The Spy Who Came In from the Refrigerator

Privacy Implications of Smart Meters

Cheryl Dancey Balough and
Richard C. Balough

Institute on the Law of Cyberspace
Austin, Texas – Winter 2011

What is the Smart Grid?

An electricity network that:

- Uses two-way digital communication
- Delivers electricity to consumers
- Delivers consumer energy-usage data to utility
- Enables utility to adjust consumer energy usage

Investment in Smart Grid

In October 2009, American Recovery and Reinvestment Act:

- Invested $3.4 billion in the smart grid
- Gave the money to 100+ entities in 42 states
- Allocated a large portion to smart meter projects

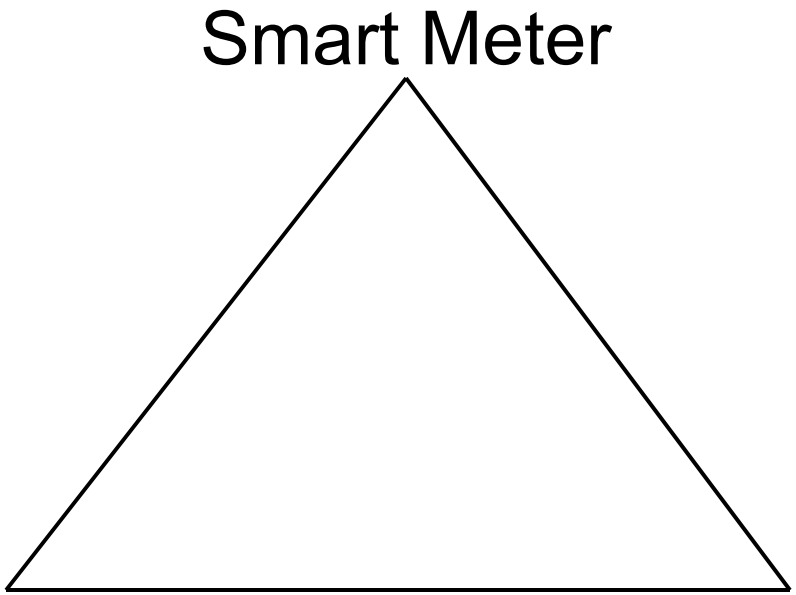
What Is a Smart Meter?

An advanced electrical meter that:

- Records energy usage in intervals of <1 hour
- Transmits that data at least daily to the utility
- Can receive instructions back from the utility

Purpose: Improve energy efficiency and reduce energy consumption

Roles of HAN and HEMS



Home Area Network
(connects energy-using devices to control device)

Home Energy Management System
(software that permits management of devices)

So What Is the Concern?

Key Questions

- What data can/will be captured?
- Who will have access to the data?
- What will be done with the data?

Privacy Impact Assessment

National Institute of Standards and Technology conducted a privacy assessment

- Issued draft report in September 2009
- Received 450 comments from 34 entities

What Is Fueling the Concerns?

1. Wealth of information that will be available
2. People need electricity → no viable options
3. Current laws do not adequately protect privacy

Wealth of Information Available

Information about what occurs inside the home

- By street address/unit
- By room
- By smart appliance
- By intelligent socket
- By electric vehicle's ID
- By 15-minute interval
- On real-time basis 24/7

How Information Is Available

Captured by smart meter and made available:

- Over utility or broadband wires
- On websites (utility or third party)
- On in-home display
- Via HAN Wi-Fi
- Via home energy management system (HEMS)

To Whom Is Information Available

- Electric utility
- Resident/unit owner?
- Third parties?
- Law enforcement?
- General public via inadvertent disclosure?

Resident/Owner Access

What happens in the following situations?

- Renter → to tenant or owner or both?
- Occupancy/owner moves → to subsequent tenant or owner?
- Condominium → to association or management?

Third Party Access

Which third parties have access

- Home energy management system suppliers?
  - Google PowerMeter
  - Microsoft Hohm
  - Cisco, Opower, General Electric, etc.
- Smart appliance manufacturers?
- Vendors of complementary devices/systems?
- Co-branders?
- Litigants?

Third Party Access

When will third parties have access

- By default?
- Based on contract language?
- Based on public utility commission (PUC) rules?
- Based on third party's own privacy policy?
- By subpoena?

One HEMS CEO: "The way we've anticipated dealing with [privacy concerns] is to opt-out customers who are unhappy with the analysis."

Law Enforcement Access

What will be required from law enforcement

- A request to the utility for data mining?
- Court order or search warrant?

Lack of Consumer Options

- Reliance on electricity
- PUC orders for 100% installation
- Click-through agreements with no opt-outs
- Lack of clarity as to who owns data

Current Laws Provide Inadequate Privacy Protection

- Limitations on tracking devices
- Privacy Act of 1974
- Wiretap Act
- Stored Communications Act
- Computer Fraud and Abuse Act
- Section 5 of Federal Trade Commission Act
- Fourth Amendment

Limitations on Tracking Devices

US DOJ: "The government is not required to use a warrant when it uses a tracking device"

SCOTUS: Warrantless monitoring of beeper *inside* a house violates the Fourth Amendment

Issue: Smart meters "track" energy usage inside the house, but data are by design conveyed outside the house on utility or broadband wires

Privacy Act of 1974

Requires use of “fair information practices”

BUT requirements do not have force of law against electric utilities or third parties

Wiretap Act

Intentional interception and disclosure of wire or electronic communications is a crime

EXCEPTION: if one of the parties (utility?) has given prior consent

EXCEPTION: for provider of communication service (utility?) “while engaged in an activity which is a necessary incident to the rendition of his service”

Stored Communications Act

Prohibits unlawful disclosure of stored communications by provider of electronic communications service to the public

BUT is an electric utility a provider of electronic communications service?

EXCEPTION: Provider can disclose contents if a "necessary incident to the rendition of the service"

Computer Fraud and Abuse Act

Intentional unauthorized access of protected computers, including those used in interstate commerce, is a crime

BUT access by third parties and law enforcement may be authorized

Section 5 of FTC Act

Prohibition on “unfair methods of competition in or affecting commerce” has been used to enforce companies’ stated privacy policies

BUT no federal law consistently requires privacy policies, fine print may contain exceptions, and consumers rarely read the policies

Fourth Amendment

Guarantees right to be free from unreasonable search and seizure

Reasonableness requires

- An actual, subjective expectation of privacy and
- An expectation society recognizes as reasonable

Limitations on Fourth Amendment

SCOTUS: "Intrusion into a constitutionally protected area constitutes a search . . . where . . . technology in question *is not in general public use*"

SCOTUS: "A person has no legitimate expectation of privacy in information that he voluntarily turns over to third parties"

Courts in 4 states have held that there is no reasonable expectation of privacy in energy consumption data contained in utility records

What Is Next?

Quick action is needed

- To protect consumers
  - Smart meters continue to be rolled out
  - Unprecedented threats to privacy inside home
- To ensure success of smart meters
  - Avoid horror stories on news of privacy invasions
  - Avoid backlash by PUCs and legislators

About the Presenters

Cheryl Dancey Balough focuses her practice on helping clients protect their ideas, their intellectual capital—including trademarks, copyrights, and trade secrets—and their privacy. She holds a JD from Chicago-Kent College of Law and an MBA from Northwestern University.

Richard C. Balough has been providing counsel to clients for over 30 years. In addition to serving as legal counsel for start-up, small and medium-sized companies and high technology companies, he has counseled city and county governments, as well as a consumer advocacy group. He holds a JD and LLMs in intellectual property law and information technology and privacy law from The John Marshall Law School.

Contact Information

Cheryl Dancey Balough
Richard C. Balough

BALOUGH LAW OFFICES, LLC
1 N. LaSalle Street, Suite 1910
Chicago, IL 60602
312.499.0000
www.balough.com

cbalough@balough.com
rbalough@balough.com