
NISTIR 7628 *Guidelines to Smart Grid Cyber Security* Volume II: Privacy Briefing

September 29, 2010

CSWG Privacy Subgroup Lead: Rebecca Herold (rebeccaherold@rebeccaherold.com)

Subgroup Member: Brent Struthers (brent.struthers@neustar.biz)

NIST Point of Contact: Tanya Brewer (tanya.brewer@nist.gov)

Twiki: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy>



Disclaimer

The views and opinions expressed within this briefing are those of the presenters, speaking on behalf of themselves as well as in representation of the diverse membership within the CSWG Smart Grid Privacy Subgroup.

Their opinions and views are not necessarily those of NIST.

Agenda

- Morning (10:00 AM – Noon)
 - CSWG privacy sub-group mission
 - Overview of privacy sub-group demographics
 - What is privacy?
 - What is “personal information” in the Smart Grid?
 - Consumer-to-utility Privacy Impact Assessment (PIA)
 - Legal frameworks and considerations
- Afternoon (1:00 PM – 4:00 PM)
 - Data collection and availability
 - Commissioning and enrolling issues
 - Wireless access
 - Accessibility via the Internet
 - Third party access
 - Law enforcement access
 - Mitigating privacy concerns
 - Work going forward

Smart Grid Privacy Group Scope/Mission

To identify and clearly describe privacy concerns within the Smart Grid and opportunities for their mitigation. In addition, the group strives to clarify privacy expectations, practices, and rights with regard to the Smart Grid by:

- ❑ Identifying potential privacy problems and encouraging the use of relevant existing fair information practices
- ❑ Seeking the input of and educating Smart Grid entities, subject matter experts, and the public on options for protecting privacy of, and avoiding misuse of, personal information used within the Smart Grid
- ❑ Providing recommendations for coordinating activities of relevant local, state, and federal agencies regarding Smart Grid privacy related issues
- ❑ Making recommendations and providing information to organizations developing privacy policies and practices that promote and protect the interest of Smart Grid consumers and organizations

Smart Grid Privacy Group Scope/Mission

Try to answer questions such as those received informally on September 21:

- ❑ *“How will information about my energy consumption (days, times, amounts, and other use profile information) be used shared with business partners?”*
- ❑ *“Will there be any public way to verify addresses or names of clients of the grid?”*
- ❑ *“Any and all PII will be considered private and confidential I hope. Or will they make the mistakes of so many others in the past of doing reverse lookups based on meter numbers or neighborhood consumption reports?”*
- ❑ *“How would I know if my utility or third party follows these [NISTIR7628] guidelines?”*
- ❑ *“What steps should a regulator take to ensure privacy? “*
- ❑ *“Do the Fair Information Practice principles (“FIPs”) provide a sound and adaptable framework for addressing consumer privacy concerns or are they just the baseline?”*
- ❑ *“How secure are the meters, HAN and other communication devices (secure in the means of protecting customer information)?”*
- ❑ *“What types of “click and consent” models will be used?”*
- ❑ *“How will information be shared and used, and how will it be protected?”*
- ❑ *“What kind privacy protections will be in place prior to allowing third party access?”*

Group Demographics

The NIST Smart Grid Privacy Subgroup currently includes:

- ❑ Energy and Utilities Industry Experts
- ❑ State Public Utilities Commission Representatives
- ❑ Information Security Experts
- ❑ Privacy Experts
- ❑ Attorneys and Legal Experts
- ❑ University Professors and Students

Other technical, operational and privacy experts, from all regions, are welcome to join the group!

What Is Privacy?

What Is Privacy?

- ❑ No universal definition
- ❑ Means many things to different groups and individuals
- ❑ Is NOT the same as confidentiality



What Is Privacy?

- Four Dimensions of Privacy
 - Personal information
 - Describes specific aspects of an individual
 - Personal privacy
 - The rights to control the integrity of one's one body
 - Behavioral privacy
 - The right of individuals to make their own choices about what they do and keep certain personal behaviors from being shared with others
 - Personal communications privacy
 - The right to communicate without undue surveillance, monitoring, or censorship

What Is Privacy?

- Impact of the Smart Grid on Privacy
 - The Smart Grid will greatly expand the amount of data that will be monitored, collected, aggregated, and analyzed
 - This expanded information, particularly from customer sites, raises added privacy concerns
 - The Smart Grid is an “always on” passive participation network
 - The innovative technologies of the Smart Grid pose new legal issues for privacy within the home and other properties

What Is Privacy?

Some identified Smart Grid privacy concerns (1/2):

- Fraud
 - Attribute energy consumption to another location
 - “Phishing” and “pharming” schemes to get customers to share personal information

- Determine Appliances Used
 - Smart meter and home automation network data may track use of specific appliances
 - Manufacturers may want this information
 - Could impact appliance warranties

What is Privacy?

Some identified Smart Grid privacy concerns (2/2):

- Determine Personal Behavior Patterns
 - Can reveal specific times/locations of energy usage

- Perform Real-Time Surveillance
 - If people are in a facility/residence, what they are doing, sleeping patterns, number of people present

- Non-Grid Commercial Uses of Data
 - Could reveal lifestyle information
 - Potential for profiling users/individuals

“Personal Information” in the Smart Grid

“Personal Information” in the Smart Grid

- “Traditional” personal information items, such as:
 - Name
 - Address
 - Credit card number
 - Social Security Number
 - Etc.

- “Anonymous” data in the Smart Grid may not be so anonymous after all

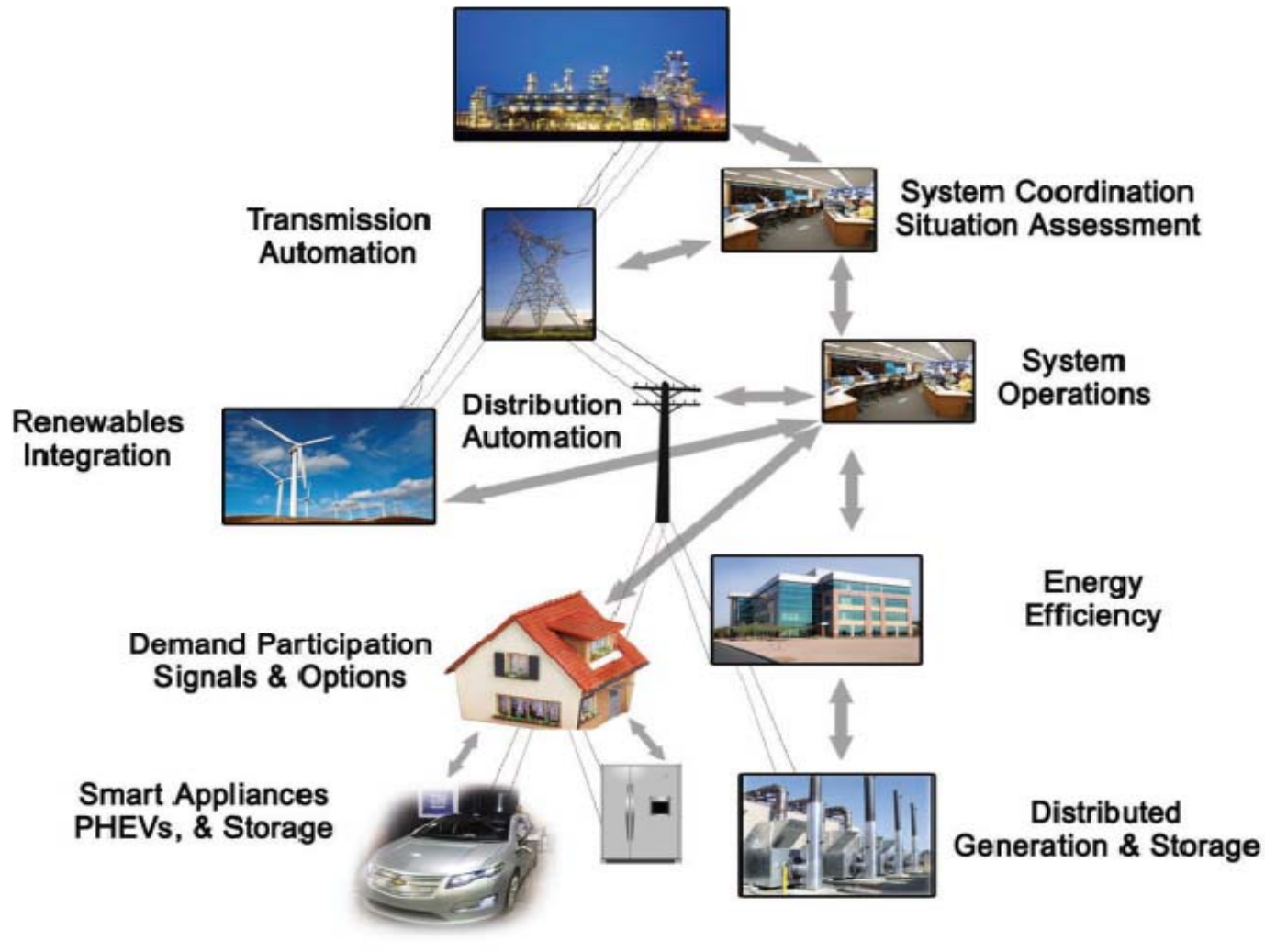
- Some types of energy usage/creation data

Consumer-to-Utility Privacy Impact Assessment (PIA)

Consumer-to-Utility PIA

- PIA = Privacy Impact Assessment
- Process for determining the privacy, confidentiality, and security risks associated with the collection, use, and disclosure of personal information
- Performed July – August 2009
- Used the following as primary evaluation criteria:
 - American Institute of Certified Public Accounts (AICPA)
 - Generally Accepted Privacy Principles (GAPPs),
 - The Organisation for Economic Cooperation and Development (OECD) Privacy Principles
 - 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

Consumer-to-Utility PIA



Retrieved 8/27/09 from page 2 at http://www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf.

Consumer-to-Utility PIA

PIA Findings Included (1/2):

- 1. Management and Accountability:** Lack of 1) documented information security and privacy responsibilities and authority; (2) information security and privacy training and awareness programs; and (3) monitoring access to Smart Grid data.
- 2. Notice and Purpose:** Be more transparent and clearly provide notice documenting the types of information items collected and the purposes for collecting the data.
- 3. Choice and Consent:** Establish processes to give consumers a choice, where possible and feasible, about the types of data collected and how it is used.
- 4. Collection and Scope:** Only the minimum amount of data necessary for services, provisioning, and billing should be collected.
- 5. Use and Retention:** The Smart Grid will provide data that can be used in additional ways not currently possible; usage and retention requirements should be established.

Consumer-to-Utility PIA

PIA Findings Included (2/2):

- 6. Individual Access:** Smart meter data may be stored in multiple locations to which the consumer may not have ready access; access policies and processes should be established.
- 7. Disclosure and Limiting 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, and only with those authorized.
- 8. Security and Safeguards:** Establish strong security safeguards to protect energy data from loss, theft, unauthorized access, disclosure, copying, use, or modification.
- 9. Accuracy and Quality:** Ensure Smart Grid data is accurate, complete, and relevant for the identified purposes for which they were obtained, and that it remains accurate throughout the data lifecycle.
- 10. Openness, Monitoring, and Challenging Compliance:** Allow consumers opportunity and processes to challenge compliance, along with performing periodic PIA and establishing breach response processes.

Legal Frameworks and Considerations

Legal Frameworks and Considerations

- Existing Regulatory Frameworks
 - US Energy Regulations
 - US Federal Laws:
 - Healthcare: E.g., HIPAA/HITECH
 - Financial: E.g., GLBA, FACTA, Red Flags Rule
 - Education: E.g., FERPA, CIPA
 - Communications: E.g., First Amendment to the U.S. Constitution, ECPA, TCPA
 - Government: E.g., Privacy Act of 1974, Computer Security Act of 1987, E-Government Act of 2002.
 - Online Activities: E.g., CAN-SPAM Act, USA PATRIOT Act,
 - Privacy in the Home: E.g., Fourth and Fourteenth Amendments to the U.S. Constitution.
 - Employee and Labor Laws: E.g., ADA, EEO Act
 - US State/Territory Laws
 - International Laws

- Legal Protections

Legal Frameworks and Considerations

- Smart Grid Data Ownership
- Applicability of Existing Laws & Regulations to the Smart Grid
- General Invasion of Privacy Concerns with Smart Grid Data
- Smart Grid Data Introduces a New Privacy Dimension

Data Collection & Availability

Data Collection & Availability

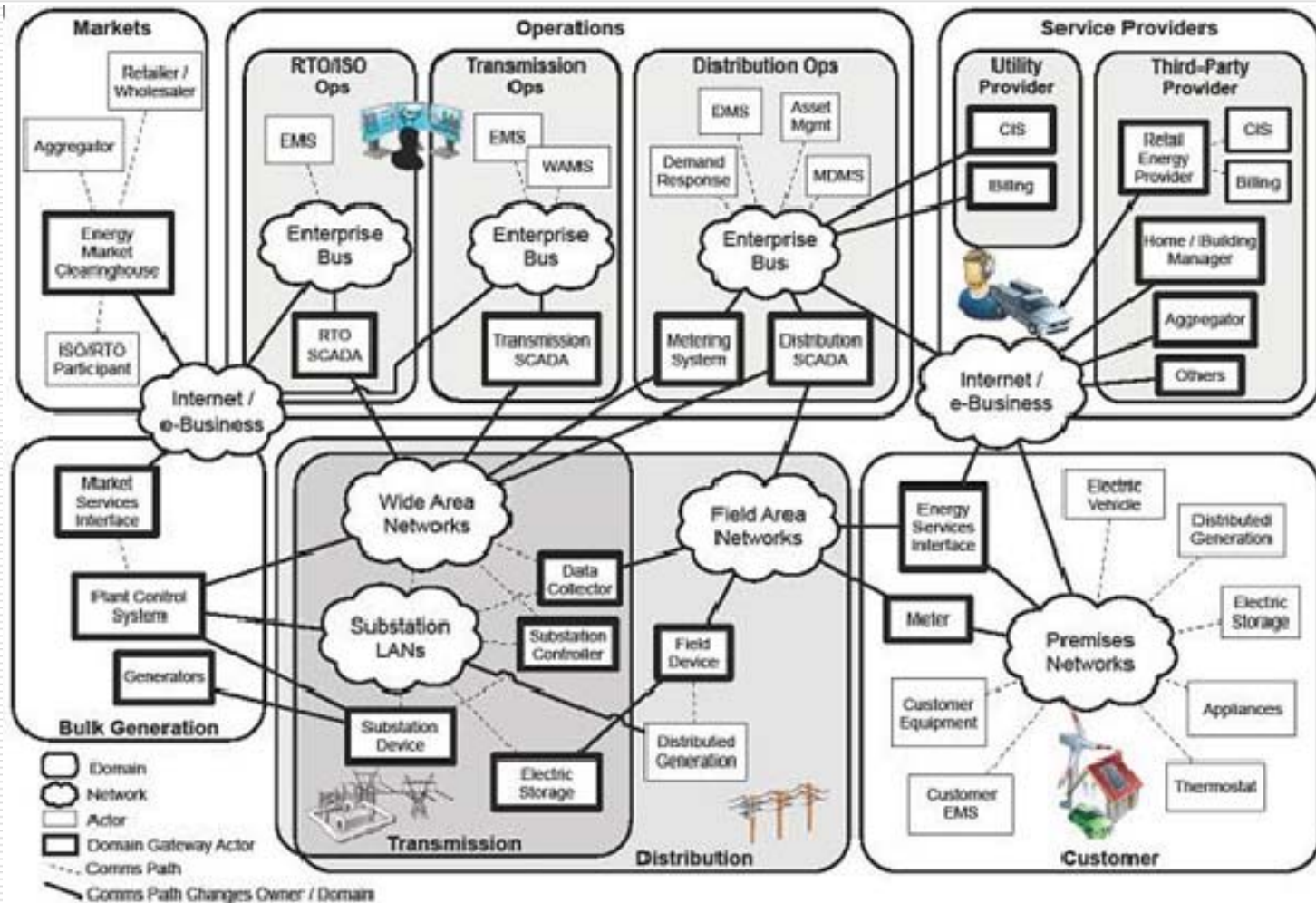


Figure 5-2 NIST Conceptual Model

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.

Data Collection & Availability

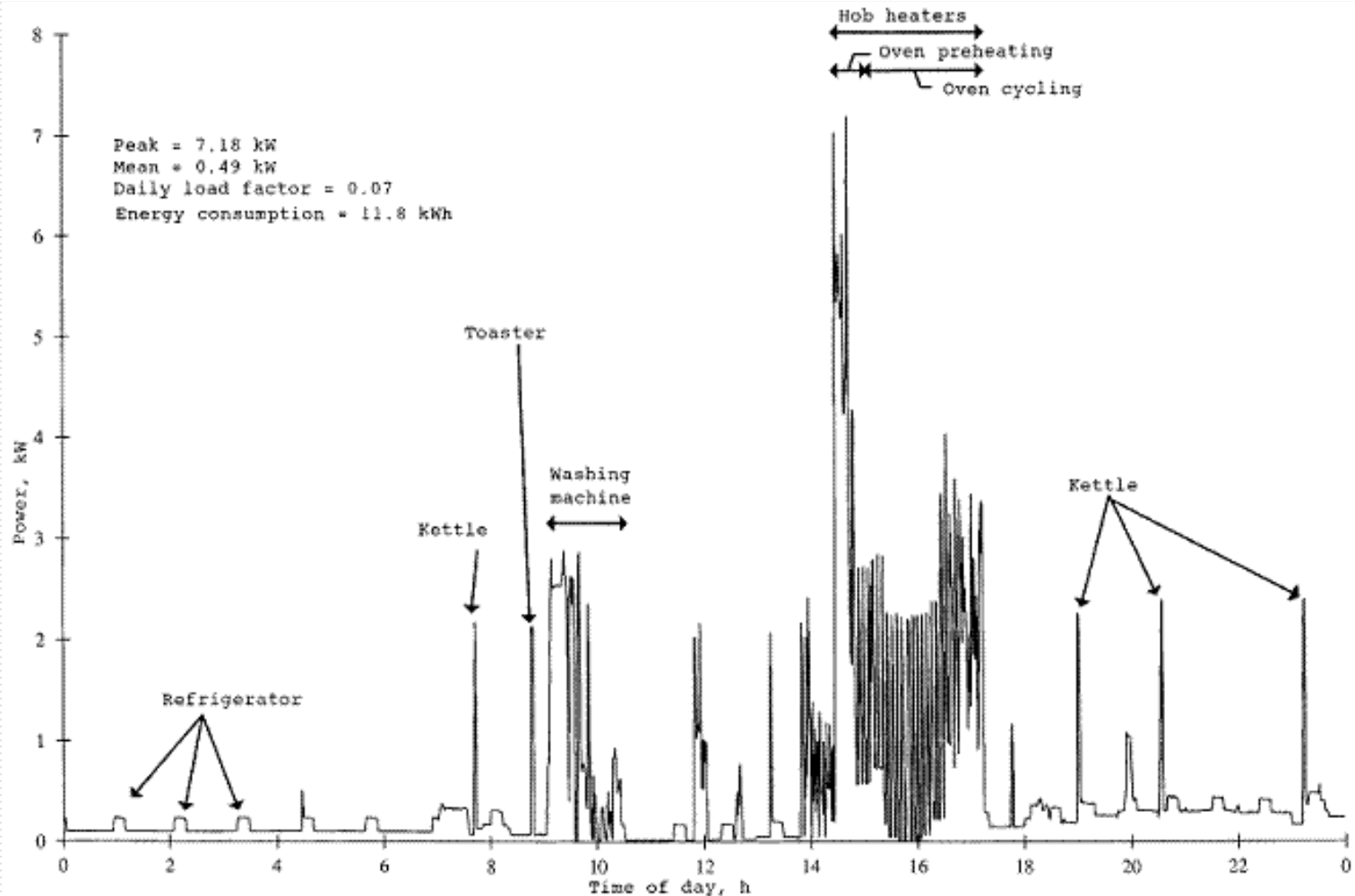


Figure 5-1 How power use can reveal personal activities through nonintrusive appliance load monitoring

Elias Leake Quinn, *Smart Metering & Privacy: Existing Law and Competing Policies*, Spring 2009, at 3. Available at http://www.dora.state.co.us/puc/DocketsDecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-Smart_GridPrivacy.pdf.

Data Collection & Availability

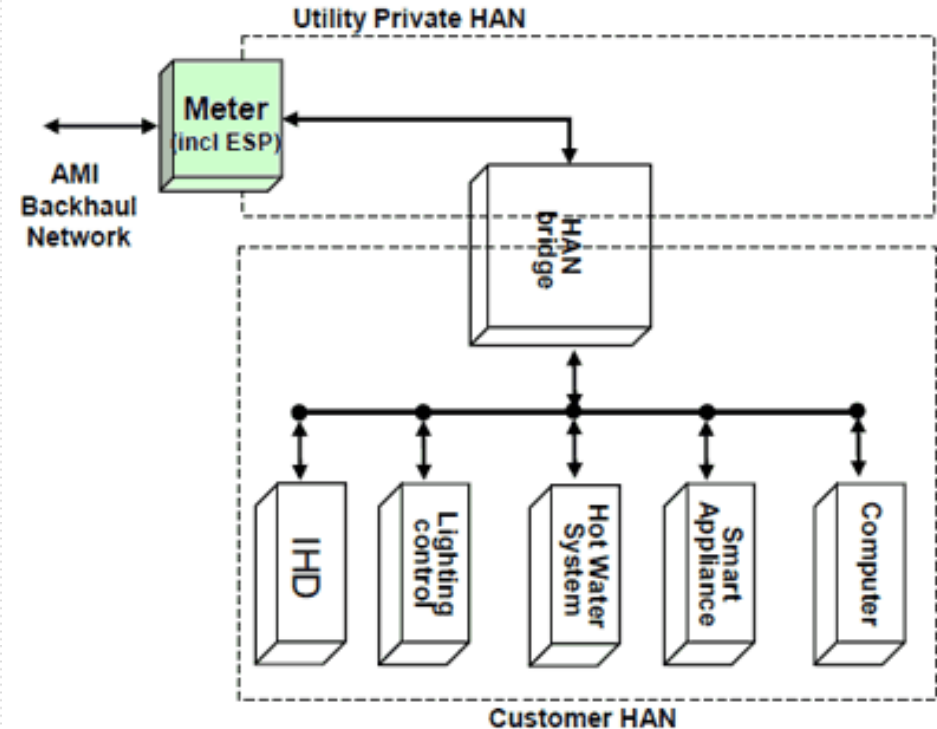
Data with potential privacy impacts includes that which:

- ❑ Captures detailed energy usage at a location, whether in real-time or on a delayed basis
- ❑ Identifies location / recharge information for PEVs or other location-aware appliances
- ❑ Identifies individual meters or consumer-owned equipment and capabilities

Commissioning & Enrolling Issues

Commissioning & Enrolling Issues

- Commissioning process
- Registration process
- Enrollment process
- Examples
 - HAN device
 - PEV special rate
 - Demand-response
 - Prepay program
 - Etc.
- Data involved
- Data flows
- Data usage



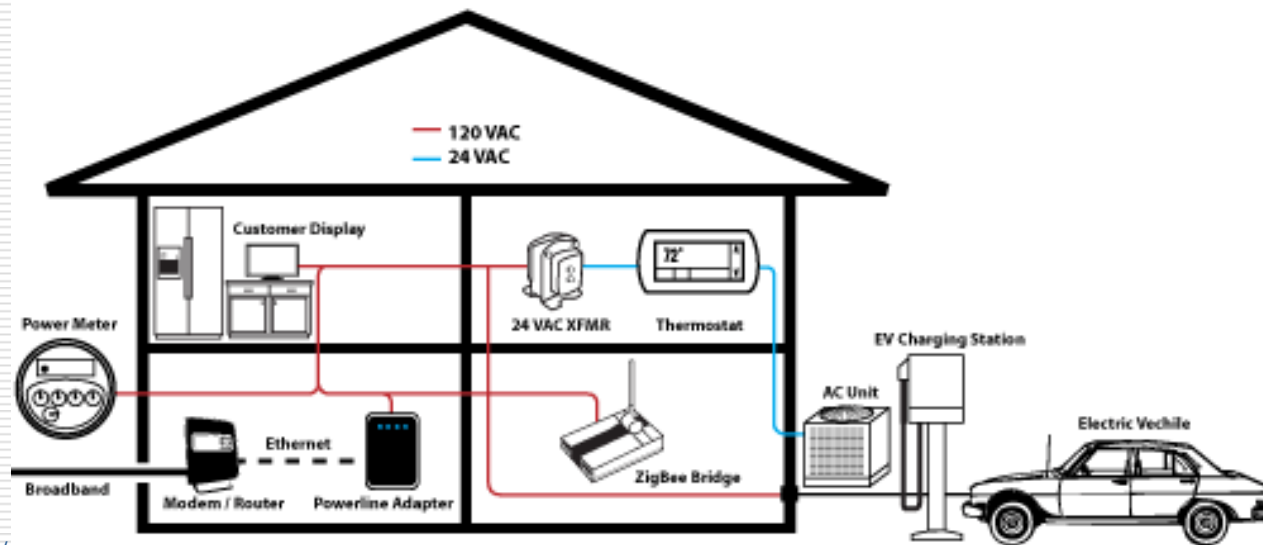
From

<http://new.dpi.vic.gov.au/energy/projects-research-development/smart-meters/home-area-network>

Wireless Access

Wireless Access

- ❑ Smart meters
- ❑ Smart appliances
- ❑ Vulnerabilities and privacy impacts
- ❑ More work planned



Taken from <http://>

Data Access Via Internet

Data Access Via Internet

- Smart Grid data accessibility through the Internet
 - Social Media sites
 - Storage/backup sites
 - Energy usage monitoring
 - Etc.

- More work planned



From
<http://www.electronichouse.com/article/weet-a-watt-now-available/C212/>
Sept 22 2010

Access by Third Parties

Access by Third Parties

- Three privacy challenges presented by third-party access to Smart Grid data -
 1. That companies representing themselves as consumer electricity management services are what they represent themselves to be
 2. What consumers are told about how their information will be used is true
 3. 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.

Law Enforcement Access to Data

Potential for Law Enforcement Requests

- Law enforcement has used aggregate utility data in the past.
 - **Kyllo vs. United States**
 - Subpoena issued for utility records to help further case against Kyllo not questioned by courts.
 - Law enforcement use of thermal imaging device without search warrant found unconstitutional by Supreme Court.
 - In what realm does smart grid data fall?

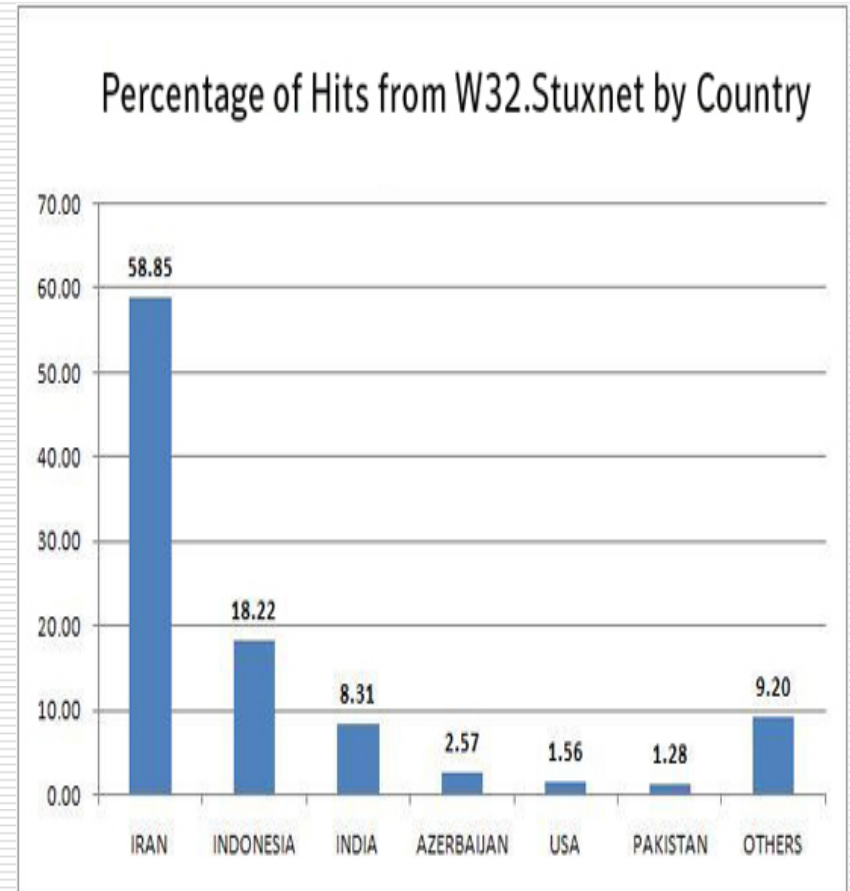
- To what extent more detailed smart grid data will hold an interest to law enforcement is yet unknown.

Law Enforcement Use of Telecom Data

- Records production, historic data (subpoena)
 - Tier 1 carriers get about 200,000 requests per year
 - Criminal 90%; Civil 10%
- Real-time (court orders)
 - Monitoring conversation or tracking, inbound and outbound numbers.
 - Tier 1 carriers get from hundreds to a couple thousand court orders per year.
- Equipment designed around needs of LE
 - Law enforcement needs so complex that Congress required telcos to set up networks to handle.

Access to Data for What Purpose?

- Law Enforcement Physical Crimes
 - Illegal drug operations
- Law Enforcement Cyber Crimes
 - Potential area of future study
 - Investigation of cyber attacks on grid
- Civil Litigant/Private Investigators
 - Divorce proceedings



From http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-071400-3123-99 Sept 22 2010

Access to which data?

□ Historical

- Long-term usage information
- Where were you on the night of...?
- PEV charging routines.
- Data retention requirements

□ Real-time

- Kidnapper has three likely destinations. Is one currently showing power usage?

Types of Data

- Detailed energy usage at a premise
 - Law Enforcement
 - Identify suspicious or illegal activity, or determine presence of occupants.
 - Civil Litigants
 - Determine presence of occupants.

Examples:

1. Law enforcement narrowing location of a kidnapping suspect to one of a number of potential locations.
2. Divorce court determining veracity of claim spouse was at home.

Types of Data, cont.

- Identifies Location
 - Law Enforcement
 - Tracking current location or movement patterns over time
 - Civil Litigants
 - Determining presence (or lack thereof) at a specific locale

Examples:

1. Law enforcement establishing travel between known drug distribution points.
2. Divorce court determining travel between possible rendezvous points.

Types of Data, cont.

- Identification of Household Appliances
 - Law Enforcement
 - Energy use patterns consistent with illegal activity
 - Civil Litigants
 - Identify activities on premise

Examples:

1. Law enforcement collecting evidence to support investigation of meth lab, or to detect presence of many computers used in hacking operation.
2. Divorce court seeking information on appliances (ex. hot tub) in use on a certain date and time.

What Laws Apply?

- What existing laws cover access to this data?
 - Is this communications data?
 - Is it utility records?
 - Is it data subject to 4th amendment protections?
 - Is it something new not covered under current legal regimes?

An area requiring more focus.

Mitigating Privacy Concerns

Mitigating Privacy Concerns

1. Conduct PIAs
 - Initial PIA before making the decision to deploy and/or participate in the Smart Grid
 - Subsequent PIAs as appropriate, such as following organization and systems changes, new and updated laws, and privacy breaches
2. Develop and formally document privacy policies and practices
3. Use 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

Mitigating Privacy Concerns

4. Educate the public about the privacy risks within the Smart Grid and what they as consumers can do to mitigate them
 - Government
 - Utilities
 - Smart Grid vendors
5. Share information concerning solutions to common privacy-related problems
6. All Smart Grid entities should collect only the energy and personal data necessary for the purposes of the smart device operations
7. Implement standards, laws and regulations

Work Going Forward

Work Going Forward

- Address privacy issues for businesses (commercial, institutional, industrial)
- Address privacy issues related to energy generation
- Add more privacy use cases
- Add more energy regulations/laws and privacy laws to the appendix
- Add more discussion of opt-in versus opt-out: what real choices are possible to allow Smart Grid functioning and what is not?

Work Going Forward

- Expand upon data collection endpoints/paths (e.g., private internetworks, storage media devices, etc.) that will be part of the Smart Grid
- Recommend training activities and awareness communications for the public & Smart Grid entities
- Discuss possibilities for certifying Smart Grid entities, devices, software, etc. as being privacy friendly and the associated metrics

Work Going Forward

- Expand upon PEV issues
- Discuss National Strategy for Trusted IDs in Cyber Space (NSTIC) impact on privacy in the Smart Grid
- Expand upon Internet- and wireless-related issues
- Others yet to be identified; going through methodical process to try and identify all possibilities



From

http://selecttelde11.blogspot.com/2009_09_01_archive.html

Sept 22 2010

Questions?



To get involved contact:

- ❑ CSWG Privacy Subgroup Lead: Rebecca Herold (rebeccaherold@rebeccaherold.com)



- ❑ NIST Point of Contact: Tanya Brewer (tanya.brewer@nist.gov)

Twiki: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy>