Privacy and the Law in Demand Response Energy Systems

Deirdre K. Mulligan, Jack I. Lerner,
Caitlin Sislin, Bethelwel Wilson, Joseph Lorenzo Hall, Erin Jones, Jen King,
Samuelson Law, Technology & Public Policy Clinic
www.samuelsonclinic.org
University of California, Berkeley

Agenda

- Review Goals of Legal/Privacy Team
- Technology & Privacy – General Principles
- Current Project – Areas of Examination
- Questions to Ask
- Mapping Legal Rules Onto System Architecture
- Conclusion

Legal/Privacy Team Goals

- ✓ Meet with technologists, read literature, understand current and planned systems to assess the architectural and data needs of the system.
- ✓ Research existing federal and state law with respect to: privacy expectations in home versus business records; state regulations on use and disclosure of utility records
- Meet with users of ESP data (utility, regulator, law enforcement) to understand/survey institutional data practices and policies controlling data use

"…how, when, and at what level does privacy matter?"

- Importance of legal context as well as social context
- Expectations of privacy are shaped by what is technically possible, technical possibility in turn informs courts' analysis of reasonableness

Relation between technology and privacy

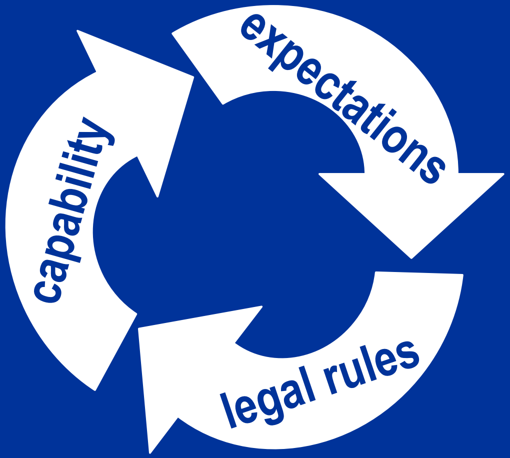
- **Micro level** – focus on empowering individuals – information and tools to effectuate privacy in various contexts

- **Macro level** – what kind of world do we want to live in

"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*

Status Quo, Technology, & Law



"reasonable expectation of privacy"

dog sniff, aerial photography

Thermal imaging

Distinctions

Is it sensed or recorded?

- Activity that generates records held by others
- Activity that is imperceptible without trespass
- Activity that can be perceived (sensed) from outside, “Plain view”
- Activity that is rendered perceptible by technology

Where is the activity taking place?

- home versus public street?

What is sensed?

- Just illegal activity, contraband?
- Mix of legal and illegal activities?

Pot diaries

- *Starkweather*

  “The public awareness that such records are routinely maintained…negate[s] any constitutionally sufficient expectation of privacy…”

- *Kyllo*

  "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."

- *Caballes*

  “Well trained narcotics detection dog, one that does not expose non-contraband items that otherwise would remain hidden from public view during a lawful traffic stop generaly does not implicate legitimate privacy interests.”

Lessons

- A little recording can mean a lot
- Location matters (people, activity, data)
- Use of well trained technologies (precise and accurate) by government with low false positives are outside the 4th A because they are not searches (at least in some instances)
- "Police only" technology is unreasonable invasion, readily available technology maybe not

Current Project:

Demand Response Energy System

Three Areas of Examination

- Sensor networks within home
  - High expectation of privacy; legal protections through property and privacy; potential of network to expose information to others without trespass
- Flow of data to utility
  - Change in form of data and change in data capture may be significant for privacy; potential to expose increasing amounts of private activity to third parties; relationship between strong privacy property rules protecting home and weaker rules in data maintained by utility
- Gateway device
  - Software? Service? Who owns and controls? Implications for privacy

Three Implementation Scenarios

- Centralized Implementation
  - Data concentrator located on utility premises
  - Control of load through a broadcast network
  - Communications to utility through one-way collector network
- Distributed Implementation
  - Intelligent portal located on consumer premises
  - Portal controls load based on pre-configuration by consumer
  - All communications to and from utility go through the portal
  - Separate commercial WAN used for communications
- Hybrid Implementation
  - Third-party data and network management services

Overview of Use and Disclosure in Three Implementation Scenarios

- Possible threats to privacy
  - Anti-competitive use of consumer data
  - Sale and disclosure of consumer data in “business records”
  - Unregulated, unrestricted access to real-time information

- Entities we’re concerned about having access to data
  - Public utilities
  - Private third parties
  - Law enforcement

Questions to Ask

- Meter and Storage:
  - Where, at what level of granularity, and for how long data is captured, transmitted, and stored?
- What are the conditions for:
  - Reuse?
  - Access?
- Access to what?

Public Utilities

- Current privacy protections for utility records
  - Business records: some confidentiality protections, minimal legal process protections
  - Personal information protections

- Designers ought to consider these privacy principles
  - Where is the intelligence, at home or at the utility?
  - How much data must be reported, full disclosure to concentrator or calibrated disclosure from portal?
  - Where is data stored: home/ utility/ third party?

Third Party Data Managers

- Generally, fewer protections apply
- Designers ought to consider
  - At what level of granularity does the information leave the home (where is the intelligence)?
  - How will the communication channels work: full access, or separate pathways requiring formal audit policies?

Law enforcement access

- Current rules for tech-assisted criminal investigation: relatively stringent (*Kyllo*)
- Current rules for law enforcement access to utility records: lax
- How to reconcile the two?
  - Will unfiltered sensor network data be accessible to law enforcement?
  - Spectrum of access:

    monthly utility bills → sensor networks
- Designers should consider:
  - *Where do police access information?*
  - *What kind of information is available at that point?*

Mapping Legal Rules onto System Architecture

Goals

- Keeping data in the home to the extent possible, and protecting it to the extent possible when it does leave the home
- Demonstrating where security concerns aren’t coextensive with privacy concerns:

  Once access is granted, what protections govern the process and aftermath of access?
- Hard (technology) v. soft (legal) protections: we seek to protect privacy prospectively, in design

Elements Analyzed

- Drawn from reference design: structural and functional elements, combined
  - Resources
  - Consumer Appliances
  - Utility Applications
  - Wide Area Network

Resources

- Resources are *information* and *storage*
- Goals: define purposes for data use, limit data disclosure to support only those purposes

Anonymity → *Pseudonymity* → *Nymity*

Consumer Appliances

- Appliances are
  - Internal: sensor network, thermostat
  - Internal/ external: meter, portal/ concentrator/ gateway
- Goals: Keeping data management functions at home (prevent creation of business records), minimizing data storage and maximize audit controls

Utility Applications

- Goal: ensure that *ever-evolving* rules for information processing/ transfer always incorporate privacy
- Applications allow utilities to access meter data to fulfill specific functions:
  - Load forecasting and scheduling coordination
  - Marketing and rate management
  - Assets and service management
  - Billing systems
  - Settlement
  - Customer Care
- Designers ought to consider
  - Identifying data requirements exactly
  - Creating separate pathways for billing/ pricing
  - Interoperability
  - Crisis management

Wide Area Network

- Goals:
  - protect raw usage data from entering external networks as much as possible
  - at every step, minimize granularity of information transmitted
- Unclear whether state and federal law provides any protections to this WAN. . .

Summary:
Value-Driven Architecture

- Architectural choices constrain policy
- Policy choices if considered in architectural design can be “hardened”
- Need to identify policy goals – privacy, security, other – in order to engage in iterative process during design phase
- Must understand stakeholder needs, technology, law, and have clear objectives

Summary:
Legal/Privacy Next Steps

- ✓ Meet with technologists, read literature, understand current and planned systems to assess the architectural and data needs of the system.
- ✓ Research existing federal and state law with respect to: privacy expectations in home versus business records; state regulations on use and disclosure of utility records
- Meet with users of ESP data (utility, regulator, law enforcement) to understand/survey institutional data practices and policies controlling data use

Legal/Privacy Team

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

Jack I. Lerner, Clinical Fellow, SLTPPC

Caitlin Sislin, Clinic Student Intern SLTPPC

Bethelwel Wilson, Clinic Student Intern SLTPPC

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

Erin Jones, Clinic Summer Intern SLTPPC

Jen King, Clinic Summer Intern SLTPPC, SIMS Masters Program