

Privacy and the Law in Demand Response Energy Systems

**Deirdre K. Mulligan, Jack I. Lerner,
Erin Jones, Jen King, Caitlin Sislin, Bethelwel Wilson, Joseph Hall
Samuelson Law, Technology & Public Policy Clinic**

www.samuelsonclinic.org

University of California, Berkeley

Agenda

- What is demand response?
- Goals of Legal/Privacy Team
- General Principles of Technology & Privacy
- Legal Landscape
- Mapping Legal Rules Onto Demand Response Architectures

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

Background

- Response to California Energy Crisis 2000-01
 - CEC & CPUC Roles
 - PIER
- Statewide Pricing Pilot 2003-04
- Current CPUC proceedings on deployment of advanced metering and demand response
- (Federal) Energy Policy Act of 2005
- California Proposition 80

Legal/Privacy Team Goals

- ✓ 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:
 - expectations in home versus business records
 - regulations on use and disclosure of utility records
- ✓ 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.



General Principles of Technology & Privacy



“...how, when, and at what level does privacy matter?”

- Legal context and social context are ***both*** important
- Expectations of privacy are shaped by what is technically possible, what is technically possible in turn informs a court’s analysis of ***reasonableness***

Status Quo, Technology, & Law

“reasonable expectation of privacy”



dog sniffing
aerial photography

thermal imaging

Pot diaries

- U.S. v. Starkweather (9th Cir. 1992)
“The public awareness that such records are routinely maintained...negate[s] any constitutionally sufficient expectation of privacy...”
- *Kyllo v. U.S.* (2001)
“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 -- at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the 4th A was adopted.”

Lessons Learned

- A little recording can mean a lot:
 - Generates records held by others
- Location matters:
 - Imperceptible without trespass or in plain view?
 - Home versus public street
 - Is only rendered perceptible by technology?
- Government use of precise, accurate technologies with low false positives may be **outside** the 4th A
- Use of “Police-Only” technology is unreasonable, but use of readily available technology may not be



Legal Landscape

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 means new access points for law enforcement to obtain customer data:
 - Easier access to business records held by third parties?
 - Access to unfiltered sensor network data?
 - Where else might police access information?

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

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

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
 - Highest legal protection for this data through property and privacy law
 - Consumer preference to keep data in-home
 - Potential of network to expose information to others without trespass
- With increasing intelligence in-home, more potential for on-site processing,
 - 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
 - Customer preference for utility ownership of system so privacy and data handling requirements clear
- **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


- **Possible threats to privacy**
 - Sale or disclosure of data in “business records”
 - Unregulated, unrestricted access to real-time information
- **Mining of hourly data may expose information on in-home activity**
 - Explore aggregation, anonymization
 - Use of in-home processing capability to reduce exposure
 - Need to balance utility system optimization via data mining and customer privacy
- **Access to in-home sensor data may expose information on in-home activity**
- **Over time, utility may start to look like a telecommunications provider**
 - Disclosure restrictions on personal calling patterns, service program choices, and individual or aggregated demographic 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 incorporate privacy and technological developments as they evolve**
 - Strong privacy protections should travel with the data



"It would be foolish to contend that the degree of privacy secured to citizens by the 4th A has been entirely unaffected by the advance of technology...the question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."

-- U.S. Supreme Court, *Kyllo*

Recommendations: security

- Encryption is recommended over manufacturers' proprietary formats for securing data over the entire transmission path, from meter to utility.
- We recommend that designers adhere to published, well-studied, and where possible, provably secure standards.
- We recommend the use of authentication for all data.
- We recommend that spread-spectrum radios be used if feasible.
- We recommend that a single-hop network be used if possible for 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 the a customer's reasonable expectation of privacy in his activities and preferences, and CEC regulation should enforce this principle.

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.



Summary: Legal/Privacy Next Steps

- ✓ Learn more about what can be learned from data mining of sensor data
- ✓ Looking for collaborations

Legal/Privacy Team

Deirdre K. Mulligan, Director SLTPPC, Acting
Clinical Professor of Law

Jack I. Lerner, Clinical Fellow, SLTPPC

Erin Jones, Clinic Summer Intern SLTPPC

Jen King, Clinic Summer Intern SLTPPC, SIMS
Masters Program

Caitlin Sislin, Clinic Student Intern SLTPPC

Bethelwel Wilson, Clinic Student Intern SLTPPC

Joseph Lorenzo Hall, Clinic Student Intern
SLTPPC, SIMS Ph.D Program