

1 **Privacy of Consumer Information and Devices in the Electric Power Industry**

2
3 prepared by

4
5 Author: Rik Drummond*, Drummond Group Inc.

6
7 Editors: Dr. Kenneth Wacks*, www.kenwacks.com,
8 Conrad Eustis, Portland General Electric,
9 Rebecca Herold, Rebecca Herold & Associates, LLC

10
11 Additional Participants: Dr. Matthew Schneider, Emerson Electric Co,
12 Larry Silverman, GridPlex, Inc.

13
14 presented to

15
16 Home-to-Grid Domain Expert Working Group
17 established by
18 GridWise Architecture Council & NIST

19
20 October 31, 2009

21
22 Version: 3.0¹

23 * Member, GridWise Architecture Council, U.S. Department of Energy

24 **Executive Overview**

25 The Energy Independence and Security Act of 2007 mandated that NIST report to Congress
26 on cyber security for the electricity grid. NIST established a Smart Grid Cyber Security
27 Coordination Task Group and is issuing position papers. Privacy is an important adjunct to
28 security and uses some of the same data tools. However, privacy goes beyond data tools and
29 confidentiality. How personal information is collected, used, shared, stored, retained, and
30 disposed of all impact privacy. Stringent and effective security can be in place and still result in
31 egregious privacy breaches that fall outside of security controls. The Smart Grid Cyber Security
32 Coordination Task Group sought input about home-to-grid issues from Home-to-Grid Domain
33 Expert Working Group members and was consulted in the development of this paper on privacy.

¹ In April 2009, the Home-to-Grid Domain Expert Working Group (H2G DEWG) accepted a proposal by Rik Drummond to investigate privacy and appointed editors to assist him. Rik and the editors consulted with privacy experts at NIST during the development of this paper. Version 1.0 of this document was submitted to the DEWG on October 2, 2009. The H2G DEWG reviewed this document on October 2 and 16, and established a formal procedure for submitting comments during a period of 26 days. Three comments were received from two organizations, resulting in Version 2.0. Version 2.0 was reviewed by the H2G DEWG on October 30, resulting in this Version 3.0.

34 Recommendations in this paper are based not only upon the expertise and suggestions of the
35 NIST security task group members, but also on internationally accepted privacy principles.

36 With the advent of the Smart Electric Power Grid in North America privacy concerns have
37 arisen in two general areas related to smart meters and Demand Response (AMR, AMI and
38 DR)²:

- 39 1. Ownership and misuse of consumer data.
- 40 2. Remote control of consumer premises devices and misuse of that control, and the
41 related data.

42 The usage data being collected from home, commercial and industrial sites are sufficient to
43 provide surveillance-level information on the activities at a specific location. In the
44 residential sector many activities can be revealed through analysis of usage data collected
45 that could compromise privacy, such as:

- 46 • In residential premises usage analysis reveals use of lights, computers,
47 dishwashers, freezers being turned on and off, garage doors being opened and
48 closed; Jacuzzis being used in the wee hours of the morning and, in general, usage
49 patterns that reveal sleep and activity cycles of the family. The “Cycle of Life”
50 could be determined at the location.
- 51 • For a commercial business, usage analysis may reveal proprietary competitive
52 advantages.

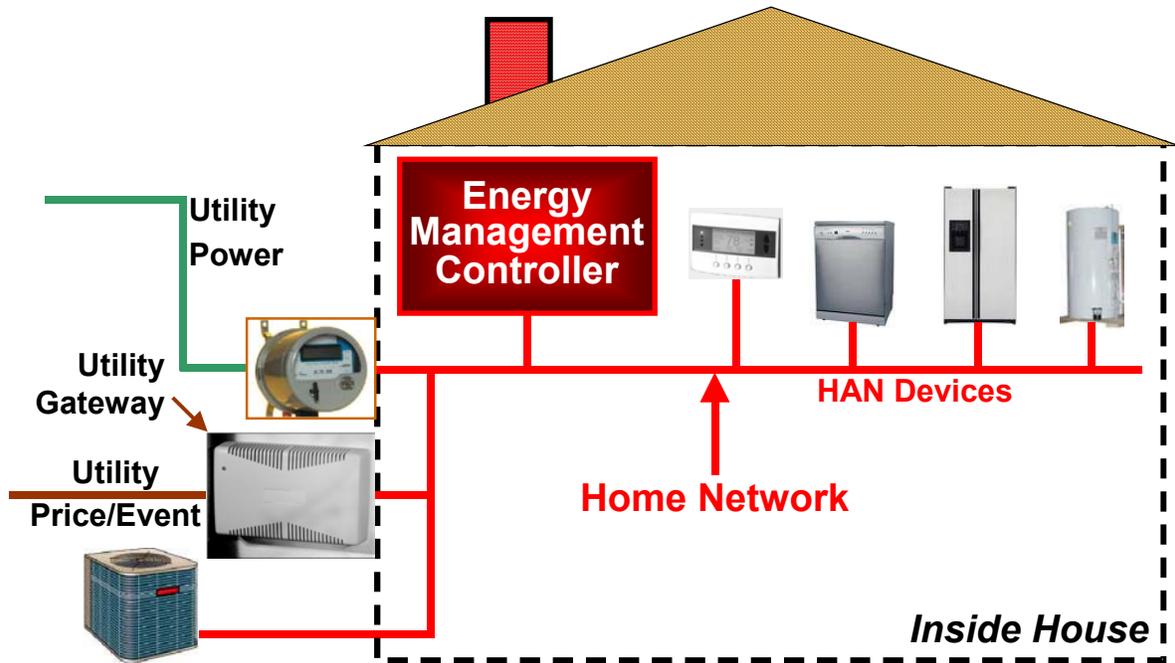
53 Because of the potential abuse of these data we recommend the following assumptions be
54 made about data produced by AMI, AMR and DR-related systems:

- 55 • These data are assumed legally owned by the end electric consumer.
- 56 • The service provider is only a steward of the usage data with specific
57 responsibilities and restrictions.

58 We believe that not using a legal relationship between the consumer and the service provider
59 would put the consumer at risk by allowing the inappropriate monitoring of their premises by
60 service providers and/or third-parties without knowledge of the consumer. To preclude
61 abuse consumer rights and Other-party responsibilities must be put into regulations and laws
62 as privacy mandates.

63 Following are brief descriptions of some of the consequences if the consumer does not own
64 the data from these systems. Figure 1 is an example (but not comprehensive and not the only
65 model) of a configuration illustrating electricity supplied from a service provider with the
66 associated data activity and devices that cause concern using AMI, AMR and DR
67 architectures.

² AMR = Automatic Meter Reading
AMI = Advanced Metering Infrastructure
DR = Demand Response



68

69

Figure 1 – Distributed Load Control for Premises Equipment

70 **Definitions**

- 71 • Consumer – any user of electrical power purchased from another entity.
- 72 • Energy Service Provider-the business entity responsible for fulfilling the
- 73 Consumer’s electric energy needs.
- 74 • Distribution Utility – the business entity that provides the physical path for
- 75 electricity delivery to the Consumer premise, but not necessarily the energy
- 76 retailer.
- 77 • Other(s) – an intermediate party that may provide specific retail energy-related
- 78 services related to electric service use and or delivery, e.g., a DR signals, usage
- 79 data collection and customer billing. It could be anyone other than the consumer
- 80 who has the ability to receive electric usage data.

81 **Theme of recommended policy**

82 Consumers have and retain Legal Ownership of their devices and data. These data generally
 83 include time-interval measurements (watts, volts, amps) in addition to other data that can be
 84 linked to specific individuals. Consumers may grant stewardship to Other-parties with clear
 85 contractual guidelines.

86 This policy means that the consumer allows specified Others the use of the data or remote
 87 control of devices for a contractual purpose, clearly specified activities, and a defined time
 88 period. Transmission-Distribution Utilities and Energy Service Providers will have explicit
 89 authorization to use consumer data as a condition of electric service. The provider must have

90 a written policy on the use and sharing of customer data that is clearly defined in an easily
91 understandable form for the consumer. Any use or sharing of these data that exceeds
92 customer expectations requires the explicit “Consent of Use” by the Consumer. All entities
93 that hold Consumer data or manage Consumer devices must protect these assets for the
94 Consumer because these entities are merely caretakers – not the owner of either the data or
95 the devices. This relationship is not transferable and the contractual conditions are not
96 alterable unilaterally without the cancellation of the complete contract.

97 Failure to follow this policy structure has detrimental consequences for the users of DR, AMI
98 and AMR systems. Breaches of this policy could include unintended and deliberate use and
99 misuse of data by third parties for nefarious purposes, such as the following unintended
100 information gleaned from the data:

- 101 • Personal behavior patterns
- 102 • Specific devices used
- 103 • Real-time surveillance of premise location
- 104 • Cyclic activities
- 105 • Remotely casing a house for opportunities to burglarize it
- 106 • Timing and targeting
- 107 • Targeted home invasions
- 108 • Activity censoring or limitations on device operation
- 109 • Identity theft and location-specific activity data theft

110 **Theme (key issues)**

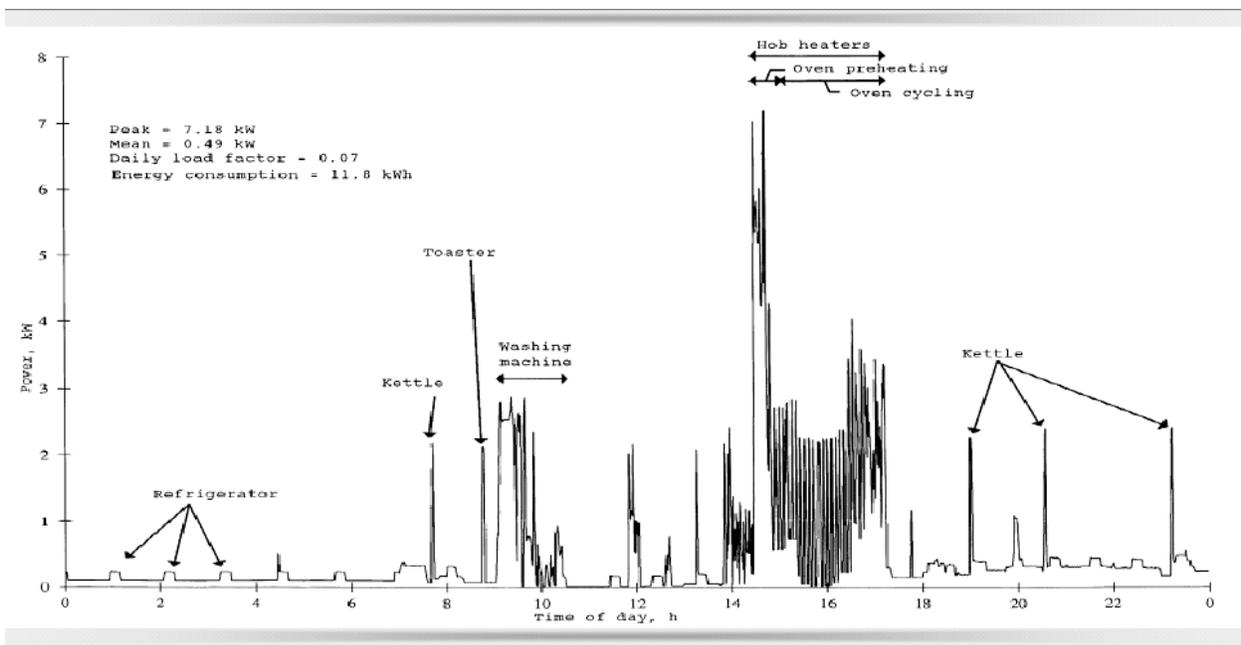
111 Consumer Data Related to AMI, AMR and Demand Response Programs mismanaged by
112 electric providers are threats to consumers of electricity. Topics to be addressed:

- 113 • Ownership of data
- 114 • Stewardship of data
- 115 • Types of data
 - 116 – Total Premise consumption of watts, volts and amps over time-intervals
 - 117 – Specific appliance- and time-based Consumption metering within the
 - 118 premise
 - 119 – Responses to control signals (For example, if a two-way communication
 - 120 system is used, this means data and responses sent from the Consumer
 - 121 premise.)
- 122 • Use of data

- 123 – Intended uses: Billing, demand management, energy conservation,
- 124 appliance identification/analysis, distribution asset management,
- 125 distributed energy resource management, etc.
- 126 – Unintended-uses: [TBD]
- 127 • Sharing of data
- 128 • Retention of data
- 129 • Disposal of data

130 Example of privacy impact – Unintended-Use.

131 Figure 2 shows the power used within a home during specific times of the day. Just viewing
 132 the grid data alone within a centralized server would not directly reveal a specific individual
 133 or household. However, if this usage data were viewed or connected to a name, address or
 134 meter identifier, it would reveal the activities of a household. This is a significant privacy
 135 concern.



136

137 **Figure 2 – Information Derived from Meter Consumption Data**

138 **Sub-Issue-1: Other-party provided data use**

139 Unless an explicit bi-lateral contract exists, Consumers may choose for energy management
 140 to use or not to use price and other information such as availability, reliability, environmental
 141 characteristics, etc. They may choose to use this information in some cases, but not always.
 142 Many consumers will not wish to have their devices controlled by any party for the
 143 foreseeable future. Not all consumers will be able or willing to participate in DR, AMI,

144 AMR programs offered by utilities or Other-parties because either they don't have the
145 wherewithal or they do not wish their usage data to be collected in time intervals by the
146 service provider.

147 Consumers should not be forced to participate in these DR programs. If they do not wish to
148 participate then they should continue to receive the services that typically predominate in
149 their market (home, commercial, and industrial are considered separate markets) without
150 prejudice or discrimination. Regulators could decide, however, that certain types of electric
151 service should be priced at a premium because of legitimate risk or economic hardships these
152 services impose on the grid.

153 **Consumer options:** consumer participation in demand response programs

154 Consumers must have a choice of levels for participation:

- 155 • No participation.
- 156 • Anonymous participation – receive published data only (control or price).
- 157 • Choose specific loads under direct control.
- 158 • Choose specific method of load control, such as personal management of
159 appliances, a gateway that can mediate for the premises, etc.

160 **Sub-Issue-2: Other-Party frequency of data collection**

161 All parties must exercise extreme care when gathering usage data especially at short (five,
162 ten minute, intervals etc.) or more frequently because it can reveal sensitive information
163 about the consumer periodic/cyclic activity. This reduces the security and privacy of the
164 consumer's premise if the data are available to a non-contractual party or to a contracted
165 party that misuses the data. All parties should have liability for inadvertent release of usage
166 data traceable to a specific customer location. All parties should state in written, publicly
167 available documents the specific types of data retained by the Other-party, how these data are
168 protected, and under what conditions the data are made available to Other-parties.

- 169 • Service providers must assume responsibilities and liability for lost or misused
170 customer data, because these data are sensitive and, in many ways, akin to detailed
171 activity surveillance data of a location. Liability risk is a key tool to guide
172 appropriate investment in data security.
- 173 • Any data collected must be the minimum necessary for the service provide by the
174 Other-party to the consumer (“the less the better”). (This principle is challenging
175 because the cost of storage is dropping.)
- 176 • Equipment makers may incorporate local intelligence in meters and gateway
177 devices that gather usage data. This local intelligence should be designed to
178 aggregate data so the minimum required data are sent to the service provider to
179 fulfill the customer request for energy management. Please note that some
180 benefits of passing detailed data upstream may be lost. Service providers and

181 customers may need to balance privacy and service benefits. Use cases need to be
182 examined for the impact of local data aggregation.

183 • Regulators must challenge service providers about the necessity for data collection
184 and establish stringent data handling rules. These rules should require that
185 customer identification data (name address, etc) not be co-located with electric
186 usage data.

187 • Customers must provide explicit documented permission for data sharing and data
188 mining. Data mining customer usage-data by a service provider can lead to both
189 beneficial and harmful results. Regulators should approve specific beneficial uses
190 permitted by a service provider. All other data mining activities should be
191 prohibited without explicit permission from the consumer. For example
192 aggregating customer usage data on a single domicile service transformer may
193 identify probable, future failure. This is especially important as electric vehicles
194 grow in popularity. Data mining can identify vehicle charge usage coincident
195 with summer air-conditioning load to locate undersized transformers before they
196 fail. On the other hand, data mining could allow creation of an accurate list of
197 homes with swimming pools, and this could be sold, thereby benefiting a
198 commercial entity at the expense of customer privacy.

199 • Service providers must have incentives to de-correlate usage and outage electric
200 data from the location of the premises as soon as practicable to ensure that the
201 data cannot be used to do historic surveillance type viewing of a residential,
202 commercial or industrial property. Regulators should ensure this.

203 • Service providers must treat correlated data as a valuable asset with appropriate
204 safeguards, and consequences for loss or theft. Specifically:

205 – Databases from Others containing usage data are considered a business
206 asset of the Other party. Such assets move from one legal entity to another
207 legal entity during the sale of assets and/or purchase of an entire company.
208 For example if a non-US electric company buys a US electric company,
209 what laws or regulations will protect consumer data when this data
210 “automatically” moves from an entity trusted by the consumer, to a new
211 legal entity of unknown trustworthiness? When approving a sale
212 transaction, regulators should examine the contract for conditions of the
213 new owner regarding acquisition of assets with customer interval usage
214 data and associated data protection promises.

215 – Energy Service Providers frequently engage third parties where the
216 engagement requires customer usage data to pass to the third party, for
217 example, to analyze the benefits of a new demand response program, or in
218 the operation of a web-based customer information portal service. In these
219 cases, energy service providers and Other-parties should be provided a
220 written statement of how customer data will be protected before the
221 contract is executed. Where possible customer-specific data should never
222 be included in the same transaction as usage data. In fact, in most cases

223 these services should be executed using usage data only; rarely are
224 customer name and address required to perform a service.

225 **Sub-Issue-3 Consumer Data Managed by Other-party**

226 • Correlated data must be kept close to customers. As data moves from appliances
227 to home network equipment to meters to service-provider back offices, these data
228 should be de-correlated as soon as possible so they cannot be linked backed to the
229 consumer or source location.

230 • For the monthly consumer bill providers who need access to more time-based
231 details the consumer should assume responsibility for maintaining detailed
232 consumption data locally. If desired the consumer may choose to hire an archivist,
233 like a bank vault.

234 • Consumers should have tools for managing personally identifiable data.
235 Consumer electronics and appliance companies might develop these tools.

236 Consumers should be educated on the benefit of installing a local energy management
237 system to minimize sharing of sensitive data. See Figure 1.

238 **Sub-Issue-4: Other-party Data aggregation and Device database protection issues.**

239 Electric usage, outage and etc. data that must be aggregated for planning and other purposes
240 should ensure the specific geographic location of individual consumers are not identifiable.
241 (The specific number of houses to aggregate is to be defined and may vary by
242 neighborhood). Additionally device usage data should not be identifiable to the location of
243 the device and must be grouped to disguise the location of the specific device. Only the data
244 tied to the geographic location should be retained to allow billing and auditing of the
245 transactions for the appropriate time periods. Statistical aggregated data to a group of
246 geographic locations will have to be kept for long periods for the planning purposes of the
247 Other-parties. These will likely be grouped in to billing and substation groups depending on
248 the market structure of the region.

249 • No correlation of data by consumers.

250 • No Correlation of data by specific location.

251 • No Correlation of data by appliance/devices that can infer the location of these
252 devices.

253 **Internationally Recognized Privacy Principles**

254 The principles in this document align with those developed by NIST, as contained in
255 Appendix A.

256
257

Annex A

Generally Accepted Privacy Principles

258 NIST provided the following international generally accepted privacy principles (GAPP),
259 which form the basis of most international, national and local data protection laws, along
260 with consideration of safeguards as found in the international information security standard
261 ISO/IEC 27001, also widely used for data protection regulatory compliance:

262 **1. Management and Accountability:** An organization should formally appoint
263 personnel to ensure that information security and privacy policies and practices exist
264 and are followed. Documented requirements for regular training and ongoing
265 awareness activities should exist and be followed. Audit functions should be present
266 to monitor all data accesses and modifications.

267 **2. Notice and Purpose:** A clearly-specified notice should exist to describe the purpose
268 for the collection, use, retention, and sharing of PII (Personally Identifiable
269 Information). Data subjects should be told this information at or before the time of
270 collection.

271 **3. Choice and Consent:** The organization should describe the choices available to
272 individuals and obtain explicit consent if possible, or implied consent when this is not
273 feasible, with respect to the collection, use, and disclosure of their PII.

274 **4. Collection and Scope:** Only PII that is required to fulfill the stated purpose should be
275 collected from individuals. Treatment of the information must conform to fair
276 information processing practices. Information should be collected directly from each
277 individual person unless there are justifiable reasons why this is not possible.

278 **5. Use and Retention:** Information should only be used or disclosed for the purpose for
279 which it was collected, and should only be divulged to those parties authorized to
280 receive it. PII should be aggregated or anonymized wherever possible to limit the
281 potential for computer matching of records. PII should only be kept as long as is
282 necessary to fulfill the purposes for which it was collected.

283 **6. Individual Access:** Organizations should provide a process for PII data subjects to
284 allow them to ask to see their corresponding PII and to request the correction of
285 perceived inaccuracies. PII data subjects must also be informed about parties with
286 whom PII has been shared.

287 **7. Disclosure and Limiting Use:** PII should be used only for the purposes for which it
288 was collected. PII should not be disclosed to any Other-parties except for those
289 identified in the notice, or with the explicit consent of the individual.

290 **8. Security and Safeguards:** PII, in all forms, must be protected from loss, theft,
291 unauthorized access, disclosure, copying, use, or modification.

292 **9. Accuracy and Quality:** Every effort should be made to ensure that the PII is
 293 accurate, complete, and relevant for the purposes identified in the notice, and remains
 294 accurate throughout the life of the PII while within the control of the organization.

295 **10. Openness, Monitoring and Challenging Compliance:** Privacy policies should be
 296 made available to PII data subjects. PII data subjects should be given the ability and
 297 process to challenge an organization’s compliance with their state privacy policies as
 298 well as their actual privacy practices.

299 The ability for smart grid devices to “roam” to other utility systems – for example, driving an
 300 electric vehicle (PEV) to visit family, and recharging it while there – creates the potential for
 301 additional flows of PII data. This might occur if the “host” utility were in a position to bill
 302 the PEV’s “home” utility for the PEV’s recharge.

303 Figure 3 provides a summary of the privacy concerns related to PII and derived PII use when
 304 disclosed to other entities and used for purposes beyond the PII collection purposes.

Privacy Concern	Discussion
1. Identity Theft	Specific combinations of PII may be used to impersonate a utility consumer, resulting in potentially severe impacts, such as negative credit reports, fraudulent utility use and other damaging consumer actions.
2. Determine Personal Behavior Patterns	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. The information revealed is a type of surveillance. The data could be (mis)used by other entities to do target marketing, by governments to try and tax specific activities and uses, and by persons with malicious intent..
3. Determine Specific Appliances Used	Smart meter and home automation network data will have the ability to track the use of specific smart appliances. Appliance manufacturers may want to get this information to know who, how and why individuals used their products in certain ways. Such information could impact appliance warranties. Insurance companies may want to use this information to approve or decline claims. And there is an unlimited number of other possible uses as yet not imagined that this data could provide.
4. Perform Real-Time Surveillance	Access to live energy use data can reveal if people are in the residence, what they are doing, where they are in the residence, and so on. This not only presents a safety risk, with burglars and vandals using it to their destruction, but it could also be used to do target marketing based upon home energy use behaviors.

Privacy Concern	Discussion
5. Reveal Activities Through Residual Data	Several articles have been published warning that if the data on the metering devices is not effectively or completely removed, the residual data can reveal to the new meter user, or entity that possess the meter, the activities of the former owner. If true, not only does this present similar concerns to those listed in the first three concern topics, it could also be used by activists or others who have agendas to reveal what they view as a lack of social responsibility. However, to prevent any tampering of historical data and to satisfy the size constraints for the new meters — providing more functionality in the same physical meter box — the data is not likely to be stored within the smart meter itself. But, the possibility of storing data within home meters should be considered in any meter functionality plans so that if it does become possible to store PII in smart meters the privacy issues will be appropriately addressed.
6. Target Home Invasions	Malicious use of meter data for specific consumers could lead to a wide number of problems, such as physical invasions to the home because crooks could tell when residents were away, whether or not they have an alarm system, and so on.
7. Provide Accidental Invasions	Combinations of meter data, analyzed for one purpose, could reveal unexpected information about the residents that is then used to the detriment of the residents.
8. Activity Censorship	The meter data could reveal resident activities or uses that utility companies may then subsequently decide are inappropriate or should not be allowed. Without restrictions, if this information could then shared with local government, law enforcement, or public media outlets the residents could suffer embarrassment, harassment, loss of vital appliances, or any number of other damaging actions.
9. Decisions and Actions Based Upon Inaccurate Data	With meter data being stored in potentially many locations, accessed by so many different individuals and entities, and used for a very wide variety of purposes, it is a significant risk that the PII data will become inappropriately modified. Automated Smart Grid decisions made for home energy use could not only be detrimental for residents (e.g., restricted power, thermostats turned to dangerous levels, and so on) but decisions about Smart Grid power use and activities could be based upon inaccurate information.

Privacy Concern	Discussion
<p>10. Reveal Activities When Used With Data From Other Utility Services</p>	<p>Even more personal activities and derived PII could be revealed if the power meter PII was combined with the PII from other utilities and utility meters, such as those for gas, water, and so on. This is of particular concern when the different utility services are provided by the same corporate entity (combined Gas and Electric utilities, or municipal co-ops that may also provide water and sewer services, for example)</p>

305
306

Figure 3 – Privacy Impacts for Disclosure and Misuse of Personally Identifiable Information (PII)