Title
Privacy Considerations in Demand Response Energy Systems

Permalink
https://escholarship.org/uc/item/9589w6h4

Author
Mulligan, Deirdre K.

Publication Date
2006
Privacy Considerations in Demand Response Energy Systems

Deirdre K. Mulligan, UCB
dmulligan@law.berkeley.edu
Research Summary

**Goal:** Identify Privacy and Security Issues in implementation of DRE and propose relevant technology and policy solutions.

**Research Agenda:**

- ✓ Meet with technologists to understand current and planned systems, and assess the architectural and data needs of the system.
- ✓ Research existing federal and state privacy law:
- ✓ Meet with utilities and other developers of demand response infrastructure to understand data practices and policies controlling data use
- ✓ Meet with law enforcement to learn about their demand for and practices regarding utility data.
What is demand response?

- Step 1: advanced metering
- Step 2: time-varying energy rates
  - Voluntary manual response to changes in price
- Step 3: new technology elements
  - Voluntary automatic response to changing tariffs OR
  - Forced response to signal from utility
- Step 4: the Wired House
Theoretical Implementation Models

• Centralized Implementation
  – Communication to utility through one-way collector network
  – Data concentrator at utility
  – Load-control through broadcast network

• Distributed Implementation
  – Intelligent portal on consumer premises
  – Communications to and from utility go through portal
  – Portal controls load based on pre-configuration by consumer

• Hybrid Implementation
  – Third-party data and network management services
CA Public Utilities Privacy Laws

• Different amounts of protection for utility records and personal information
  – Written consent required for release of personal data: billing, credit, usage
  – Utility records may be released in certain circumstances if customer not identified
  – Exceptions for law enforcement

• More extensive protection in telecommunications:
  – Calling patterns, service choices, individual or aggregated demographic data may not be released without written consent.
Privacy Laws regarding other parties

Third Party Service Provider / Data Manager
• Data security & data handling practices promulgated from utility to third party through contract and audit

Law Enforcement
• Relatively stringent rules for tech-assisted criminal investigation (Kyllo)
• Relatively easy access to utility records
• New infrastructure potentially creates new data and new points for law enforcement to obtain it:
  – Easier access to business records held by third parties?
  – Access to unfiltered sensor network data?
Unauthorized Access to Computer Systems

• Federal computer fraud laws apply to intentional, unauthorized access to “a computer” which “obtains … information”
  – What elements in DR system count as “computers”?
  – Does lack of access-control imply authorization?
• Federal wiretap laws apply to interception of “electronic communications”
• CA penal code defines expansive set of unauthorized computer use offenses
  – Access or use of data or services, provision or assisting provision of means of access
Privacy under California Constitution

- California Courts have determined that consumers do have a reasonable expectation of privacy in PERSONAL information under some circumstances
- Themes
  - Virtual current biography
  - Disclosure not volitional
- *People v. Chapman*, 36 Cal. 3d 98 (1984) (customer who paid to keep her name, phone number, and address unlisted in telephone directories had a reasonable expectation of privacy in that data, and so a warrant was required to obtain that data from the telephone company)
Mapping Legal Rules Onto Demand Response Architectures
Expected Implementation: Meters & In-home elements

• **Short term**
  – Meters with limited storage and processing capability
  – All data collected and processed at utility

• **Medium term**
  – Meters with increasing storage and processing capability
  – Two-way communication from utility to meter, smart thermostat

• **Long term**
  – Network of in-home sensors communicating with meter, smart thermostat, other in-home smart appliances
  – Significant process capability and intelligence inside the home
Legal / Privacy Issues: Meters & In-home elements

- Consumer has high expectation of privacy for in-home data
  - Consumer sentiment and law both favor privacy of in-home activities
  - Potential of in-home network to expose information
- With increasing intelligence in-home, more potential for on-site processing need for secure appliance
  - Meter computing bill?
- Security & encryption of in-home transmissions
  - In-home sensor data & transmissions may expose information on in-home activity
Expected implementation: Data Transmission to Utility

- **Short term**
  - Substation scheduling collection of hourly data from individual meters
  - Data routed to utility for aggregation and processing
  - Segments of transmission path outsourced
  - Use of public/private wireless transmission systems
  - Encryption on selected segments on cost-benefit basis

- **Longer term**
  - Move to broadband over powerline, provision of additional services with BPL
  - Utility ownership of key hardware
Legal/Privacy Issues: Data Transmission to Utility

• Currently, meter data security based on proprietary data format rather than encryption

• Unclear levels of privacy protection when customer data passes from utility to third party
  – Security & data handling requirements enforced by utility through contract and audit
  – Unclear whether law enforcement can access more easily
  – If utility owns system existing privacy and data handling requirements apply

• Over time, utility may start to look like a telecommunications provider
  – Telecom corporation responsible for ensuring privacy of communications over its telephone system
Expected Implementation: Data Processing and Use

- **Short term**
  - Central collection and storage of hourly data from advanced meters
  - Aggregation of data for billing
  - Real time access to data by customer service
  - Data feedback to customer for education purposes

- **Longer term**
  - Upgrade of legacy systems to adapt to increased data set
  - Data mining
  - Research looking for ways to use hourly data to optimize systems, reduce operating costs, improve load planning
  - Storage of 7 years worth of hourly data
Legal/Privacy Issues: Data Processing and Use

• **Introduction of Independent Third-party processors**
  – Outside existing regulatory privacy framework
  – Sale or disclosure of data in “business records”
  – Unregulated, unrestricted access to real-time information

• **Data at utility may reveal information on in-home activity**
  – Potential to represent/infer in-home activities from remotely stored data

• **Mining of hourly data may expose information on in-home activity**
  – Need to balance utility system optimization via datamining and customer privacy

• **Over time, utility may know a lot about occupants**
  – Uncertain what can be gleaned through consumption patterns, service program choices and other information
  – Given heightened knowledge may become more desirable source of information
Specific Architectural Choices to Promote Privacy

- Identify precise data requirements for utility sub-systems (e.g., billing)
  - Create separate pathways for systems that require identifiable data
- Minimize amount of raw usage data that enters external networks
  - Use in-home processing capability
- Minimize granularity of information transmitted, at every step
- Focus on security
  - No security = no privacy
Goals

1. Keep data in-home as much as possible, protect to the extent possible when data leaves the home
   • Meter-computing-bill an example
   • Split data paths for billing and other functions
   • Aggregation / anonymization of high granularity data
   • Security of data in the home also an issue

2. Protect privacy prospectively, through design
   • Hard (technology) v. soft (legal) protections
   • Architectural choices will constrain subsequent policy choices
   • Policy choices are “hardened” when incorporated in architectural design

3. Ensure that rules and regulations respond to technological developments
   • Strong privacy protections should travel with the data
   • May need to heighten standards if data becomes more revealing
Recommendations: security

- Encryption is recommended over manufacturers’ proprietary formats for securing data over the entire transmission path, from meter to utility.
- Designers should adhere to published, well-studied, and where possible, provably secure standards.
- Authentication should be used for all data.
- Spread-spectrum radios should be used if feasible.
- A single-hop network should be used if possible for in-home sensor networks.
Recommendations: systems development

• Access to hourly customer usage data should be limited within the utility.
• Separate data pathways should be built into the system.
• In-home processing capability should be developed to enable the performance of necessary energy-related functions in-home: energy monitoring, demand response control, self-education, and billing.
• Smart appliances and BPL systems for the home should be designed to protect customers’ reasonable expectations of privacy in activities and preferences.
Recommendations: regulation

• Data privacy and business record handling rules must apply uniformly to data held by utilities AND 3d parties.
• CPUC should set guidelines as to how much data should be stored for purposes of customer service and other functions.
• Data-mining of hourly usage data should be monitored and regulated.
• Law enforcement access to utility records should require a warrant.
• Services provided via broadband over powerline (BPL) should be subject to stricter telecommunications laws.
• Collection of data from in-home smart appliances, sensors, smart thermostats should be prohibited.
Status Quo, Technology, & Law

“reasonable expectation of privacy”

dog sniffing
aerial photography

thermal imaging
Future work

✓ What can sensor data reveal about in-home activities?
✓ Seek out collaborations to implement recommendations.
Legal/Privacy Team

Deirdre K. Mulligan, Director SLTPPC, Clinical Professor of Law
Jack I. Lerner, Clinic Fellow, SLTPPC

Clinic Student Interns:
Erin Jones Ph.D, Boalt (Law)
Jen King, SIMS Masters Program
Caitlin Sislin, Boalt (Law)
Bethelwel Wilson, Boalt (Law)
Joseph Lorenzo Hall, SIMS Ph.D