *See* text of the Massachusetts breach notice law at http://www.mass.gov/legis/laws/seslaw07/sl070082.htm.

[15] Most public utility commissions have significant customer privacy policies that predate the Smart Grid.

[16] Edison Electric Institute, a trade association of investor-owned electric utilities, is developing a formal position on customer data access, which it expects to finalize during 2010.

The privacy subgroup is presently conducting an overview of the laws, regulations, and standards relevant to the privacy of energy consumption data, and its preliminary list of applicable state laws and regulations is given in Appendix A.

5.3.5 General Invasion of Privacy Concerns with Smart Grid Data

Two aspects of the Smart Grid may raise new legal privacy issues. First, the Smart Grid significantly expands the amount of data available in more granular form as related to the nature and frequency of energy consumption and creation, thereby opening up more opportunities for general invasion of privacy. Suddenly a much more detailed picture can be obtained about activities within a given dwelling, building, or other property, and the time patterns associated with those activities make it possible to detect the presence of specific types of energy consumption or generation equipment. Granular energy data may even indicate the number of individuals in a dwelling unit, which could also reveal when the dwelling is empty or is occupied by more people than usual. The public sharing of information about a specific location's energy use is also a distinct possibility. For example, a homeowner rigged his washing machine to announce the completion of its cycle via his social networking page so that the machine need not be monitored directly.[17] This raises the concern that persons other than those living within the dwelling but having access to energy data could likewise automate public sharing of private events without the dwellers' consent—a general invasion of privacy.

The concern exists that the prevalence of granular energy data could lead to actions on the part of law enforcement —possibly unlawful in themselves—and lead to an invasion of privacy, such as remote surveillance or inference of individual behavior within dwellings, that could be potentially harmful to the dwelling's residents. Law enforcement agencies have already used monthly electricity consumption data in criminal investigations. For example, in *Kyllo v. United States*,[18] the government relied on monthly electrical utility records to develop its case against a suspected marijuana grower.[19] Government agents issued a subpoena to the suspect's utility to obtain energy usage records and then used a utility-prepared "guide for estimating appropriate power usage relative to square footage, type of heating and accessories, and the number of people who occupy the residence" to show that the suspect's power usage was "excessive" and thus "consistent with" a marijuana-growing operation.[20]

As Smart Grid technologies collect more detailed data about households, one concern identified by the privacy group as well as expressed by multiple published comments is that law enforcement officials may become more interested in accessing that data for investigations or to develop cases. For instance, agencies may want to establish or confirm presence at an address at

[17] For a demonstration of how this was done, *see* the video, "Washing Machine Twitter Hack," by Ryan Rose at http://vimeo.com/2945872.

[18] *Kyllo v. United States*, 533 U.S. 27 (2001). *See* http://www.law.cornell.edu/supct/html/99-8508.ZO.html.

[19] *Id*. at page 30. The Supreme Court opinion in this case focuses on government agents' use of thermal imaging technology. However, the district court decision discusses other facts in the case, including that government agents issued a subpoena to the utility for the suspect's monthly power usage records. *See Kyllo v. United States*, 809 F. Supp. 787, 790 (D. Or. 1992), *aff'd*, 190 F.3d 1041 (9th Cir. 1999), *rev'd*, 533 U.S. 27 (2001).

[20] *Kyllo v. United States*, 809 F. Supp. 787, 790 (D. Or. 1992), *aff'd*, 190 F.3d 1041 (9th Cir. 1999), *rev'd*, 533 U.S. 27 (2001).

a certain critical time or even establish certain activities within the home —information that may be readily gleaned from Smart Grid data.

However, the Supreme Court in *Kyllo* clearly reaffirmed the heightened Fourth Amendment privacy interest in the home and noted this interest is not outweighed by technology that allows government agents to "see" into the suspect's home without actually entering the premises.[21] The Court stated, "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search" and is "presumptively unreasonable without a warrant."[22]

Second, unlike the traditional energy grid, the Smart Grid may be viewed as carrying private and/or confidential electronic communications between utilities and end-users, possibly between utilities and third parties[23], and between end-users and third parties. Current law both protects private electronic communications and permits government access to real-time and stored communications, as well as communications transactional records, using a variety of legal processes.[24] Moreover, under the Communications Assistance for Law Enforcement Act (CALEA), telecommunications carriers and equipment manufacturers are required to design their systems to enable lawful access to communications.[25] The granular Smart Grid data may also have parallels to call detail records collected by telecommunications providers. It is unclear if laws that regulate government access to communications will also apply to the Smart Grid.

In short, the innovative technologies of the Smart Grid pose new legal issues for privacy of the home, as well as any type of property location that has traditionally received strong Fourth Amendment protection. As Justice Scalia wrote in *Kyllo*: "The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[26]

5.3.6 Smart Grid Introduces a New Privacy Dimension

The ability to access, analyze, and respond to much more precise and detailed data from all levels of the electric grid is critical to the major benefits of the Smart Grid—and it is also a significant concern from a privacy viewpoint, especially when this data and data extrapolations are associated with individual consumers or locations. Some articles in the public media have raised serious concerns[27] about the type and amount of billing, usage, appliance, and other related information flowing throughout the various components of the Smart Grid.

---

[21] *Kyllo*, 533 U.S.

[22] *Kyllo*, 533 U.S.

[23] The term "third party" is one that is not well defined. The SGIP-CSWG privacy subgroup recognizes third party access as a significant issue and plans to address this in more depth in a future version of the chapter.

[24] Such as the Electronic Communications Privacy Act; 18 U.S.C. § 2510. *See* http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_119.html.

[25] *See* http://thomas.loc.gov/cgi-bin/bdquery/z?d103:H.R.4922:.

[26] *Kyllo*, 533 U.S.

[27] One example of this is available at http://www.istockanalyst.com/article/viewiStockNews/articleid/3461363.

There are also concerns across multiple industries about data aggregation of "anonymized" data.[28] For example, in other situations, associating pieces of anonymized data with other publicly available non-anonymous data sets has been shown by various studies to actually reveal specific individuals.[29] Figure 5-1 illustrates how frequent meter readings may provide a detailed timeline of activities occurring inside a metered location and could also lead to knowledge about specific equipment usage or other internal home/business processes.

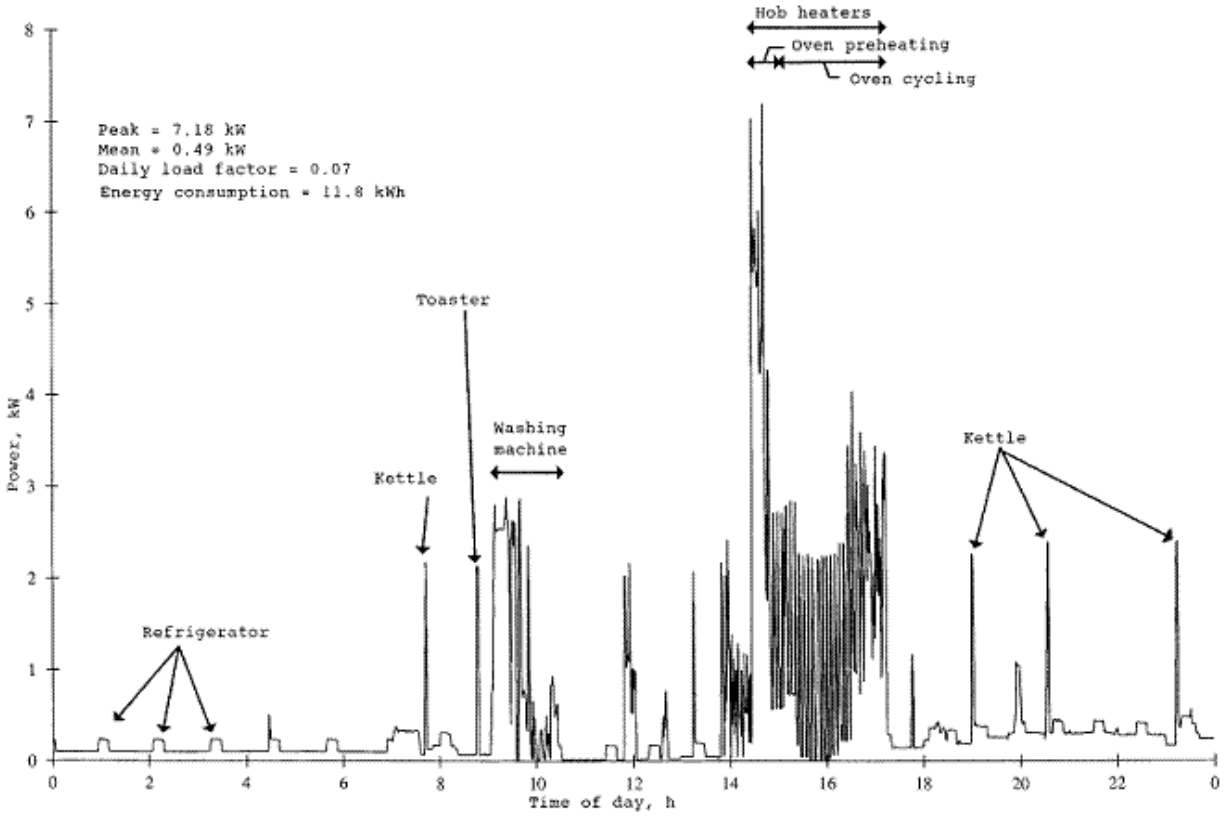

Figure 5-1 Power Usage to Personal Activity Mapping [30]

Smart meter data raises potential surveillance possibilities posing physical, financial, and reputational risks. Because smart meters collect energy usage data at much shorter time intervals than in the past (in 15-minute or sub-15-minute intervals rather than once a month), the information they collect can reveal much more detailed information about the activities within a dwelling or other premises than was available in the past. This is because smart meter data provides information about the usage patterns for individual appliances—which in turn can

28 The Electronic Privacy Information Center (EPIC), http://epic.org/privacy/reidentification/, provides news and resources on this topic.

[29] For one such study, see the technical paper, "Trail Re-identification: Learning Who You are From Where You Have Been," by Bradley Malin, Latanya Sweeney and Elaine Newton, abstract available at http://privacy.cs.cmu.edu/people/sweeney/trails1.html.

[30] Elias Leake Quinn, *Smart Metering & Privacy: Existing Law and Competing Policies, Spring 2009*, at page 3. Available at http://www.dora.state.co.us/puc/DocketsDecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-Smart GridPrivacy.pdf. A hob heater is a top of stove cooking surface.

reveal detailed information about activities within a premise through the use of nonintrusive appliance load monitoring (NALM) techniques.[31] Using NALM, appliances' energy usage profiles can be compared to libraries of known patterns and matched to identify individual appliances.[32] For example, research shows that analyzing 15-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances.[33, 34] The graph shown above (Figure 5-1) depicts NALM results as applied to a household's energy use over a 24-hour period. NALM techniques have many beneficial uses, including pinpointing loads for purposes of load balancing or increasing energy efficiency. However, such detailed information about appliance use can also reveal whether a building is occupied or vacant, show residency patterns over time, and reflect intimate details of people's lives and their habits and preferences inside their homes.[35] In 1989, George W. Hart, one of the inventors of NALM, explained the surveillance potential of the technique in an article in IEEE Technology and Society Magazine.[36] As the time intervals between smart meter data collection points decreases, appliance use will be inferable from overall utility usage data and other Smart Grid data with even greater accuracy.

In general, more data, and more detailed data, may be collected, generated, and aggregated through Smart Grid operations than previously collected through monthly meter readings and distribution grid operations. Figure 5-2 presents the NIST conceptual model illustrating how data collection can be expected to proliferate as networked grid components increase. In addition to utilities, new entities may also seek to collect, access, and use smart meter data (e.g., vendors creating applications and services specifically for smart appliances, smart meters, and other building-based solutions). Further, once uniquely identifiable "smart" appliances are in use, they will communicate even more specific information directly to utilities, consumers, and other entities, thus adding to the detailed picture of activity within a premise that NALM can provide.

---

[31] *Id*. at page A-2. The development of NALM involved a real-time monitoring device attached to a meter to log energy consumption. Researchers then worked backward from that information using complex algorithms to reconstruct the presence of appliances. Since smart meters and these NALM devices operate similarly, the same research and techniques can be reused to identify appliances.

[32] *Id*. at page A-4 n.129 (discussing the maintaining of appliance profile libraries).

[33] Research suggests this can be done with accuracy rates of over 90 percent. *See* Elias Leake Quinn, *Privacy and the New Energy Infrastructure*, Feb. 15, 2009, http://ssrn.com/abstract=1370731, at page 28.

[34] *See also* Steven Drenker & Ab Kader, *Nonintrusive Monitoring of Electric Loads*, IEEE Computer Applications in Power at pages 47, 50 (1999), noting the near perfect identification success rate in larger two-state household appliances such as dryers, refrigerators, air conditioners, water heaters, and well pumps. *Available at* http://ieeexplore.ieee.org/iel5/67/17240/00795138.pdf?arnumber=795138.

[35] For instance, daily routines such as showers and baths could be identified, as well as whether the customer "prefers microwave dinners to a three-pot meal." *Id*. Quinn, *Privacy and the New Energy Infrastructure*, at page 5.

[36] George W. Hart, Residential Energy Monitoring and Computerized Surveillance via Utility Power Flows, IEEE Technology and Society Magazine, June 12, 1989, http://ieeexplore.ieee.org/iel5/44/1367/00031557.pdf?arnumber=31557.

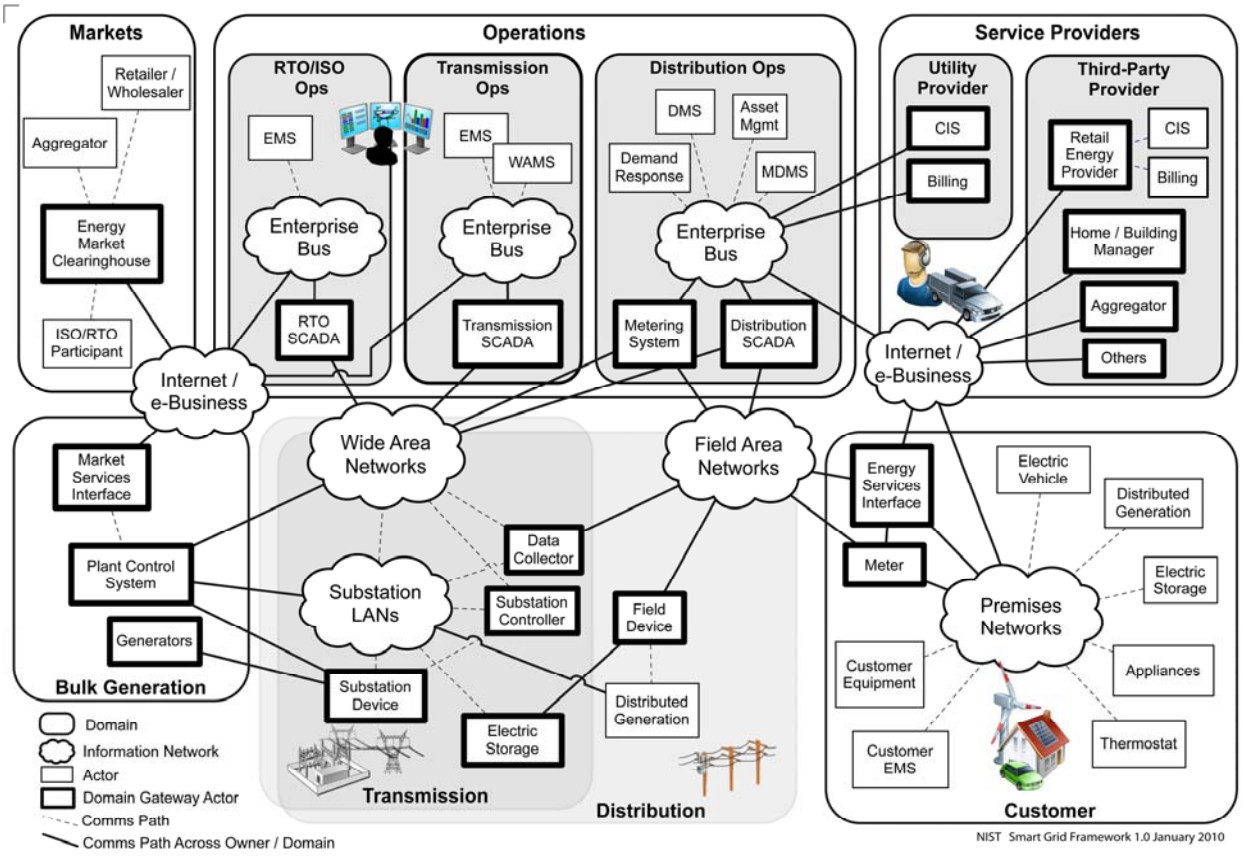

Figure 5-2 NIST Conceptual Model [37]

The proliferation of smart appliances, utility devices, and devices from other entities throughout the Smart Grid, on both sides of the meter, means an increase in the number of devices that may generate data. The privacy risks presented by these smart appliances and devices on the consumer side of the meter are expanded when these appliances and devices transmit data outside of the home area network (HAN) or energy management system (EMS) and do not have documented security requirements, effectively extending the perimeter of the system beyond the walls of the premises.

Data may also be collected from plug-in electric vehicles (PEVs). Charging data may be used to track the travel times and locations for the PEV owners.

5.4 CONSUMER-TO-UTILITY PRIVACY IMPACT ASSESSMENT

A PIA is a comprehensive process for determining the privacy, confidentiality, and security risks associated with the collection, use, and disclosure of personal information. PIAs also define the measures that may be used to mitigate and, wherever possible, eliminate the identified risks. The Smart Grid PIA activity provides a structured, repeatable type of analysis aimed at determining how collected data can reveal personal information about individuals or groups of individuals, and the focus of the PIA can be on a segment within the grid or the grid as a whole. Privacy risks

[37] *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.* Available at http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

may be addressed and mitigated by policies and practices that are instituted throughout the implementation, evolution, and ongoing management of the Smart Grid.

The privacy subgroup conducted a PIA for the consumer-to-utility portion of the Smart Grid during August and September 2009. In the months following the PIA, the group considered additional privacy impacts and risks throughout the entire Smart Grid structure.

The focus of the privacy subgroup has been on determining (1) the types of information that may be collected or created that can then reveal information about individuals or activities within specific premises (both residential and commercial), (2) determining how these different types of information may be exploited, and (3) recommending business policies and practices to mitigate the identified privacy risks. Entities of all types that provide, use, or obtain data from the Smart Grid can also benefit from performing PIAs to determine privacy risks and then take action to mitigate those risks.

The following questions were identified and addressed in the process of performing the consumer-to-utility PIA and in the follow-on discussion of the findings:

1. What personal information may be generated, stored, transmitted, or maintained by components and entities of the Smart Grid?
2. How is this personal information new or unique compared with personal information in other types of systems and networks?
3. How is the use of personal information within the Smart Grid new or different from the uses of the information in other types of systems and networks?
4. What are the new and unique types of privacy risks that may be created by Smart Grid components and entities?
5. What is the potential that existing laws, regulations, and standards apply to the personal information collected by, created within, and flowing through the Smart Grid components?
6. What could suggested standardized privacy practices look like for all entities using the Smart Grid so that following them could help to protect privacy and reduce associated risks?

5.4.1 Consumer-to-Utility PIA Basis and Methodology

In developing a basis for the consumer-to-utility PIA, the privacy subgroup reviewed the available documentation for use cases for the Advanced Metering Infrastructure (AMI)[38] and other published Smart Grid plans covering the interactions between the consumers of services and the providers of those services. The group also reviewed numerous data protection requirements and considered global information security and privacy protection laws, regulations, and standards to assemble the criteria against which to evaluate the consumer-to-utility aspects of Smart Grid operations. Taken into account were numerous U.S. federal data protection requirements and Fair Information Practice Principles, also often called “Privacy Principles,” that are the framework for most modern privacy laws around the world. Several

[38] *See* “AMI Systems Use Cases” at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/AugustWorkshop/All_of_the_Diagrams_in_one_document.pdf.

versions of the Fair Information Practice Principles have been developed through government studies, federal agencies, and international organizations.

For the purposes of this PIA, the group used the American Institute of Certified Public Accounts (AICPA) Generally Accepted Privacy Principles (GAPPs),[39] the Organisation for Economic Cooperation and Development (OECD) Privacy Principles, and information security management principles from the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) *International Standard ISO/IEC 27001*[40] as its primary evaluation criteria:

- The ten AICPA principles are entitled Management, Notice, Choice and Consent, Collection, Use and Retention, Access, Disclosure to Third Parties, Security for Privacy, Quality, and Monitoring and Enforcement.
- With respect to the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[41] the group's particular focus was on the *Annex to the Recommendation of the Council of 23rd September 1980: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*,[42] wherein paragraphs 7–14 of Part Two[43] outline the basic principles of national application, and on the "Explanatory Memorandum,"[44] wherein those principles are amplified (by paragraph number) in subsection II.B.[45] The enumerated OECD principles relate to Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Openness, and Individual Participation.
- *International Standard ISO/IEC 27001* provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS).

The general privacy principles and ISMS described here and adopted for use in the PIA are designed to be applicable across a broad range of industries and are considered internationally to be best practices but are generally not mandatory. However, most privacy experts agree that data protection laws throughout the world have been built around these principles.

5.4.2 Summary PIA Findings and Recommendations

The consumer-to-utility PIA conducted by the privacy subgroup revealed valuable insights about the general consumer-to-utility data flow and privacy concerns, and indicated that significant areas of concern remain to be addressed within each localized domain of the Smart Grid. For

[39] *See* "AICPA's Generally Accepted Privacy Principles" at http://www.compliancebuilding.com/2009/01/09/aicpas-generally-accepted-privacy-principles/.

[40] *See* http://webstore.iec.ch/preview/info_isoiec27001%7Bed1.0%7Den.pdf.

[41] *See* full OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" at http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html.

[42] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#guidelines.

[43] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2.

[44] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#memorandum.

[45] *Id*. at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#comments.

example, as Smart Grid implementations collect more granular, detailed, and potentially personal information, this information may reveal business activities, manufacturing procedures, and personal activities in a given location. It will therefore be important for utilities to consider establishing privacy practices to protect this information.

As noted in section 5.3,[46] which focuses on privacy laws and legal considerations, the PIA also revealed the lack of privacy laws or policies directly applicable to the Smart Grid. Accordingly, opportunities remain for developing processes and practices to identify and address Smart Grid privacy risks.

Organizations that collect or use Smart Grid data can use the Privacy Group's PIA findings to guide their own use of PIAs and develop appropriate systems and processes for Smart Grid data. Organizations can also use the six questions listed in subsection 3.5 (p. 16) when conducting their own PIAs and then examine their findings with the ten privacy principles listed below. The answers to these questions are essential both for efficient data management in general and for developing an approach that will address privacy impacts in alignment with all other organizational policies regarding consumer data. Where an organization has defined privacy responsibilities, policies, and procedures, that organization should consider reviewing its responsibilities and updating or potentially augmenting its policies and procedures to address the new privacy issues associated with the Smart Grid. Each entity within the Smart Grid can follow a similar methodology to perform its own PIAs to ensure privacy is appropriately addressed for its Smart Grid activities.

The following points summarize the PIA findings and recommendations as presented in the draft *NIST Smart Grid High-Level Consumer-to-Utility Privacy Impact Assessment*[47] in relation to the privacy principles used as the basis for the PIA. Each enumerated privacy principle statement is followed by the related findings from the PIA and the suggested privacy practices that may serve to mitigate the privacy risks associated with each principle:

1. **Management and Accountability**: Organizations that access or provide data to the Smart Grid should appoint personnel to a position responsible for ensuring that documented information security and privacy policies and practices exist and are followed. Information security and personal information privacy practices should include requirements for regular training and ongoing awareness activities. Audit functions should also be present to monitor the Smart Grid data access activities.

   Findings:

   Some organizations that participate within the Smart Grid (1) do not have documented information security and privacy responsibilities and authority within the organization; (2) do not have information security and privacy training and awareness programs; and (3) do not monitor access to Smart Grid data.

[46] *See* 5.3.2, Existing Regulatory Frameworks, and 5.3.4, Applicability of Existing Data Protection Laws and Regulations to the Smart Grid.

[47] *See* full draft PIA report at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGPrivacy/NIST_High_Level_PIA_Report_-_Herold_09_09_09_w-edits.doc.

Privacy Practices Recommendations:

- **Assign privacy responsibility**. Each organization collecting or using Smart Grid data from or about consumer locations should create (or augment) a position or person with responsibility to ensure that privacy policies and practices exist and are followed. Responsibilities should include documenting, ensuring the implementation of, and managing requirements for regular training and ongoing awareness activities.
- **Establish privacy audits**. Audit functions should be modified to monitor all energy data access.
- **Establish law enforcement request policies and procedures**. Organizations accessing, storing, or processing energy data should include specific documented incident response procedures for incidents involving energy data.

2. **Notice and Purpose:** A clearly specified notice should exist and be shared in advance of the collection, use, retention, and sharing of energy data and personal information.

   Findings:

   The data obtained from systems and devices that are part of the Smart Grid and accompanying potential and actual uses for that data create the need for organizations to be more transparent and clearly provide notice documenting the types of information items collected and the purposes for collecting the data.

   Privacy Practices Recommendations:

   - **Provide notification for the personal information collected**. Any organization collecting energy data from or about consumers should establish a process to notify consumer account inhabitants and person(s) paying the bills (which may be different entities), when appropriate, of the data being collected, why it is necessary to collect the data, and the intended use, retention, and sharing of the data. This notification should include information about when and how information may or may not be shared with law enforcement officials. Individuals should be notified before the time of collection.
   - **Provide notification for new information use purposes and collection**. Organizations should update consumer notifications whenever they want to start using existing collected data for materially different purposes other than those the consumer has previously authorized. Also, organizations should notify the recipients of services whenever they want to start collecting additional data beyond that already being collected, along with providing a clear explanation for why the additional data is necessary.

3. **Choice and Consent**: The organization should describe the choices available to consumers with regard to the use of their associated energy data that could be used to reveal personal information and obtain explicit consent, if possible, or implied consent when this is not feasible, with respect to the collection, use, and disclosure of this information.

Findings:

Currently it is not apparent that utilities or other entities within the Smart Grid obtain consent to use the personal information generated and collected for purposes other than billing. As smart meters and other smart devices increase capabilities and expand sharing of the data throughout the Smart Grid, organizations should establish processes to give consumers a choice, where possible and feasible, about the types of data collected and how it is used.

Privacy Practices Recommendation:

- **Provide notification about choices**. The consumer notification should include a clearly worded description to the recipients of services notifying them of (1) any choices available to them about information being collected and obtaining explicit consent when possible; and (2) explaining when and why data items are or may be collected and used without obtaining consent, such as when certain pieces of information are needed to restore service in a timely fashion.

4. **Collection and Scope**: Only personal information that is required to fulfill the stated purpose should be collected from consumers. This information should be obtained by lawful and fair means and, where appropriate and possible, with the knowledge or consent of the data subject.

   Findings:

   In the current operation of the electric utilities, data taken from traditional meters consists of basic data usage readings required to create bills. Under the Smart Grid implementation, smart meters will be able to collect other types of data. Home power generation services will also likely increase the amount of information created and shared. Some of this additional data may constitute personal information or may be used to determine personal activities. Because of the associated privacy risks, only the minimum amount of data necessary for services, provisioning, and billing should be collected.

   Privacy Practices Recommendations:

   - **Limit the collection** of data to only that necessary for Smart Grid operations, including planning and management, improving energy use and efficiency, account management, and billing.
   - **Obtain the data** by lawful and fair means and, where appropriate and possible, with the knowledge or consent of the data subject.

5. **Use and Retention**: Information within the Smart Grid should be used or disclosed only for the purposes for which it was collected. Smart Grid data should be aggregated in such a way that personal information or activities cannot be determined, or anonymized wherever possible to limit the potential for computer matching of records. Personal information should be kept only as long as is necessary to fulfill the purposes for which it was collected.

Findings:

In the current operation of the electric utilities, data taken from traditional meters is used to create consumer bills, determine energy use trends, and allow consumers to control their energy usage both on-site and remotely. The Smart Grid will provide data that can be used in additional ways not currently possible.

Privacy Practices Recommendations:

- **Review privacy policies and procedures**. Every organization with access to Smart Grid data should review existing information security and privacy policies to determine how they may need to be modified. This review should include privacy policies already in place in other industries, such as financial and healthcare, which could provide a model for the Smart Grid.
- **Limit information retention**. Data, and subsequently created information that reveals personal information or activities from and about a specific consumer location, should be retained only for as long as necessary to fulfill the purposes that have been communicated to the energy consumers. When no longer necessary, consistent with data retention and destruction requirements, the data and information, in all forms, should be irreversibly destroyed. This becomes more important as energy data becomes more granular, more refined, and has more potential for commercial uses.

6. **Individual Access**: Organizations should provide a process to allow for individuals to request access to see their corresponding personal information and energy data, and to request the correction of real or perceived inaccuracies. Personal information individuals should also be informed about parties with whom their associated personal information and energy data has been shared.

   Findings:

   In the current operation of the electric utilities, data may be manually read from the meters. Consumers also have the capability to read the meters through physical access to the meters. Under a Smart Grid implementation, smart meter data may be stored in multiple locations to which the consumer may not have ready access.

   Privacy Practices Recommendations:

   - **Consumer access**. Any organization possessing energy data about consumers should provide a process to allow consumers access to the corresponding energy data for their utilities account.
   - **Dispute resolution**. Smart Grid entities should establish documented dispute resolution procedures for energy consumers to follow.

7. **Disclosure and Limiting Use**: Personal information should not be disclosed to any other parties except those identified in the notice and only for the purposes originally specified or with the explicit informed consent of the service recipient.

   Findings:

   As Smart Grid implementations collect more granular and detailed information, this information is capable of revealing activities and equipment usage in a given location. As

this information may reveal business activities, manufacturing procedures, and personal activities, significant privacy concerns and risks arise when the information is disclosed without the knowledge, consent, and authority of the individuals or organizations to which the information applies.

Privacy Practices Recommendation:

- **Limit information use**. Data on energy or other Smart Grid service activities should be used or disclosed only for the authorized purposes for which it was collected.
- **Disclosure**. Data should be divulged to or shared only with those parties authorized to receive it and with whom the organizations have told the recipients of services it would be shared.

8. **Security and Safeguards**: Smart Grid energy data and personal information, in all forms, should be protected from loss, theft, unauthorized access, disclosure, copying, use, or modification.

   Findings:

   Smart Grid data may be transmitted to and stored in multiple locations throughout the Smart Grid. Establishing strong security safeguards is necessary to protect energy data from loss, theft, unauthorized access, disclosure, copying, use, or modification.

   Privacy Practices Recommendations:

   - **Associate energy data with individuals only when and where required**. For example only link equipment data with a location or consumer account when needed for billing, service restoration, or other operational needs. This practice is already common in the utility industry and should be maintained and applied to all entities obtaining or using this data as the Smart Grid is further deployed.
   - **De-identify information**. Energy data and any resulting information, such as monthly charges for service, collected as a result of Smart Grid operations should be aggregated and anonymized by removing personal information elements wherever possible to ensure that energy data from specific consumer locations is limited appropriately. This may not be possible for some business activities, such as for billing.
   - **Safeguard personal information**. All organizations collecting, processing, or handling energy data and other personal information from or about consumer locations should ensure that all information collected and subsequently created about the recipients of Smart Grid services is appropriately protected in all forms from loss, theft, unauthorized access, disclosure, copying, use, or modification. While this practice is commonly in effect in the utility industry, as other entities recognize commercial uses for this information, they too should adopt appropriate requirements and controls. In addition, given the growing granularity of information from Smart Grid operations, the responsibility for these existing policies should be reviewed and updated as necessary.
   - **Do not use personal information for research purposes**. Any organization collecting energy data and other personal information from or about consumer

locations should refrain from using actual consumer data for research until it has been anonymized and/or sufficiently aggregated to assure to a reasonable degree the inability to link detailed data to individuals. Current and planned research is being conducted both inside and outside the utility industry on the Smart Grid, its effects upon demand response, and other topics. The use of actual information that can be linked to a consumer in this research increases the risk of inadvertent exposure via traditional information sharing that occurs within the research community.

9. **Accuracy and Quality**: Processes should be implemented by all businesses participating within the Smart Grid to ensure as much as possible that energy data and personal information are accurate, complete, and relevant for the purposes identified in the notice [*see* §5.4.2-2], and that it remains accurate throughout the life of the energy data and personal information while within the control of the organization.

   Findings:

   The data collected from smart meters and related equipment will potentially be stored in multiple locations throughout the Smart Grid. Smart Grid data may be automatically collected in a variety of ways. Establishing strong security safeguards will be necessary to protect the information and the information's accuracy. Since Smart Grid data may be stored in many locations, and therefore be accessed by many different individuals/entities and used for a wide variety of purposes, personal information may be inappropriately modified. Automated decisions about energy use could be detrimental for consumers (e.g., restricted power, thermostats turned to dangerous levels, and so on) if it happens that decisions about energy usage are based upon inaccurate information.

   Privacy Practices Recommendation:

   - **Keep information accurate and complete**. Any organization collecting energy data from or about consumer locations should establish policies and procedures to ensure that the Smart Grid data collected from and subsequently created about recipients of services is accurate, complete, and relevant for the identified purposes for which they were obtained, and that it remains accurate throughout the life of the Smart Grid data within the control of the organization.

10. **Openness, Monitoring, and Challenging Compliance**: Privacy policies should be made available to service recipients. These service recipients should be given the ability to review and a process by which to challenge an organization's compliance with the applicable privacy protection legal requirements, along with the associated organizational privacy policies and the organizations' actual privacy practices.[48]

    Findings:

    Currently electric utilities follow a wide variety of methods and policies for communicating to energy consumers how energy data and personal information is used. The data collected from smart meters and related Smart Grid equipment will potentially be stored in multiple locations throughout the Smart Grid, possibly within multiple states

[48] Using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, the Federal Trade Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information.

and outside the United States. This complicates the openness of organizational privacy compliance and of a consumer being able to challenge the organization's compliance with privacy policies, practices, and applicable legal requirements.

Privacy Practices Recommendations:

- **Policy challenge procedures**. Organizations collecting energy data, and all other entities throughout the Smart Grid, should establish procedures that allow Smart Grid consumers to have the opportunity and process to challenge the organization's compliance with their published privacy policies as well as their actual privacy practices.
- **Perform regular privacy impact assessments**. Any organization collecting energy data from or about consumer locations should perform periodic PIAs with the proper time frames, to be determined by the utility and the appropriate regulator, based upon the associated risks and any recent process changes and/or security incidents. The organizations should consider sending a copy of the PIA results for review by an impartial third party and making the results of the review public. This will help to promote compliance with the organization's privacy obligations and provide an accessible public record to demonstrate the organization's privacy compliance activities. Organizations should also perform a PIA on each new system, network, or Smart Grid application and consider providing a copy of the results in similar fashion to that mentioned above.
- **Establish breach notice practices**. Any organization with Smart Grid data should establish policies and procedures to identify breaches and misuse of Smart Grid data, along with expanding or establishing procedures and plans for notifying the affected individuals in a timely manner with appropriate details about the breach. This becomes particularly important with new possible transmissions of billing information between utilities and other information between utilities and other entities providing services in a Smart Grid environment (e.g., third-party service providers).

5.5 PERSONAL INFORMATION IN THE SMART GRID

As the PIA showed, energy data and personal information can reveal something either explicitly or implicitly about specific individuals, groups of individuals, or activities of those individuals. Smart Grid data such as energy usage measurements, combined with the increased frequency of usage reporting, energy generation data, and the use of appliances and devices capable of energy consumption reporting, provide new sources of personal information.

The personal information traditionally collected by utility companies can be used to identify individuals through such data as house number and/or street address, homeowner or resident's first, middle, or last name, date of birth, and last four digits of the SSN. Smart Grid data elements that reflect the timing and amount of energy used, when correlated with traditional personal information data elements, can provide insights into the life style of residential consumers and the business operations of commercial and industrial consumers.[49]

[49] The ability to determine personal activities according to energy consumption data alone was demonstrated recently in quotes from a Siemens representative in an article published in the Washington Post: "We, Siemens, have the technology to record it (energy consumption) every minute, second, microsecond, more or less live," said Martin

With a few exceptions (e.g., SSN and credit card numbers), rarely does a single piece of information or a single source permit the identification of an individual or group of individuals. However, in recent years it has been shown through multiple research studies[50] and incidents[51] that a piece of seemingly anonymous data (date of birth, gender, zip code) that on its own cannot uniquely identify an individual may reveal an individual when combined with other types of anonymous data. If different datasets that contain anonymized data have at least one type of information that is the same, the separate sets of anonymized information may have records that are easily matched and then linked to an individual. It is also possible the matches to an individual may be narrowed to the point that linking becomes an easy task.[52] (This may particularly be seen in sparsely populated geographical areas.)

Another study published in 2009 illustrates the increasing ease of aggregating data into personally identifiable information. Carnegie Mellon researchers Alessandro Acquisti and Ralph Gross assessed the predictability of SSNs by knowing the date and geographic location of an individual subject's birth and found that they could predict the first five digits for 44% of those born after 1988 on the first attempt and 61% within two attempts.[53]

Pollock of Siemens Energy, an arm of the German engineering giant, which provides metering services. "From that we can infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data." *See* "Privacy concerns challenge smart grid rollout," Reuters, June 25, 2010; http://www.reuters.com/article/idUSLDE65N2CI20100625.

[50]*See* Arvind Narayanan and Vitaly Shmatikov, Privacy and Security: Myths and Fallacies of "Personally Identifiable Information," Communications of the ACM, available at http://userweb.cs.utexas.edu/~shmat/shmat_cacm10.pdf. June 2010. This article points out multiple incidents and studies that have shown how combinations of data items that are anonymous individually can be linked to specific individuals when combined with other anonymous data items and "quasi-identifiers" or a piece of auxiliary information. "Consumption preferences" is specifically named as a type of human characteristic data that, when combined with other items, can point to individuals.

[51] In addition to the incidents discussed in the Narayanan and Shmatikov article previously referenced, another specific example to consider is that in 2006, AOL released anonymous information about search data that was re-identified linking to individuals by a NY Times reporter. This incident led to a complaint filed by the Electronic Frontier Foundation (EFF) with the Federal Trade Commission against AOL for violating the Federal Trade Commission Act. *See* Michael Barbaro & Tom Zeller, Jr., "A Face is Exposed for AOL Searcher No. 4417749," N.Y. TIMES, Aug. 9, 2006, at §A1, available at http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000.

[52] Latanya Sweeney, "k-anonymity: A Model for Protecting Privacy, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems," 10(5), 2002; pages 557-570, available at http://epic.org/privacy/reidentification/Sweeney_Article.pdf. Sweeney gathered data from the Massachusetts Group Insurance Commission (GIC), which purchases health insurance for state employees. GIC released insurer records to the researcher, but before doing so, with the support of the Governor's office, they removed names, addresses, SSNs, and other "identifying information" in order to protect the privacy of the employees. Sweeney then purchased voter rolls, which included the name, zip code, address, sex, and birth date of voters in Cambridge. Matched with the voter rolls, the GIC database showed only six people in Cambridge were born on the same day as the Governor, half of them were men, and the Governor was the only one who lived in the zip code provided by the voter rolls. Correlating information in the voter rolls with the GIC database made it possible to re-identify the Governor's records in the GIC data, including his prescriptions and diagnoses.

[53] Alessandro Acquisti and Ralph Gross, Predicting Social Security numbers from public data, July 7, 2009, at http://www.pnas.org/content/106/27/10975.full.pdf+html.

These cases show that data can sometimes be re-identified to specific individuals by comparing anonymized information to generally available information, or by combining two datasets to produce new and more sensitive data which was not originally contained in either dataset.

There are potential unintended consequences of seemingly anonymous Smart Grid data being compiled, stored, and cross-linked. One concern is that combining Smart Grid data, which may be considered anonymous, with other types of anonymous information might lead to identifying individuals or groups of individuals associated with an address. Computing technology and the use of certain algorithms makes this type of process much easier.

While current privacy and security anonymization practices tend to focus on the removal of specific personal information data items, the studies referenced in this section show that re-identification[54] and linking to an individual may still occur. This issue of data re-identification becomes potentially more significant as the amount and granularity of the data being gathered during Smart Grid operations increases with the deployment of more Smart Grid components. It then becomes important, from a privacy standpoint, for utilities and third parties participating in the Smart Grid to determine which data items will remove the ability to link to specific addresses or individuals whenever they perform their data anonymization[55] activities.

Table 5-1 identifies and describes potential data elements within the Smart Grid that could impact privacy if not properly safeguarded.

Table 5-1 Information potentially available through the Smart Grid

Data Element(s)	Description
Name	Party responsible for the account
Address	Location where service is being taken
Account Number	Unique identifier for the account
Meter reading	kWh energy consumption recorded at 15–60 (or shorter) minute intervals during the current billing cycle
Current bill	Current amount due on the account
Billing history	Past meter reads and bills, including history of late payments/failure to pay, if any
Home area network	Networked in-home electrical appliances and devices
Lifestyle	When the home is occupied and unoccupied, when occupants are awake and asleep, how much various appliances are used
Distributed resources	The presence of on-site generation and/or storage devices, operational status, net supply to or consumption from the grid, usage patterns
Meter IP	The Internet Protocol address for the meter, if applicable

[54] *Re-identification* is the process of relating unique and specific entities to seemingly anonymous data, resulting in the identification of individuals and/or groups of individuals.

[55] *Data Anonymization* is a process, manual or automated, that removes, or replaces with dummy data, information that could identify an individual or a group of individuals from a communication, data record, or database.

Service provider	Identity of the party supplying this account (relevant only in retail access markets)

5.6 IN-DEPTH LOOK AT SMART GRID PRIVACY CONCERNS

As outlined in the results of the PIA described earlier, there is a wide range of privacy concerns to address within the Smart Grid. These may impact the implementation of Smart Grid systems or their effectiveness. For example, a lack of consumer confidence in the security and privacy of their energy consumption data may result in a lack of consumer acceptance and participation, if not outright litigation.

In general, privacy concerns about the Smart Grid fall into one of two broad categories:

- Type I: Personal information not previously readily obtainable; and
- Type II: Mechanisms for obtaining (or manipulating) personal information that did not previously exist.

Examples of Type I concerns include detailed information on the appliances and equipment in use at a given location, including the use of specific medical devices and other electronic devices that indicate personal patterns and timings of legal and potentially illegal operations within the location, and finely grained time series data on power consumption at metered locations and from individual appliances.

Type II concerns include instances where personal information is available from other sources, and the Smart Grid may present a new source for that same information. For example, an individual's physical location can be tracked through their credit card and cell phone records today. Charging PEVs raises the possibility of tracking physical location through new energy consumption data.

Detailed pictures of activities within a house or building can be derived from "equipment electricity signatures"[56] and their time patterns. Such signatures and patterns can provide a basis for making assumptions about occupant activities (e.g., the number of individuals at a location and when the premise was unoccupied).

While technology to communicate directly with appliances and other energy consumption elements already exists, Smart Grid implementation may create broader incentives for their use. Appliances so equipped may deliver detailed energy consumption information to both their owners and operators—and to outside parties.

Table 5-2 outlines some of the possible areas of privacy concern and provides some analysis of the nature of the concern according to the Type I and II categories given above. While this is not an exhaustive list, it serves to help categorize the concerns noted.

[56] This is a term coined by our Privacy Group and not one that is officially used by any regulatory or standards group.

Table 5-2 Potential Privacy Concerns and Descriptions

Privacy Concern	Discussion	Categorization
Fraud	Attributing energy consumption to another location or vehicle (in the case of PEVs).	Type II: While fraud is an existing concern, the current system of reading consumer meters (either manual recording or electronically via "drive-by" remote meter reading systems) may allow less opportunity for data manipulation without collusion with the personnel collecting the data.
Determine Personal Behavior Patterns / Appliances Used	Smart meter and home automation network data may track the use of specific appliances. Access to data-use profiles that can reveal specific times and locations of electricity use in specific areas of the home can also indicate the types of activities and/or appliances used. Possible uses for this information include: Appliance manufacturers could use this information for product reliability and warranty purposes; Other entities could use this data to do targeted marketing.	Type I: The type of data made available by Smart Grid implementation may be both more granular and available on a broader scale.
Perform Real-Time Remote Surveillance	Access to live energy use data can reveal such things as if people are in a facility or residence, what they are doing, waking and sleeping patterns, where they are in the structure, and how many are in the structure.	Type II: Many methods of real-time surveillance currently exist. The availability of computerized real-time or near-real-time energy usage data would create another way in which such surveillance could be conducted.
Non-Grid Commercial Uses of Data	Personal energy consumption data storage may reveal lifestyle information that could be of value to many entities, including vendors of a wide range of products and services. Vendors may purchase attribute lists for targeted sales and marketing campaigns that may not be welcomed by those targets. Universities might purchase information to study student attributes and target a new student profile with simple application question profiling. Such profiling could extend to other types of profiling on employment selection, rental applications, and other situations that may not be welcomed by those targets.	Type II: Under the existing metering and billing systems, meter data is not sufficiently granular in most cases to reveal any detail about activities. However, smart meters, time of use and demand rates, and direct load control of equipment may create detailed data that could be sold and used for energy management analyses and peer comparisons. While this information has beneficial value to third parties, consumer education about protecting that data has considerable positive outcomes.

5.6.1 Data Collection and Availability

A detailed sense of activities within a house or building can be derived from equipment electricity signatures, individual appliance usage data, time patterns of usage, and other data, as illustrated at the beginning of this chapter (subsection 5.3.6, Figure 5-1). Especially when collected and analyzed over a period of time, this information can provide a basis for potentially determining about occupant activities and lifestyle. For example, a forecast may be made about the number of individuals at a premise, when the location is unoccupied, sleep schedules, work schedules, and other personal routines.[57]

While technology that communicates directly with appliances and other energy consumption elements already exists, Smart Grid implementation may create broader incentives for its use and provide easier access by interested parties. Appliances so equipped may deliver granular energy consumption data to both their owners and operators, as well as to outside parties. The increased collection of and access to granular energy usage data will create new uses for that data: for example, residential demand-response systems,[58] marketing,[59] and law enforcement.[60] Many of these new uses will be innovative and provide individual and consumer benefits, some will impact privacy, and many will do both.

The listing of "Potential Privacy Concerns and Descriptions" shown earlier (Table 5-2), outlines some of the likely uses of Smart Grid data and maps them to privacy concerns that arise from new uses. The table also lists a variety of parties that are likely to use Smart Grid data. Many of these uses are legitimate and beneficial. However, all parties that collect and use Smart Grid data should be aware of uses that impact privacy and should develop appropriate plans for data stewardship, security, and data use. Any party could intentionally or unintentionally be the source of data that is misused or that is used in a way that has negative effects on consumer privacy. "Intentional" privacy compromises might occur through voluntary disclosure of data to third parties who then share the data with others or use the data in unexpected ways, while "unintentional" impacts might arise through data breaches or criminal attacks. It is important that all Smart Grid entities handling personal information to be aware of the various possible uses of

[57] *See* Mikhail Lisovich, Deirdre Mulligan, & Stephen Wicker, *Inferring Personal Information from Demand-Response Systems*, IEEE Security & Privacy, Jan.-Feb. 2010, at pages 11-20 (presenting the results of an initial study in the types of information than can be inferred from granular energy consumption data).

[58] Federal Energy Regulatory Commission, *Assessment of Demand Response & Advanced Metering 2008, Staff Report*, Dec. 2008, available at http://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf (discussing various types of demand-response systems and pricing schemes, including those for residential *customers).*

[59] Martin LaMonica, *Microsoft Dials Hohm to Cut Home Energy Use*, CNET, June 23, 2009, *available at* http://news.cnet.com/8301-11128_3-10269832-54.html (describing Microsoft's business model for monetizing its energy consumption web application as selling contextual ads to generate revenue in the beginning, but eventually "Microsoft anticipates that it can become a sort of information broker between customers and utilities looking for ways to improve the efficiency of their customers").

[60] Law enforcement already uses energy consumption data to try to identify potentially criminal activity, like drug cultivation. *See e.g.*, Jo Moreland, *Drug Raid Has Carlsbad Family Seeing Red*, N. County Times, Mar. 25, 2004, available at http://www.nctimes.com/news/local/article_ea2047e8-59e1-551e-b173-ce89ffad4d90.html. More granular data will provide them with more valuable information that may be able to identify a wider range of illegal activities.

the data, and that they consider these factors when developing processes for data collection, handling, and disclosure.

Many potential uses arise from the generation of granular energy data, especially when it is combined with personal information. Table 5-3 broadly illustrates the various industries that may be interested in Smart Grid data. While this is not an exhaustive listing, it serves to help categorize the various concerns.

Table 5-3 Potential Privacy Impacts that Arise from the Collection and Use of Smart Grid Data

Type of Data	Privacy-Related Information Potentially Revealed by this Type of Data	Parties Potentially Collecting or Using this Type of Data	Type of Potential Use[61]	Specific Potential Uses of this Type of Data
Captures detailed energy usage at a location, whether in real-time or on a delayed basis.	*Personal Behavior Patterns and Activities Inside the Home* Behavioral patterns, habits, and activities taking place inside the home by monitoring electricity usage patterns and appliance use, including activities like sleeping, eating, showering, and watching TV. Patterns over time to determine number of people in the household, work schedule, sleeping habits, vacation, health, affluence, or other lifestyle details and habits. When specific appliances are being used in a home, or when industrial equipment is in use, via granular energy data and appliance energy consumption profiles. *Real-Time Surveillance Information* Via real-time energy use data, determine if anyone is home, what they are doing, and where they are located in the home.	Utilities	Primary	Load monitoring and forecasting; demand response; efficiency analysis and monitoring, billing.
		Edge Services[62]		Efficiency analysis and monitoring; demand-response, public or limited disclosure to promote conservation, energy awareness, etc. (e.g., posting energy usage to social media).
		Insurance Companies	Secondary	Determine premiums (e.g., specific behavior patterns, like erratic sleep, that could indicate health problems).
		Marketers		Profile for targeted advertisements.
		Law Enforcement		Identify suspicious or illegal activity; investigations; real-time surveillance to determine if residents are present and current activities inside the home.
		Civil Litigation		Determine when someone was home or the number of people present.
		Landlord/Lessor		Use tenants' energy profiles to verify lease compliance.
		Private Investigators		Investigations; monitoring for specific events.
		The Press		Public interest in the activities of famous individuals.[63]

[61] "Primary" uses of Smart Grid data are those used to provide direct services to customers that are directly based on that data, including energy generation services or load monitoring services. "Secondary" uses of data are uses that apply Smart Grid data to other business purposes, such as insurance adjustment or marketing, or to nonbusiness purposes, such as government investigations or civil litigation. "Illicit" uses of data are uses that are never authorized and are often criminal.

[62] Edge services include businesses providing services based directly upon electrical usage but not providing services related to the actual generation, transportation, or distribution of electricity. Some examples of edge services would include Google PowerMeter, Microsoft Hohm, or consulting services based upon electricity usage.

Type of Data	Privacy-Related Information Potentially Revealed by this Type of Data	Parties Potentially Collecting or Using this Type of Data	Type of Potential Use[61]	Specific Potential Uses of this Type of Data
		Creditors		Determine behavior that seems to indicate creditworthiness or changes in credit risk.[64]
		Criminals and Other Unauthorized Users	Illicit	Identify the best times for a burglary; determine if residents are present; identify assets that might be present; commit fraud; identity theft; disrupt service; corporate espionage—determine confidential processes or proprietary data.
Identifies location / recharge information for PEVs or other location-aware appliances.	*Determine Location Information* Historical PEV data, which can be used to determine range of use since last recharge. Location of active PEV charging activities, which can be used to determine the location of driver.	Utilities	Primary	Bill energy consumption to owner of the PEV; distributed energy resource management; emergency response.
		Insurance Companies	Secondary	Determine premiums based on driving habits and recharge location.
		Marketers		Profile and market based on driving habits and PEV condition.
		Private Investigators Law Enforcement/ Agencies		Investigations; locating or creating tracking histories for persons of interest.
		Civil Litigation		Determine when someone was home or at a different location.
		PEV Lessor		Verify a lessee's compliance regarding the mileage of a lease agreement.
Identifies individual meters or consumer-owned equipment and	*Identify Household Appliances* Identifying information (such as a MAC address); directly reported usage information provided by	Utilities	Primary	Load monitoring and forecasting; efficiency analysis and monitoring; reliability; demand response; distributed energy resource management; emergency response.

[63] For example, there were numerous news stories about the amount of electricity used by Al Gore's Tennessee home. *See* e.g., "Gore's High Energy-Use Home Target of Critical Report," Fox News, Feb. 28, 2007, available at http://www.foxnews.com/story/0,2933,254908,00.html.

[64] Sudden changes in when residents are home could indicate the loss of a job. Erratic sleep patterns could indicate possible stress and increased likelihood of job loss. *See e.g.*, Charles Duhigg, "What Does Your Credit-Card Company Know About You?" NY Times Mag., May 17, 2009 MM40, available at http://www.nytimes.com/2009/05/17/magazine/17credit-t.html.

Type of Data	Privacy-Related Information Potentially Revealed by this Type of Data	Parties Potentially Collecting or Using this Type of Data	Type of Potential Use[61]	Specific Potential Uses of this Type of Data
capabilities.	"Smart" appliances. Data revealed from compromised smart meter, HAN, or other appliance.	Edge Services		Efficiency analysis and monitoring; broadcasting appliance use to social media.
		Insurance Companies	Secondary	Make claim adjustments (e.g., determine if claimant actually owned appliances that were claimed to have been destroyed by house fire); determine or modify premiums based upon the presence of appliances that might indicate increased risk; identify activities that might change risk profiles.
		Marketers		Profile for targeted advertisements based upon owned and unowned appliances or activities indicated by appliance use.
		Law Enforcement		Substantiate energy usage that may indicate illegal activity; identify activities on premises.
		Civil Litigation		Identify property; identify activities on premises.
		Criminals & Other Unauthorized Users	Illicit	Identify what assets may be present to target for theft; disrupt operation of appliances or electric service; introduce a virus or other attack to collect personal information or disrupt service; compromise smart meters to steal energy.[65]

Such data might be used in ways that raise privacy concerns. For example, granular Smart Grid data may allow numerous assumptions about the health of a dwelling's resident in which some insurance companies, employers, newspapers (when regarding public figures), civil litigants, and others could be interested. Most directly, specific medical devices may be uniquely identified through serial numbers or MAC addresses, or may have unique electrical signatures; either could indicate that the resident suffers from a particular disease or condition that requires the device.[66]

[65] See Matthew Carpenter et al., "Advanced Metering Infrastructure Attack Methodology" pages 55-56 (Jan. 5, 2009), available at http://inguardians.com/pubs/AMI_Attack_Methodology.pdf (discussing how attackers could manipulate the data reported to utilities); Robert Lemos, "Hacking the Smart Grid", Tech. Rev. (Apr. 5, 2010), available at http://www.technologyreview.com/printer_friendly_article.aspx?id=24977&channel=energy&section=.

[66] Susan Lyon & John Roche, Smart Grid News, "Smart Grid Privacy Tips Part 2: Anticipate the Unanticipated" (Feb. 9, 2010), available at

More generally, inferences might be used to determine health patterns and risk. For example, the amount of time the computer or television is on could be compared to the amount of time the treadmill is used.[67] Electricity use could also reveal how much the resident sleeps and whether he gets up in the middle of the night.[68] Similarly, appliance usage data could indicate how often meals are cooked with the microwave, the stove, or not cooked at all, as well as implying the frequency of meals.[69] Many of the parties listed in the "Potential Privacy Impacts" table (Table 5-3) will not be interested in the health of the resident and will wish to use the data for purposes such as efficiency monitoring, but some parties may be interested in the behavioral assumptions Smart Grid entities could make with Smart Grid data.

5.6.2 Wireless Access to Smart Grid Meters and Secondary Devices

Future designs for some smart meters and many secondary devices (e.g., appliances and smaller devices) may incorporate wireless-enabled technology to collect and transmit energy usage information for homes or businesses.[70] Should designers and manufacturers of smart meters or secondary devices decide to incorporate wireless technology for the purpose of communicating energy usage information, then that data must be securely transmitted and have privacy protection.[71] If in the future wireless technology is used to transmit aggregate home or business energy consumption information for a unique location or dwelling, then that usage data, prior to sufficient aggregation to protect privacy, should also be protected from unauthorized use, modification, or theft.[72] There are well-known vulnerabilities related to wireless sensors and networks,[73] and breaches of wireless technology.[74] For example, "war driving" is a popular

---

http://www.SmartGridnews.com/artman/publish/Business_Policy_Regulation_News/Smart-Grid-Privacy-Tips-Part-2-Anticipate-the-Unanticipated-1873.html.

[67] Elias Quinn mentions an Alabama tax provision that requires obese state employees to pay for health insurance unless they work to reduce their body mass index. Elias Quinn, "Privacy and the New Energy Infrastructure," Feb. 2009 (draft) page 31, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731. He suggests that Smart Grid data could be used to see how often a treadmill was being used in the home.

[68] Ann Cavoukian, Jules Polonetsky, and Christopher Wolf, Privacy by Design, "SmartPrivacy For the Smart Grid: Embedding Privacy into the Design of Electricity Conservation," Nov. 2009, available at http://www.ipc.on.ca/images/Resources/pbd-smartpriv-Smart Grid.pdf (describing the types of information that could be gleaned from combining personal information with granular energy consumption data).

[69] Id. at page 11.

[70] NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, available at http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf at page 21.

[71] *See* Table 5-2 Potential Privacy Concerns and Descriptions.

[72] Data aggregation was addressed in the final HIPAA rule. *See* http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt. There may also be efficiencies that can be gained by the Smart Grid when aggregating data from transmission and processing that save money for utilities. (*See* http://portal.acm.org/citation.cfm?id=1269968). This may create a greater incentive to aggregate data. If this is the case, then proper aggregation to protect PII or sensitive data should be incorporated into the plan for data aggregation.

[73] *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.

technique used to locate, exploit, or attack insufficiently protected wireless systems.[75] Readily available portable computing devices are used to detect signals emanating from wireless technology.

5.6.3 Commissioning, Registration, and Enrollment for Smart Devices[76]

This subsection describes a method for implementing demand response using load control through an energy management system linked to a utility or a third-party service provider offering remote energy management. As explained in section 3.7, it is possible to protect consumer privacy by implementing demand response without a direct data connection between the energy service provider and home devices.

To create a home area network, devices must, at a minimum, scan for networks to join, request admission, and exchange device parameters. This initial process is called "commissioning" and allows devices to exchange a limited amount of information (including, but not limited to, network keys, device type, device ID, and initial path) and to receive public broadcast information. This process is initiated by the "installer" powering-on the device and following the manufacturer's instruction. Once a HAN device has completed the commissioning process, it may go through an additional process called "registration."

The registration process is a further step involving "mutual authentication" and authorizing a commissioned HAN device to exchange secure information with other registered devices and with a smart energy industrial provider. Registration creates a trust relationship between the HAN device and the smart energy industrial provider and governs the rights granted to the HAN device. This process is more complex than commissioning and requires coordination between the installer and the service provider. In some jurisdictions, commissioning and registration are combined into one process called "provisioning."

The final process is "enrollment." This process is applicable only when the consumer wants to sign up their HAN device for a specific service provider program, such as a demand-response, PEV special rate, or a prepay program. In this process, the consumer selects a service provider program and grants the service provider certain rights to communicate with or control their HAN device. A HAN device must be commissioned and registered prior to initiating the enrollment process. This process requires coordination between the consumer and the service provider. Each of these processes is discrete but may be combined by a service provider in order to provide a seamless consumer experience.

At each step in this process, the consumer, utility, and third-party provider must ensure that data flows have been identified and classified, and that privacy issues are addressed throughout, from initial commissioning up through service-provider-delivered service. Since each step in the process, including commissioning, registration, and enrollment, may contain personal

---

[74] Id.

[75] *See* Matthew Bierlein, "Policing the Wireless World: Access Liability in the Open Wi-Fi Era," Ohio State Law Journal 67 (5) page 200, available at http://moritzlaw.osu.edu/lawjournal/issues/volume67/number5/bierlein.pdf.

[76] The first four paragraphs of this subsection are taken from OpenHAN v1.95; http://www.smartgridug.net/sgsystems/openhan/Shared%20Documents/OpenHAN%202.0/UCAIug%20OpenHAN%20SRS%20-%20v1.95%20clean.doc.

information, sufficient privacy protections should be in place to minimize the potential for a privacy breach.

Privacy issues that should be addressed related to the registration of these devices with third parties include:

- Determining the types of information that is involved with these registration situations;
- Controlling the connections which transmit the data to the third-party, such as wireless transmissions from home area networks;[77] and
- Determining how the registration information is used, where it is stored, and with whom it is shared.

5.6.4 Smart Grid Data Accessibility via the Public Internet

The Smart Grid has the capability to allow users to interact with their electricity usage information in innovative ways, including via the Internet. Correspondingly, the transmission or publication of Smart Grid data via the Internet raises privacy challenges. Internet communications are generally unsecure unless those publishing the information take steps to protect the content against unauthorized interception, manipulation, or other compromises. Moreover, users do not always have complete knowledge of, or control over, how their data will be used. In essence, accessing Smart Grid data over the Internet creates risks similar to those when accessing any other type of personal information over the Internet.

For example, an energy management application provider may enable electricity consumers to monitor energy usage via cell phones, personal digital devices, and social networking pages. Online applications and portals, including social networking service providers, may not provide advance notification to these vendors or to their end users about changes to privacy settings, resulting in unintended public availability of consumer energy data[78]. Discussions of risk mitigation between public and private entities can help shape practices that avoid potential unintended exposures of consumer energy data. More research is needed to fully explore the vast privacy implications.

5.6.5 Smart Grid Data Access by Third Parties

The Smart Grid may increase the frequency and detail of electricity consumption information from private homes and businesses. The electricity consumption data that is collected, retained, and transmitted over Smart Grid systems may be of interest to third parties.[79] Third parties can include legitimate businesses with agreements with energy consumers to assist them in better managing energy consumption, but can also include criminals seeking to abuse or misuse data.

There are three privacy challenges presented by third-party access to Smart Grid information—

---

[77] The other chapters within NISTIR 7628 include recommendations for securing wireless transmissions, such as those from OpenHAN networks, to Smart Grid entities, as well as to third parties.

[78] *See* http://www.cs.virginia.edu/felt/privacy/

[79] California Public Utility Commission held hearings March 17-18, 2010, to explore the potential uses of Smart Grid data and privacy threats, available at http://www.californiaprogressreport.com/site/?q=node/7574.

11. That companies representing themselves as consumer electricity management services are what they represent themselves to be;
12. What consumers are told about how their information will be used is true;[80] and
13. Third-party access to electricity usage data is being used solely for the purpose set forth in the agreement.

An effective full suite of fair information practices protections is necessary for consumer privacy enforcement.

Authorized third parties may be interested in using data collected through the Smart Grid. The real-time data streaming capabilities of the Smart Grid may be very attractive to large appliance manufacturers, marketers interested in usage information on utility or non-utility dependent small appliances, devices, or other consumer products.[81] Unauthorized third parties will likely also be interested in misusing Smart Grid data for many reasons from theft of physical property, identity theft schemes, or surveillance of residences or businesses. Companies have relied strongly upon the "Notice and Choice" model to gain consumer consent for data collection, retention, and use. The marketing materials may promote lower energy bills through better management of energy consumption. However, the details of service agreements or "click-through" agreements of services offered solely over the Internet might contain more uses for data than energy management.[82] Simple notice is not enough to assure electricity consumer privacy protection. There are particular challenges for reliance upon notice and consent in online agreements. A survey of California consumers showed that they fundamentally misunderstand their online privacy rights.[83]

---

[80] FTC, Complaint "In the Matter of SEARS HOLDING MANAGEMENT CORPORATION" Docket No. C-4264, ("3. From on or about April 2007 through on or about January 2008, SHMC disseminated or caused to be disseminated via the Internet a software application for consumers to download and install onto their computers (the "Application"). The Application was created, developed, and managed for respondent by a third-party in connection with SHMC's "My SHC Community" market research program. 4. The Application, when installed, runs in the background at all times on consumers' computers and transmits tracked information, including nearly all of the Internet behavior that occurs on those computers, to servers maintained on behalf of respondent. Information collected and transmitted includes: web browsing, filling shopping baskets, transacting business during secure sessions, completing online application forms, checking online accounts, and, through select header information, use of web-based email and instant messaging services,") available at http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.

[81] Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 28 (2009), *available at* http://ssrn.com/abstract=1370731

[82] David Vladeck, Privacy: Where do we go from here?, Speech to the International Conference on Data Protection and Privacy Commissioners, Nov. 6, 2009, ("[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 today that consent today actually reflects a conscious choice by consumers,") available at http://ftc.gov/speeches/vladeck/091106dataprotection.pdf

[83] Joseph Turow, et al., Consumers Fundamentally Misunderstand the Online Advertising Marketplace, *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf

There are added complications for consent in online click-through applications or agreements because it will be difficult to assure solely through online means that the person requesting the third party energy management service is authorized to do so. For example, if application information for third party service seeks basic application information such as home address, utility account number, or name, this information would be found on a monthly bill, which is often discarded as trash. Verifying that the legitimate electricity consumer is the one requesting service may require additional steps by utilities independent of the third party service provider. In addition, users routinely click through notices. The Pew Internet and American Life Project found that 73% of users do not always read agreements, privacy statements or other disclaimers before downloading or installing programs. Further, online businesses routinely change terms of service and privacy policy without giving notice to consumers.

Third-party consumer energy use sharing agreements may cause consumers confusion regarding the source of data misuse or abuse should it occur.

5.7 MITIGATING PRIVACY CONCERNS WITHIN THE SMART GRID

Many of the concerns relating to the Smart Grid and privacy may be addressed by limiting the information required to that which is necessary from an operational standpoint.

Where there is an operational need for information, controls should be implemented to ensure that data is collected only where such a need exists. Organizations will benefit by developing policies to determine the consumer and premises information that should be safeguarded and how that information should be retained, distributed internally, shared with third parties, and secured against breach. As noted in other parts of this report, training employees is critical to implementing this policy. Similarly, Smart Grid services recipients should be informed as to what information the organization is collecting and how that information will be used, shared, and secured. Service recipients may also need the ability to inspect collected information for accuracy and quality, as recommended in the privacy principles described in the PIA material (subsection 5.4.2).

Existing business rules, standards, laws, and regulations previously considered relevant to other sectors of the economy might, if not directly applicable, be usable as models to provide protection against the Type II areas of concern described earlier (section 5.6, Table 5-2). However, because of the current technology used for the collection of the data, Type I concerns may need to be addressed by other means.
Many of the concerns relating to Smart Grid and privacy may be addressed by limiting the information required from an operational standpoint. For example, many existing implementations of demand response use direct load control, where the utility has a communications channel to thermostats, water heaters, and other appliances at consumer premises. . Although most direct load control today is one-way, if two-way communications are implemented, the pathway from the consumer may allow granular monitoring of energy consumption by appliance. This direct monitoring may provide more accurate load management, but could also pose certain privacy risks.

There are other methods that use demand response for distributed load control where the utility or third-party energy service provider delivers pricing and energy data to a consumer Energy Management System (EMS) through a gateway. Intelligent appliances and/or the consumer EMS use this pricing and energy information to optimize energy consumption according to consumer

preferences. With the insertion of a gateway and local intelligence, any feedback to the utility could be load control results for the entire household, rather than by appliance. To mitigate privacy concerns, these results need to be averaged over a long enough time interval to prevent pattern recognition against known load profiles, as explained in subsection 5.3.6. Thus, it is possible to protect consumer privacy at a macro level by choosing a system design that minimizes frequent access to granular data from outside the consumer site.

5.7.1 Use Case Mitigation Studies

Whereas PIAs provide an excellent means of identifying privacy risks, privacy use cases can be excellent tools for determining the specific steps to take to mitigate privacy risks in ways that are reasonable for the organization, not only for mitigating risks discovered during PIAs, but also for mitigating the generally known risks involved with common business activities that involve personal information. These generally known risks can be represented by common privacy use cases. With heavy reliance upon technology and information sharing, addressing privacy risks must be part of the business model today, and consideration of privacy impacts should be part of everyday business activities. Privacy use cases can provide the engineers and architects of systems and processes the guidance and information necessary for building privacy controls into systems and processes during their daily activities. Further discussion of this need to build privacy protections into systems and processes, along with the resulting benefits, is provided within the "Privacy By Design" methodology.[84]

When the general privacy concerns have been identified, the entities within each part of the Smart Grid can then look at their associated Smart Grid business processes and technical components to determine the privacy concerns that exist within their scope of Smart Grid use and participation. Privacy use cases may be utilized to represent generalizations of specific scenarios within the Smart Grid that require interoperability between systems and Smart Grid participants in support of business processes and workflow. Through structured and repeatable analysis, business use cases can be elaborated upon as interoperability/technical privacy use cases to be implemented by the associated entities within the Smart Grid. The resulting details will allow those responsible for creating, implementing, and managing the controls that impact privacy to do so more effectively and consistently.

5.7.2 Privacy Use Case Scenarios

The privacy subgroup spent several months creating a few different methods for expanding the existing NIST collection of use cases[85] to include consideration of privacy concerns. When considering which set of fair information practices to use for creating privacy use cases, it was decided to use the OECD Privacy Guidelines for the following reasons:

- They are long-established and widely recognized;

[84] "Privacy By Design" is a set of seven high-level concepts, created by Ontario Privacy Commissioner Ann Cavoukian, for organizations to follow to help ensure they establish and build privacy controls within their business processes. See more about the Privacy By Design concepts available at http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf.

[85] See the collection of use cases the Privacy Group considered and chose representative use cases available at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases.

- They are freely available; and
- They are straight-forward concepts that will be more easily and consistently utilized when building privacy controls into processes.

The larger set of amalgamated principles used to conduct the Smart Grid PIA were chosen because they better served the purposes of identifying where, within an identified system or process, the most comprehensive set of privacy concerns exist. Typically, PIAs are performed by a specific individual or specialized group within an organization, and the PIAs look at a broader scope within a system or process and go less in-depth than a privacy use case.

Privacy use cases are typically utilized by a broader community and are repeatedly used to examine a specific, narrow scope. By keeping the privacy use case process limited to one set of accepted privacy principles such as the OECD Privacy Guidelines, it will be simpler and more feasible for the privacy use cases to be consistently used and applied by the broader community.

Appendix B contains the description of the activities of the privacy subgroup for creating privacy use cases. The privacy subgroup drafted multiple privacy use cases. The following are included as examples:

1. Landlord with Tenants scenarios
2. A PEV General Registration and Enrollment Process scenario

While the privacy subgroup created a few privacy cases, work needs to continue to finish developing a more comprehensive set of privacy use cases for publication in a subsequent version of this document.

While producing the sample privacy use cases drafts, the privacy subgroup established many recommendations based upon the work that was completed. These include:

- Expanding the current collection of use cases to cover all Smart Grid entity types in addition to utilities (regulated or not) that will offer Smart Grid and smart device services;
- Including a broader list of individuals about whom the Smart Grid, smart meters, and smart devices will generate additional personal information; and
- Including within use cases, where appropriate and feasible to allow Smart Grid goals and processes to be met, a method for individuals to turn off/on certain smart meter and smart devices collection of personal information.

The work done so far on creating privacy use cases has only begun to document the functions that need to be implemented to ensure that privacy is protected in Smart Grid operations. The privacy subgroup recommends ongoing development of a comprehensive set of use cases for privacy.

5.8 Smart Grid Privacy Summary And Recommendations

5.8.1 Summary

Based upon the work and research done over the past year, the privacy subgroup reached the following conclusions:

1. The evolving Smart Grid technologies and associated new types of information related to individuals, groups of individuals, and premises may create privacy risks and challenges that are not fully addressed or mitigated by existing laws and regulations with regard to energy consumption, energy generation, billing, third-party Smart Grid applications data, and other related Smart Grid data.
2. New Smart Grid technologies, particularly smart meters, smart appliances, and similar types of endpoints, may create new privacy risks and concerns that may not be addressed adequately by the existing business policies and practices of utilities and third-party Smart Grid providers.
3. Utilities and third-party Smart Grid providers need to follow recognized privacy practices in a consistent and comprehensive fashion to effectively safeguard Smart Grid personal information and consumer privacy. Existing policies should be evaluated and revised, as required.

5.8.2 Recommendations

The challenge ahead is to create a Smart Grid Privacy Principles program that individuals accept. The goal is to have individuals participate in the Smart Grid, allowing the electric sector to thrive and innovation to occur. This will only happen when effective and transparent privacy practices are consistently implemented, followed, and enforced within the Smart Grid. To create this transparency and obtain the trust of Smart Grid participants—and based on the conclusions and the details of the associated findings—recommendations were made throughout this chapter for all entities that participate within the Smart Grid. A summary listing of all these recommendations includes:

1. Conduct a PIA before making the decision to deploy and/or participate in the Smart Grid to identify risks to the personal information Smart Grid entities collect, process, store, and otherwise handle, along with determining appropriate risk mitigation activities. Smart Grid entities can refer to the methodology followed by the privacy subgroup, as described within this report, as a model for how to do their own PIAs. PIAs should be performed as follows:
   - Conduct an initial PIA to identify existing privacy risks and establish a baseline privacy posture measurement.
   - Conduct subsequent PIAs when major changes occur within the organization, systems, or applications; when new laws and regulations are put into effect that provide requirements for how Smart Grid data is used; and at any other time an event occurs that impacts how the Smart Grid entity does business, such as following an information security incident involving personal information.
2. Develop and formally document privacy policies and practices that are drawn from the full set of OECD Privacy Principles and other sectors' privacy policies, regulations and laws that may be applicable. In particular the privacy subgroup recommends the following practices based on the Principles:
   - ***Management and Accountability***. An organization should formally appoint positions and/or personnel to ensure that information security and privacy policies and practices exist and are followed. Documented requirements for regular training and

ongoing awareness activities and communications should exist and be consistently followed. Audit functions should be present to monitor all data accesses and modifications.

- ***Notice and Purpose***. An organization should provide consumers with meaningful, clear, and full notice in advance of the collection, use, retention, or sharing of energy usage data and personal information. Such notice should provide a detailed description of all purposes for which consumer data will be used, including any purposes for which affiliates and third parties will use the data. The notice should also include how long the data will be maintained by the organization and which third parties the data will be shared with. Clear, full, and accurate notice prior to data collection is essential to enabling other principles.
- ***Choice and Consent***. An organization should clearly, fully, and accurately describe the choices available to individuals, and to the extent practicable, obtain explicit approval for the collection and use of their personal information. Consumers should have the option to forgo data collection and services that are not related to the core services provided by the organization.[86]
- ***Collection and Scope***. Only personal information that is required to fulfill the stated purpose specified under the Notice and Purpose principle should be collected. Treatment of the information should conform to these privacy principles.
- ***Use and Retention***. Information should be used or disclosed only for the purpose for which it was collected and should be divulged only to those parties authorized to receive it. Personal information should be aggregated or anonymized wherever possible to limit the potential for revealing private information. Personal information should be kept only as long as is necessary to fulfill the purposes for which it was collected.
- ***Individual Access***. Organizations should provide a process whereby individuals may ask to see their corresponding personal information and to correct inaccuracies. Individuals should be informed about parties with whom personal information has been shared.
- ***Disclosure and Limiting Use***. Personal information should be used only for the purposes for which it was collected. Personal information should not be disclosed to any other parties except those identified in the notice for purposes identified in the notice, or with the explicit consent of the service recipient. Unless disclosure is compelled by a subpoena, warrant, or court order, organizations should seek prior consumer approval for disclosure of consumer data to third parties.
- ***Security and Safeguards***. Personal information in all forms should be protected from loss, theft, unauthorized access, inappropriate disclosure, copying, use, or modification.

[86] For example, while they may not have a choice about collection necessary for load balancing, electricity customers should have the option to prohibit utilities from collecting information about their appliances for marketing uses.

3. Develop a comprehensive set of privacy use cases that will help utilities and third-party Smart Grid providers to rigorously track data flows and the privacy implications of collecting and using data, and help the organization to address and mitigate the associated privacy risks within common technical design and business practices.
4. Educate the public about the privacy risks within the Smart Grid and what they as consumers can do to mitigate them.
5. Share information concerning solutions to common privacy-related problems with other Smart Grid market participants.
6. Manufacturers and vendors of smart meters, smart appliances, and other types of smart devices, should collect only the energy and personal data necessary for the purposes of the smart device operations. The defaults for the collected data should be established to use and share the data only as necessary to allow the device to function as advertised.

Given these realities, findings, and recommendations, the privacy subgroup hopes that the information contained in this chapter will serve as a useful guide and reference for the wide variety of Smart Grid domain players, policymakers, and lawmakers who have, or may have in the future, have responsibility for consumer energy consumption data.

APPENDIX C
STATE LAWS – SMART GRID AND ELECTRICITY DELIVERY REGULATIONS

State	Code Topic and Links
Alabama	Title 37 Public Utilities Private Contractor providing electricity service Section 37-4-30, Electric cooperatives empowered to furnish telephone service. Section 37-6-41, Cooperatives authorized to supply electrical energy or telephone service or both. Section 37-6-45 http://www.legislature.state.al.us/CodeofAlabama/1975/coatoc.htm
Alaska	
Arizona	42-5063 Definition of Utility - Providing to retail electric customers ancillary services, electric distribution services, electric generation services, electric transmission services and other services related to providing electricity. Customer Protection against unfair and deceptive practices. It has very good consumer protection language http://law.justia.com/arizona/codes/title30/00806.html Statute 30-803 Competition in retail supply of electricity; open markets http://law.justia.com/arizona/codes/title30/00803.html
Arkansas	
California	General Provisions and Definitions http://law.justia.com/california/codes/puc/201-248.html Independent System Operator http://law.justia.com/california/codes/puc/345-352.7.html Distributed Energy Resources http://law.justia.com/california/codes/puc/353.1-353.15.html Privacy Protection of customer data http://law.justia.com/california/codes/puc/2891-2894.10.html
Colorado	Article 25 Public Utility Commission Power to regulate utilities http://law.justia.com/colorado/constitution/cnart25.html
Connecticut	Chapter 98 http://search.cga.state.ct.us/dtsearch_pub_statutes.html Sec. 7-148ee. Establishment of corporation to manufacture, distribute, purchase or sell electricity, gas or water. Chapter 101 http://search.cga.state.ct.us/dtsearch_pub_statutes.html Municipal Gas and Electric Plant All regulatory measures under Chapter 101 http://search.cga.state.ct.us/dtsearch_pub_statutes.html
Delaware	Title 26 Public Utilities http://delcode.delaware.gov/title26/index.shtml#TopOfPage
District of Columbia	Title 34
Florida	Title 27 Regulated Utilities

State	Code Topic and Links
	http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=Ch0350/titl0350.htm&StatuteYear=2009&Title=-%3E2009-%3EChapter%20350 Chapter 366 http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=Ch0366/titl0366.htm&StatuteYear=2009&Title=-%3E2009-%3EChapter%20366
Georgia	Article 2, 6 http://www.lexis-nexis.com/hottopics/gacode/default.asp
Hawaii	http://www.capitol.hawaii.gov/site1/hrs/searchhrs.asp?query=public+utility&currpage=1 §269-16 Regulation of utility rates; ratemaking procedures. http://www.capitol.hawaii.gov/hrscurrent/Vol05_Ch0261-0319/HRS0269/HRS_0269-0016.htm
Idaho	Title 61 http://www.legislature.idaho.gov/idstat/Title61/T61.htm
Illinois	Chapter 220 http://www.ilga.gov/legislation/ilcs/ilcs2.asp?ChapterID=23
Indiana	Title 8 http://www.in.gov/legislative/ic/code/title8/
Iowa	
Kansas	Chapter 66-101 http://www.kslegislature.org/legsrv-statutes/statutesList.do 66-1901-66-1903 http://www.kslegislature.org/legsrv-statutes/statutesList.do
Kentucky	Title 24 Public Utilities Generally http://www.lrc.ky.gov/KRS/278-00/CHAPTER.HTM
Louisiana	Louisiana Public Utilities Definition http://www.legis.state.la.us/lss/lss.asp?doc=99873 http://www.legis.state.la.us/lss/lss.asp?doc=99891, http://www.legis.state.la.us/lss/lss.asp?doc=99803, http://www.legis.state.la.us/lss/lss.asp?doc=104770
Maine	Public Utilities http://www.mainelegislature.org/legis/statutes/35/title35ch0sec0.html
Maryland	Statute 1-101 Definitions http://mlis.state.md.us/asp/statutes_Respond2.asp?article=gpu&section=1-101 § 6-109. Duty of owner, lessee, or user of equipment. § 7-306. Net energy metering. § 7-509. Electric company's authority to regulate. Title 6. High voltage lines Title 7. Gas, electric, and water companies
Massachusetts	
Michigan	Chapter 460 http://www.legislature.mi.gov/%28S%28dlr2op45qzqa4jeojatzee55%29%29/mileg.aspx?page=GetObject&objectname=mcl-chap460
Minnesota	Chapter 216-217 https://www.revisor.mn.gov/revisor/pages/statute/statute_chapter.php?year=2006&start=216&close=217&history=&border=0 Chapter 453 Municipal Electric Power

State	Code Topic and Links
	https://www.revisor.mn.gov/revisor/pages/statute/statute_chapter.php?year=2006&start=216&close=217&history=&border=0 Chapter 455 Electric Light and Power Plants https://www.revisor.mn.gov/revisor/pages/statute/statute_chapter_toc.php?year=2006&chapter=455&history=&border=0
Mississippi	
Missouri	
Montana	Title 69 Public Utilities and Carriers https://www.revisor.mn.gov/revisor/pages/statute/statute_chapter_toc.php?year=2006&chapter=455&history=&border=0 Title 69 Chapter 3 Regulation of Public Utilities http://data.opi.state.mt.us/bills/mca_toc/69_3.htm
Nebraska	
Nevada	Title 58 Chapter 701 http://www.leg.state.nv.us/NRS/NRS-701.html Renewable Energy Program http://www.leg.state.nv.us/NRS/NRS-701B.html Chapter 703 Public Utility Commission http://www.leg.state.nv.us/NRS/NRS-703.html Regulation of Public Utilities http://www.leg.state.nv.us/NRS/NRS-704.html Utilities Owned by Local Government http://www.leg.state.nv.us/NRS/NRS-710.html
New Hampshire	Statutes http://www.gencourt.state.nh.us/rsa/html/indexes/indexresults.asp Definitions http://www.gencourt.state.nh.us/rsa/html/xxxiv/374-a/374-a-1.htm Private Generation and Sell of Electricity http://www.gencourt.state.nh.us/rsa/html/xxxiv/362-a/362-a-2-a.htm Customer Defined http://www.gencourt.state.nh.us/rsa/html/xxxiv/378/378-7-c.htm Public Utility Defined http://www.gencourt.state.nh.us/rsa/html/xxxiv/362/362-2.htm
New Jersey	
New Mexico	
New York	Electric Utility Cooperatives and Corporations http://public.leginfo.state.ny.us/menugetf.cgi?COMMONQUERY=LAWS Title 2 Article 5 Public Utility Commission http://public.leginfo.state.ny.us/menugetf.cgi?COMMONQUERY=LAWS
North Carolina	
North Dakota	Title 49 Public Utilities http://www.legis.nd.gov/cencode/t49.html
Ohio	Chapter 743 Utilities – Electric; Gas; Water http://codes.ohio.gov/orc/743
Oklahoma	
Oregon	Title 57 Utility Regulation http://www.leg.state.or.us/ors/756.html
Pennsylvania	Title 66
Rhode Island	Title 39 Public Utilities and Carriers http://www.rilin.state.ri.us/Statutes/TITLE39/INDEX.HTM

State	Code Topic and Links
South Carolina	Article 3 Electric Systems http://www.scstatehouse.gov/coderegs/c103.htm
South Dakota	Title 49 Public Utilities and Carriers http://legis.state.sd.us/statutes/DisplayStatute.aspx?Type=Statute&Statute=49
Tennessee	Title 65 Chapter 4 Public Utility Commission Authority http://michie.lexisnexis.com/tennessee/lpext.dll/tncode/270f1/272b2?fn=document-frame.htm&f=templates&2.0# Chapter 34 Territories of Electric Utility Systems http://michie.lexisnexis.com/tennessee/lpext.dll/tncode/270f1/27d62?f=templates&fn=document-frame.htm&2.0#JD_t65ch34 Chapter 23 State Rural Electrification Authority http://michie.lexisnexis.com/tennessee/lpext.dll/tncode/270f1/27985?f=templates&fn=document-frame.htm&2.0#JD_t65ch23
Texas	Utilities Code Title 2 Public Utility Regulatory Act Subtitle Electric Utilities Chapter 31 General Provisions http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.31.htm Chapter 38 Regulation http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.38.htm Chapter 39 Restructuring http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.39.htm Chapter 40 Publicly Owned http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.40.htm Chapter 41 Cooperatives http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.41.htm Chapter 43 Access to Broadband http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.43.htm
Utah	Title 54 Public Utilities http://le.utah.gov/~code/TITLE54/TITLE54.htm
Vermont	
Virginia	Title 56 Section 580 Transmission and distribution of electricity http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+56-580 Definitions http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+56-265.1
Washington	Title 54 http://apps.leg.wa.gov/rcw/default.aspx?Cite=54 Electric Power http://apps.leg.wa.gov/rcw/default.aspx?cite=54.44
West Virginia	
Wisconsin	Chapter 196 Regulation of Public Utilities http://nxt.legis.state.wi.us/nxt/gateway.dll?f=templates&fn=default.htm&d=index&jd=top Utility service for persons who are victims of Identity Theft http://www.legis.state.wi.us/statutes/Stat0196.pdf
Wyoming	Title 37 Public Utilities

APPENDIX D
PRIVACY USES CASES

The privacy subgroup—

- Reviewed a large number of existing Smart Grid use cases[87];
- Identified the privacy gaps within and among those use cases;
- Developed augmented use cases for privacy, using the traditional format used by the CSWG[88], the OECD privacy principles, and Version 2.0 of the International Security, Trust & Privacy Alliance (ISTPA) Privacy Management Reference Model;[89] and
- Summarized the key findings and observations from the collection of all the privacy use cases created.

D.1 USE CASE INVENTORY, CONSOLIDATION AND GAP ANALYSIS

The privacy subgroup developed a consolidated matrix[90]of the existing uses cases, by like topic, then looked for use cases that could represent common Smart Grid scenarios involving personal information.

The use cases were selected from several existing sources, including but not limited to IntelliGrid, Electric Power Research Institute (EPRI), and Southern California Edison (SCE). Review of this collection of use cases revealed the following:

- The existing use cases relate to utilities but not to the third parties that will also be part of the Smart Grid.
- It is not clear that the current use cases include non-regulated (e.g., third parties) Smart Grid entities or services that do not operate through the smart meter. All of the use cases reviewed require registration with a regulated Smart Grid entity and operation through the smart meter. More use cases are needed to make the available set comprehensive.
- The use cases represent situations where data is captured from not only utilities, but also from smart devices, such as a HAN or a PEV using a different plug.
- All of the use cases—
  - Referred to an individual customer, even though the information collected could be from an individual, a dwelling with multiple individuals, or business other than the

[87] See the collection of use cases that the Privacy Group considered and chose representative use cases available at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases.

[88] See Appendix A in Draft 2 of NISTIR 7628, available at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTIR7628Feb2010/DRAFT2_NISTIR_7628_Jan-31-2010_clean.pdf, to see how the security groups involved in this research formatted their use cases.

[89] Developed by the International Security, Trust & Privacy Alliance (ISTPA) in 2009;

[90] See the collection of use cases that the Privacy Group considered and chose representative use cases available at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/UseCases.

customer paying the Smart Grid entity bill. However, information within the Smart Grid could be personal information about a tenant, a household member, a visitor, a patient, an employee that the customer may not have the authority to grant permission to collect, and so on.

- Referred to a customer and the Smart Grid entity, even though the information collected could be from multiple individuals and could go to many entities outside of the utility.

- Reviewed assumed that if the service goes "through" the Smart Grid it has to involve the utility. There is no pass-through capability that allows an individual or business entity to enter into an agreement with a third-party using Smart Grid personal information and additional personal information generated by the smart device that travels over the grid channels.

- Assume that the Smart Grid entity can know what electronic devices are on/off/running at a premise and do not address a privacy option that could be turned on/off at some level by the individual at the premise.

- None of the use cases reviewed—

  - Made mention of a privacy policy being disseminated and being agreed to by customers.

  - Specified privacy functionality.

  - Depicted a non-regulated entity (e.g., third parties) offering a service directly to an individual or business via a smart meter.

  - Specified smart devices that communicated outside of the Smart Grid, directly with the Internet or otherwise.

D.2 INCORPORATING PRIVACY INTO EXISTING SMART GRID USE CASES

Based upon the findings the privacy subgroup recommends the following guidelines for improving upon use cases to address privacy issues—

- Add on to the existing use cases by including privacy functionality to the scenarios.
- Include information within the use cases for the existence of such things as privacy policies, training, and so on as indicated within the PIA recommendations.
- Include within the use case scenarios (1) a relationship with the utility, (2) a joint relationship with the Smart Grid utility and non-regulated entity, and (3) a relationship solely with a non-regulated entity.
- Create use cases that—
  - Include third parties that will be part of the Smart Grid.

- Include privacy options where individuals within service locations can turn on and off the ability for utilities to detect electronic devices that are using energy.
- Depict a non-regulated entity offering a service directly to an individual or business via the smart meter.
- Depict scenarios that involve smart devices and other entities within the Smart Grid communicating directly with the Internet and other non-Smart Grid entities.
- Depict groups of individuals as being the customer, or individuals at service locations who are not the entities that pay for the services. (e.g., renters that pay utilities to the landlord, not the utility)
- Include the Smart Grid entity making an agreement with a third-party and the third-party making the agreement with the individual or business entity, much like the iPhone model. In this model, the individual or business entity may or may not be the customer, but may be the owner of a smart device that communicates with the smart meter.

D.3 PRIVACY USE CASE EXAMPLES

This appendix contains the details for two example privacy use cases that were identified as examples to map to the OECD Privacy Guidelines privacy protection and fair information practices model. Each of the applicable principles is noted in the steps provided with each use case.

For reference while reviewing these privacy use cases, here is a summary of the OECD Privacy Guidelines:

1. **Collection Limitation Principle**: 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.
2. **Data Quality Principle**: 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, compete and kept up-to-date.
3. **Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 except—
    - with the consent of the data subject; or
    - by the authority of law.
5. **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. **Openness Principle**: 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, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle**: An individual should have the right—
   a. To obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b. To have communicated to him, data relating to him
      i. within a reasonable time;
      ii. at a charge, if any, that is not excessive;
      iii. in a reasonable manner; and
      iv. in a form that is readily intelligible to him;
   c. To be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and
   d. To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8. **Accountability Principle**: A data controller should be accountable for complying with measures that give effect to the principles stated above.

D.4 PRIVACY USE CASE #1: LANDLORD WITH TENANTS

"Utility Use Case Landlord/Tenant enrolls in/uses/is billed by a Smart Meter Program. In this use case, the tenant has a PEV.

D.4.1 Use Case Assumptions

- The Landlord has an account with the utility for the smart meter. The Landlord pays for all electrical service at the Tenants' premises except for the PEV.
- Each Tenant associated with a Smart Meter has the right to prevent the Landlord from obtaining detailed energy usage that would depict the presence of electrical devices in the unit as this would be an invasion of privacy.
- PEV Tenant has an account with utility and electrical service at a premise served by the utility.
- PEV and utility have communications capabilities, enabled by utility provided Energy Services Communication Interface (ESCI).
- The Tenant awareness of the utility and vehicle programs is prompted by both the utility providers and the vehicle manufacturers.
  - The utility offers PEV programs and services for its customers and will provide the necessary support processes for enrollment, communications, and billing

  - The Vehicle manufacturer would provide information to the customer about fuel and/or emission gains of the vehicles offered and promote the utility and convenience of connecting to the grid

- Utility maintains information on all Landlord's Smart Meters and Tenant's PEVs enrolled in the PEV programs, including demand side management programs, associated PEV IDs, Landlord IDs, and premise IDs. The Landlord is permitted detail reports, only if the Tenant allows such, even though the Landlord is paying for the electricity.
- For the purposes of this use case all of the 'DEFINE' Privacy Reference Model operational requirements have been established such that the Landlord and the Tenant have only to 'SELECT' their choices.

D.4.2 Step-by-Step Breakdown

Scenario: Landlord enrolls in the Smart Meter program. Tenants provide (or not) permission for Landlord to see detailed Smart Meter Reports and the Utilities Company turns on the service

This scenario describes the enrollment and initial usage of the Smart Meter Program.

Step 0.5 - The Landlord awareness of the utility and Smart Meter programs is prompted by both the utility providers and the Smart Meter manufacturers.

Step 1 - Landlord initiates request to enroll Smart Meter(s) in a Smart Meter Program by contacting Utility and provides Landlord, Tenant and Smart Meter information (i.e. Landlord Account information, Tenant associated with Smart Meter, SM ID, etc.). [Note: Landlord uses phone, Internet, or other communications channel.]
OECD Data Quality Principle: Collection of Personal data by the Landlord should be relevant to the purposes for which it will be used as stated by the Smart Meter provider.

Step 2 - Utility authenticates Landlord, Landlord account, and Premise information, and. collects Smart Meter information including SM ID and associated Tenant information
OECD Security Safeguards Principle: Utility must ensure proper authentication procedures are followed prior to creating a new account.

Step 3 - Utility presents Landlord with Smart Meter Program information and Smart Meter Program selections.
OECD Purposes Specification Principle: The collection of personal data should be specified by the Landlord to any Tenant and the subsequent use of the data limited to the fulfillment of those purposes
OECD Openness Principle: Utility makes available information collection and use policies to Landlord.

Step 4 - Landlord selects Smart Meter Program and Service Plan, sets Smart Meter program parameters. The Landlord and Smart Meter are now enrolled in a utility Smart Meter program.

Step 4.1 - Tenant initiates request to set up Smart Meter(s) preferences by contacting Utility and provides Landlord, Tenant and Smart Meter information (i.e. Landlord Account information, Tenant associated with Smart Meter, SM ID, etc.). [Note: Tenant uses phone, Internet, or other communications channel.]
OECD Openness Principle: Utility and Landlord make available information collection and use policies to tenant.

Step 4.2 - Utility authenticates Tenant, Landlord account, and Premise information, and collects Smart Meter information including SM ID and associated Tenant information.
OECD Security Safeguards Principle: Utility must ensure proper authentication procedures are followed by Landlord and Tenant prior to collection of Smart Meter information.

Step 4.3 - Utility presents Tenant with Smart Meter Program information and Smart Meter Program selections.
OECD Purpose Specification Principle: Tenant should be informed of the purposes for which personal data are collected should be specified not later than at the time of collection and the use limited to the fulfillment of those purposes.
OECD Use Limitation Principle: Tenant personal data should not be disclosed, made available, or otherwise used for purposes other than those specified by the Tenant.

Step 4.4 - Tenant selects Smart Meter Program and Service Plan, sets Smart Meter program parameters. The Landlord, Tenant and Smart Meter are now enrolled in a utility Smart Meter program.
OECD Individual Participation Principle: Utility must ensure proper procedures are followed for collection of Smart Meter information.

Step 5 - Tenant uses electrical services at their premise location.

Step 6 - Smart Meter and Energy Services Communications Interface (ESCI) initiate a secure communications session.
OECD Security Safeguards Principle: Utility must ensure communications channel over which information will flow is appropriately secured.

Step 7 - Smart Meter ID is transmitted to ESCI.
OECD Security Safeguards Principle: Utility must ensure communications channel over which information will flow is appropriately secured.

Step 8 - ESCI maintains communication session and security between Smart Meter and Utility. ESCI transmits request for validating Smart Meter ID to Utility, includes Premise ID.
OECD Security Safeguards Principle: Same as Step 6, plus ensuring smart meter ID matches account created.

Step 9 - Utility identifies and authenticates Smart Meter ID and Premise ID.
OECD Security Safeguards Principle: Utility ensures receiving IDs are correct before beginning session.

Step 10 - Utility transmits confirmation message via ESCI to Smart Meter indicating successful binding with premise ESCI. Confirmation message includes authentication parameters for Smart Meter. [Note: Authentication parameters would include utility rate program information.]
OECD Security Safeguards Principle: Utility ensures data is safeguarded

Step 11 - Smart Meter receives confirmation message and sets authentication parameters.
OECD Security Safeguards Principle: Utility ensures data is safeguarded and only authorized access to the data is allowed

Step 12 - Smart Meter transmits via ESCI message to Utility acknowledgement of receipt of valid confirmation message and setting of authentication parameters
OECD Security Safeguards Principle: Utility ensures data is safeguarded and provides security and authentication for access to the data

Step 13 - Utility transmits message via ESCI to discover EUMD at Tenant Premise; message includes authentication parameters for EUMD. [Note: Authentication parameters would include utility rate program information (e.g. interval size, etc.).]
OECD Security Safeguards Principle: Utility ensures data is safeguarded, data is correct and sent to valid Customer (Tenant)

Step 14 - EUMD receives discovery message and sets authentication parameters.
OECD Security Safeguards Principle: Utility ensures data is safeguarded and data security procedures are followed

Step 15 - EUMD transmits via ESCI message to Utility acknowledgement of receipt of valid discovery message and setting of authentication parameters
OECD Security Safeguards Principle: Utility ensures data is safeguarded and data security procedures are followed

Step 16 - ESCI transmits confirmation message to PEV indicating successful communication session binding of PEV to Utility, meaning that charging can proceed according to enrolled PEV program. [Note: Authentication between Utility and Smart Meter is now complete and the Smart Meter processing can proceed according to the enrolled Smart Meter program criteria]
OECD Security Safeguards Principle: Utility ensures data is safeguarded and data security procedures are followed

Step 17 - Smart Meter prepares for collection of electrical usage based on Landlord-selected preferences, Tenant-selected preferences and enrolled Smart Meter program.
OECD Data Quality Principle: Utility ensures that meter collects only personal data relevant to the purposes for which the data is to be used and be accurate, compete and kept up-to-date.
OECD Purpose Specification Principle: Utility follows Tenant preferences regarding personal data collection and the subsequent limited use

OECD Use Limitation Principle: Utility maintains process so that personal data is not disclosed, made available or otherwise used for purposes other than those specified by the Tenant

Step 18 - Utility prepares for report of electrical usage based on Landlord-selected preferences, Tenant-selected preferences and enrolled Smart Meter program.
OECD Individual Participation Principle: Data and usage collection reports should be made available to Tenant according to their preferences
OECD Accountability Principle: Utility is held accountable for complying with data security and access requirements

D.5 PRIVACY USE CASE #2: PEV GENERAL REGISTRATION AND ENROLLMENT PROCESS

Customers are interested in fueling vehicles with electricity. Electric vehicles (EV), plug-in vehicles (PEV) and plug-in hybrid vehicles (PHEV) are emerging transportation options for consumers. Electric utilities desire to support these emerging loads with electricity at “off peak” times when energy costs are low and generation and power delivery assets are underutilized. PEV manufacturers are interested in working with utilities to develop customer rates/programs which could provide consumers with an increased incentive to purchase a PEV. To enable utility customer rates/programs specifically to customers with PEVs, the utility must offer special services for these customers. These services include the ability to enroll, register, and initially setup communications between a PEV and the utility (one-time setup), the ability to repeatedly re-establish communications for each PEV charging session (repeat communications/re-binding), the ability to provide PEV charging (and other) status information to customer information channels (e.g. web, display devices), and the ability to correctly bill PEV customers according to their selected rates/programs.

The Utility may offer the Customer a PEV tariff that provides a low rate for off-peak charging and a higher rate for on-peak charging. The utility must provide services to support energy supplied to customer PEV. These services include enrollment into a PEV program, PEV communications session binding, PEV energy billing, and PEV information services. The utility will implement an enrollment system for Customers with a PEV including registration and commissioning. The utility’s Energy Services Communication Interface (ESCI) allows for the establishment of a communications session (communications binding), at a premise location each time a PEV plugs in for charging. Energy supplied to the PEV is reported to the utility for billing and presentation to the Customer. Information related to utility PEV programs, energy usage, and PEV charging status/information will be made available to the Customer for viewing via a website or other customer provided display equipment. This use case covers general information for the following five scenarios:

1. Enrollment Process to Time of Use (TOU) Program
2. Enrollment Process to Direct Load/Device Control (DDC) Program
3. Enrollment Process to Real Time Pricing (RTP) or Hourly/Periodic Pricing Program
4. Enrollment Process to Critical Peak Pricing (CPP) or Hourly/Periodic Pricing Program
5. Enrollment Process to Active Load Management Program

- These programs apply to routine or prearranged customer, vehicle usage and charging events.
- It is expected that the enrollment process would identify the customers normal charging pattern, specific details on the vehicle(s) operated that could be matched with anticipated load info to predict minimum effects on the grid.

D.5.1 Use Case Assumptions

- PEV Customer has an account with utility and electrical service at a premise served by the utility.
- PEV and utility have communications capabilities, enabled by utility provided Energy Services Communication Interface (ESCI).
- The customer awareness of the utility and vehicle programs is prompted by both the utility providers and the vehicle manufacturers.
  - The utility offers PEV programs and services for its customers and will provide the necessary support processes for enrollment, communications, and billing
  - The Vehicle manufacturers would provide information to the customer about fuel and/or emission gains of the vehicles offered and promote the utility and convenience of connecting to the grid
- Utility maintains information on all Customers and PEVs enrolled in the PEV programs, including demand side management programs, associated PEV IDs, customer IDs, and premise IDs
- EUMD function can be inclusively located anywhere in a zone from the PEV and the branch circuit panel connection.
- In the absence or failure of PEV-utility communications, or if PEV ID validation fails, PEV charging will always proceed; however, without the incentive rates and with all energy charges accruing to the premise customer according to the premise customer's default rate/service plan.
- The actual PEV charging processes, including scenarios for intra-and inter- utility roaming, are covered in use case P2.
- End Use Measurement Device (EUMD) is always available for PEV charging. If not available, charging will proceed without incentive rates and with all energy charges accruing to the premise customer. This may or may not prevent certain charging status indicators / metrics being available to customer for presentation/display purposes.
- EUMD function can be inclusively located anywhere in a zone from the PEV and the branch circuit panel connection.

To allow for possibility of the EUMD being a part of/within the PEV, PEV is a sub-meter to the primary utility billing meter at any premise (as opposed to being a separate service account with dual meter socket adapter)

The PEV and Utility will communicate to implement one or more the previously described Utility programs

D.5.2 Step by Step Breakdown

Scenario: Customer enrolls in PEV program (Basic Enrollment) and completes initial setup for PEV– Utilities communications

This scenario describes the most common sequence (basic process) of the utility enrolling a PEV customer into a utility program/ service specifically for customers with PEVs. As described in the main Narrative section, the customer is enrolling in a PEV program/service that may provide for the opportunity to fuel a vehicle at a lower cost during off-peak periods based on one of the utility programs enumerated in the main Narrative section. This scenario involves both enrollment of the PEV and steps needed to establish an initial communications session with the utility.

Step 0.5 - The customer awareness of the utility and vehicle programs is prompted by both the utility providers and the vehicle manufacturers.

Step 1 - Customer initiates request to enroll PEV in a PEV Program by contacting Utility and provides Customer and PEV information (i.e. Customer Account information, PEV ID, etc.). [Note: Customer uses phone, Internet, or other communications channel. Preference for PEV is PEV VIN #]
OECD Collection Limitation Principle: Utility collects data by action of the customer

Step 2 - Utility authenticates Customer, Customer account, and Premise information, and collects PEV information including PEV ID.
OECD Security Safeguards Principle: Customer Account data authenticated by Utility to establish identification for PEV

Step 3 - Utility presents Customer with PEV Program information and PEV Program selections.
OECD Purpose Specification Principle: Utility communications to Customer regarding data collection practices

Step 4 - Customer selects PEV Program and Service Plan, sets PEV program parameters (e.g., guest charging, allow roaming, etc.). The Customer and PEV are now enrolled in a utility PEV program.
OECD Individual Participation Principle: Customer confirms data collection arrangements with Utility

Step 5 - Customer connects at their premise location. [Note: The connection could be using either EVSE corset or Premise EVSE. In this scenario we will consider that PEV is connected through EVSE cordset]

Step 6 - PEV and Energy Services Communications Interface (ESCI) initiate a secure communications session. [Note: Implementation could have PEV or ESCI as initiator of session.]
OECD Security Safeguards Principle: Utility establishes secure interface and authenticates session for data collection

Step 7 - PEV ID is transmitted to ESCI. [Note: Unique PEV ID will ultimately support portability of charging, among other purposes.
OECD Security Safeguard Principle: Utility collects Customer data through PEV identification using secure interface and by rearranged process and procedure to secure the data

Step 8 - ESCI maintains communication session and security between PEV and Utility. ESCI transmits request for validating PEV ID to Utility, includes Premise ID.
OECD Security Safeguard Principle: Utility maintains secure interface to transmit data it has collected. Data is also validated according to Utility procedures

Step 9 - Utility identifies and authenticates PEV ID and Premise ID. [Note: PEV binds with utility]
OECD Data Quality Principle: Utility confirms identity and authenticates data per collection practices

Step 10 - Utility transmits confirmation message via ESCI to PEV indicating successful binding with premise ESCI. Confirmation message includes authentication parameters for PEV.
OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission

Step 11 - PEV receives confirmation message and sets authentication parameters.
OECD Security Safeguards Principle: Utility confirms data transmission

Step 12 - PEV transmits via ESCI message to Utility acknowledgement of receipt of valid confirmation message and setting of authentication parameters.
OECD Security Safeguards Principle: Utility through secure interface confirms data transmission

Step 13 - Utility transmits message via ESCI to discover EUMD at Customer Premise; message includes authentication parameters for EUMD. [Note: Authentication parameters would include utility rate program information (e.g. interval size, etc.).]
OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission

Step 14 - EUMD receives discovery message and sets authentication parameters.
OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission

Step 15 - EUMD transmits via ESCI message to Utility acknowledgement of receipt of valid discovery message and setting of authentication parameters.
OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission

Step 16 - ESCI transmits confirmation message to PEV indicating successful communication session binding of PEV to Utility, meaning that charging can proceed according to enrolled PEV program. [Note: Authentication between Utility and PEV is now complete and charging can proceed according to the enrolled PEV program criteria]

OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission using validation process according to Customer preferences

Step 17 - PEV prepares for charging based on Customer-selected preferences and enrolled PEV program. Charging may be delayed based upon Customer preferences or grid reliability criteria (e.g., off-peak economy charging, demand response event underway, short, randomized charging delay to promote grid stability, etc.)
OECD Security Safeguards Principle: Utility communicates data through secure interface and confirms data transmission using validation process according to Customer preferences

APPENDIX E
PRIVACY RELATED DEFINITIONS

Because “privacy” and associated terms mean many different things to different audiences, it is important to establish some definitions for the terms used within this chapter to create a common base of understanding for their use. The energy-specific terms are defined within Appendix I. The definitions of the terms related to privacy, as they are used within this chapter, follow.

E.1 PRIVACY IMPACT ASSESSMENT

A privacy impact assessment (PIA) is a structured, repeatable, type of analysis of how information relating to or about individuals, or groups of individuals, is handled. A report, similar to that of an audit report, is generated to describe the types of privacy risks discovered based upon each privacy category, to document the findings, and then to provide recommendations for mitigating the privacy risk findings. Common goals of a PIA include:

1. Determining if the information handling and use within the identified scope complies with legal, regulatory, and policy requirements regarding privacy;
2. Determining the risks and effects of collecting, maintaining, and disseminating information in identifiable, or clear text, form in an electronic information system or groups of systems; and
3. Examining and evaluating the protections and alternative processes for handling information to mitigate the identified potential privacy risks.

E.2 PERSONAL INFORMATION

“Personal information” is a broad term that includes personally identifiable information (PII), in addition to other types of information. Personal information may reveal information about, or describe, an individual, or group of individuals, such as a family, household, or residence. This information includes, but is not limited to, such information as name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, statements made by, or attributed to, the individual, and utility usage information, all of which could be used to impact privacy.

Personal information includes not only PII, as defined below, but also information that may not be specifically covered within existing laws, regulations or industry standards, but does have recognized needs for privacy protections. For example, a social networking site may reveal information about energy usage or creation.

Personal information within the Smart Grid includes, but is not be limited to, information that reveals details, either explicitly or implicitly, about a specific individual’s or specific group’s type of premises and energy use activities. This is expanded beyond the normal "individual" component because there could be negative privacy impacts for all individuals within one dwelling or building structure. This can include items such as energy use patterns, characteristics related to energy consumption through smart appliances, and other types of activities. The energy use pattern could be considered unique to a household or premises similar to how a fingerprint or DNA is unique to an individual.

Personal information also includes energy use patterns that identify specific appliances or devices that may indicate a medical problem of a household member or visitor; the inappropriate use of an employer issued device to an employee that is a household member or visitor; the use of a forbidden appliance in a rented household. Smart appliances and devices will create additional information that may reveal a significant amount of additional personal information about an individual, such as what food they eat, how much they exercise and detailed physical information. This would also become a privacy issue in a university, office setting, healthcare facility and so on.

E.3 PERSONALLY IDENTIFIABLE INFORMATION (PII)

"PII" is information that has been defined within existing laws, regulations and industry standards, as those specific types of information items that can be tied to a unique individual in certain situations and has some current form of legal protection as a result. For example, the U.S. Health Insurance Portability and Accountability Act requires the following types of individually identifiable information to be safeguarded:

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo-codes
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death;
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers (including energy bill account numbers, credit card numbers, and so on)
- Certificate and license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device Identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images;
- Any other unique identifying number, characteristic, or code

With the exception of those terms specifically naming energy, the above are the items defined within the Health Insurance Portability and Accountability Act (*HIPAA*) of 1996, which arguably

has the widest definition of PII within the existing U.S. federal regulations. More identifiers may be added to the list as the Smart Grid evolves and as regulations change.

E.4 COMPOSITE PERSONAL INFORMATION

"Composite personal information" is non-personal information items that, when combined with certain other non-personal information items, can become personal information. In other words, it is the aggregation or combination of non-personal information that reveals insights into personal lives, characteristics and activities, thus forming personal information. Consider a zip code, gender, and birth year. If you look at each of these separately, it would be hard to say you can link each of them to a specific individual. However, if you look at the three items in combination, you may be able to identify a specific individual, particularly in more sparsely populated geographic locations.

E.5 PRIVATE INFORMATION

"Private information" is information that is associated with individuals or groups of individuals, which could reveal details of their lives or other characteristics that could impact them. Private information is not necessarily information that, on its own, is linked to individuals directly.

Private information is typically a classification of information that individuals use for themselves. It is a broad and general term that is more ambiguously used than other privacy terms. For example, the combination to a bank safety deposit lock is private, but the combination number itself does not point to any specific individual. As another example, some individuals consider how they voted in presidential elections to be private information that they do not want any others know. Other individuals, however, communicate how they voted on bumper stickers for the world to see because they have determined that, for them, it is not private information.

Individuals often consider PII to be a type of private information, and personal information could also be private information. For utilities, market data that includes information about a negotiated price for a customer is likely considered by the customer to be private information; they may not want their friends, neighbors or the general public to see this information. Smart device data from within consumer dwellings could also be a type of private information. Private information could cause harm to the associated individuals or groups if misused or accessed by those who do not have a business need. "Private information" is a term used by individuals that indicates information they have determined they do not want others to know, and is not a term used as a data classification type by business organizations.

E.6 CONFIDENTIAL INFORMATION

"Confidential information" is information for which access should be limited to only those with a business need to know, and that could result in compromise to a system, data file, application, or other business function if inappropriately shared. Confidential information is a common term used by businesses as one of their data classification labels. For example, the formula for Coca-Cola is confidential. The plans for a new type of wind turbine, that have not yet been publicized, are confidential.

Market data that does not include customer specific details may be confidential. Many types of personal information can also fall within the "Confidential Information" data classification label. Information can be confidential at one point in the information lifecycle, and then become public at another point in the lifecycle. Information that an organization does not want shared outside of

their organization, which they consider to be proprietary, is considered to be confidential information. Confidential information must have appropriate safeguards applied to ensure only those with a business need to fulfill their job responsibilities can access the information.

E.7 INDIVIDUAL

Any specific person.

E.8 SMART GRID ENTITY

An entity that participates within the Smart Grid and that collects, stores, uses, shares, transfers across borders, or retains Smart Grid data.