Smart Grid Privacy

NARUC Webinar

June 10, 2011

Deirdre K. Mulligan
Assistant Professor, School of Information and Director, Berkeley Center for Law and Technology

Jennifer M. Urban
Assistant Professor of Law and Director of the Sameuelson Law, Technology & Public Policy Clinic

University of California Berkeley Boalt Hall School of Law

Chuck Goldman, Staff Scientist
Electricity Markets and Policy Group
Lawrence Berkeley National Laboratory

This is another in a series of webinars created to support smart grid activities of the FERC/NARUC Smart Grid Collaborative. This webinar privacy issues principally regarding the collection and management of smart meter data. The presentation today will be provided by Deirdre Mulligan and Jennifer Urban. Both presenters are professors associated with the UC Berkeley Boalt Hall School of Law. Both presenters have been actively involved in smart grid metering and privacy proceedings.

Deirdre K. Mulligan (http://www.ischool.berkeley.edu/people/faculty/deirdremulligan) is Assistant Professor, School of Information and a Faculty Director of the Berkeley Center for Law and Technology, at the University of California Berkeley Boalt Hall School of Law. She was the founding director of the Samuelson Clinic from 2001-2008 and staff counsel at the Center for Democracy & Technology in Washington. Professor Mulligan has written several articles on smart grid and data privacy. She also completed two studies for the California Energy Commission, one addressing network security and advanced metering and the other privacy and smart grid information flows.

Jennifer M. Urban (http://www.law.berkeley.edu/php-programs/faculty/facultyProfile.php?facID=579) is Assistant Clinical Professor of Law and a Co-Director of the Samuelson Law, Technology & Public Policy Clinic at the University of California Berkeley Boalt Hall School of Law. She was the founding director of the USC Intellectual Property & Technology Law Clinic and prior to that an attorney with the Venture Law Group in Silicon Valley. Professor Urban has been active in the California Public Utility Commission Smart Grid Privacy proceeding, providing testimony as the attorney for the Center for Democracy & Technology.

Overview of Talk

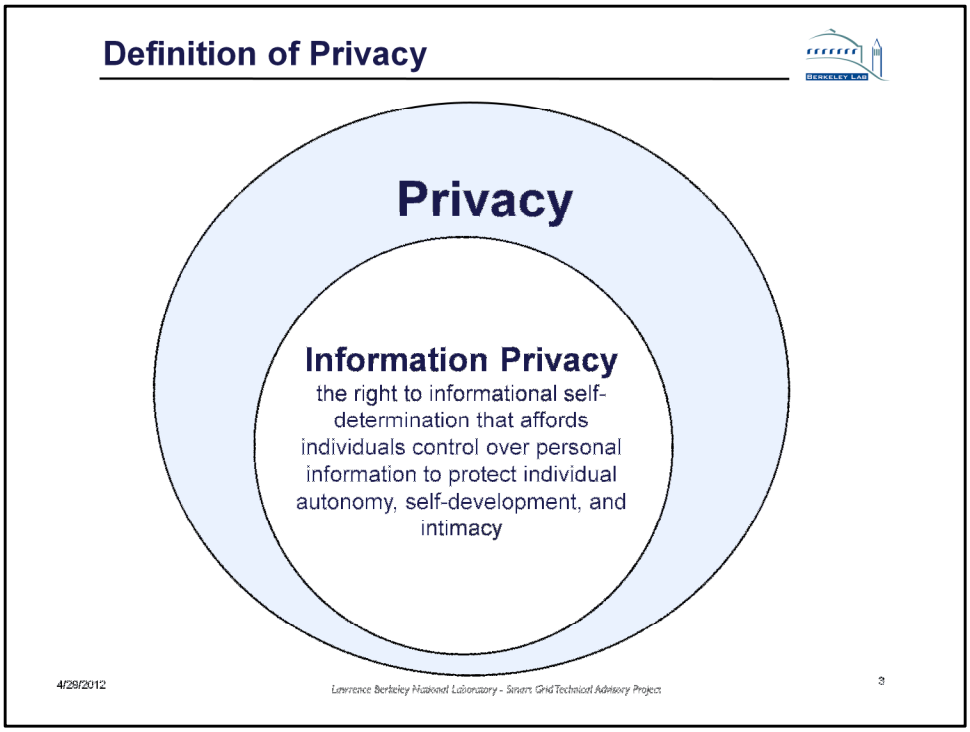
- Privacy: Information Privacy
- Smart Grid
  - New Information Flows
  - New Entities
  - Gaps in legal/regulatory framework
- CPUC decision
- Discussion

4/29/2012 Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project 2

The agenda for this webinar is divided into four segments.

The bulk of the material covered in today's webinar is available in a report funded by a California Energy Commission Public Interest Energy Research grant that was published in November 2010. A link to that report is provided in the reference slide at the end of this webinar presentation.

This webinar focuses on information privacy, information flows that will evolve from the smart grid, and legal and other gaps. This webinar will also review the recent California Public Utility Commission (CPUC) decision on privacy. The CPUC decision is the first of what we expect will be many regulatory commission decision addressing smart grid and meter data privacy. As the first state level decision to address the privacy issue it provides a good framework both for identifying the issues and potential solutions.



What is privacy. Is it really an ambiguous concept or can a more narrow definition be established.

For this webinar we are focusing on information privacy. It is a well defined concept that is specified in this definition. The primary context of information privacy is to provide individuals with control over personal information. This definition is well established both in the US and other parts of the world.

Fair Information Practices (FIP) Principles

§2. **Transparency** – *organizations should provide notice to individuals regarding their use, disclosure, and retention of personally identifiable information (PII).*

§3. **Purpose Specification** – *organizations should seek individual consent to collect, disclose, and retain PII.*

§4. **Individual Participation** – *organizations should articulate specific purposes for collecting PII, and specific uses for PII they collect.*

§5. **Data Minimization** – *organizations should collect only PII that is "directly relevant and necessary to accomplish the specified purpose(s)" and retain data no longer than necessary.*

§6. **Use & Disclosure Limitation**: *organizations should use PII only for the purposes stated in their notices.*

§7. **Data Quality & Integrity**: *organizations should keep PII accurate, relevant, timely, and complete.*

§8. **Data Security** – *organizations should implement adequate safeguards to protect against loss, unauthorized use, modification, and unintended disclosure.*

§9. **Accountability & Auditing** – *organizations should audit employees' and contractors' actual use of PII, to ensure compliance with the other FIPs.*

4/29/2012 *Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project* 4

This definition of privacy has been operationalized and implemented through a set of what is referred to as Fair Information Practices (FIP) and Principles.

The eight principles provided on this slide is only one version of FIPs that have been developed to address multiple sectors that go back to one of the original developments by the Department of Health Education and Welfare in the 1970's. At the international level FIPs are recognized by the Organization for Economic Cooperation and Development and in the European Union by State of Protection Directives.

In the US many statues refer to and reflect these principles. These FIPs are also referred to in the NIST security and privacy working group documents as well as the CPUC privacy decision.

Information Flows

- Source of Data
- Recipient
- Use
- Mechanism of transmission
- Nature of the data (explicit and implicit)

4/29/2012 Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project 5

Many of the slides that follow will concentrate on information flows, especially the new sources of data and devices that are expected to be introduced by the smart grid.

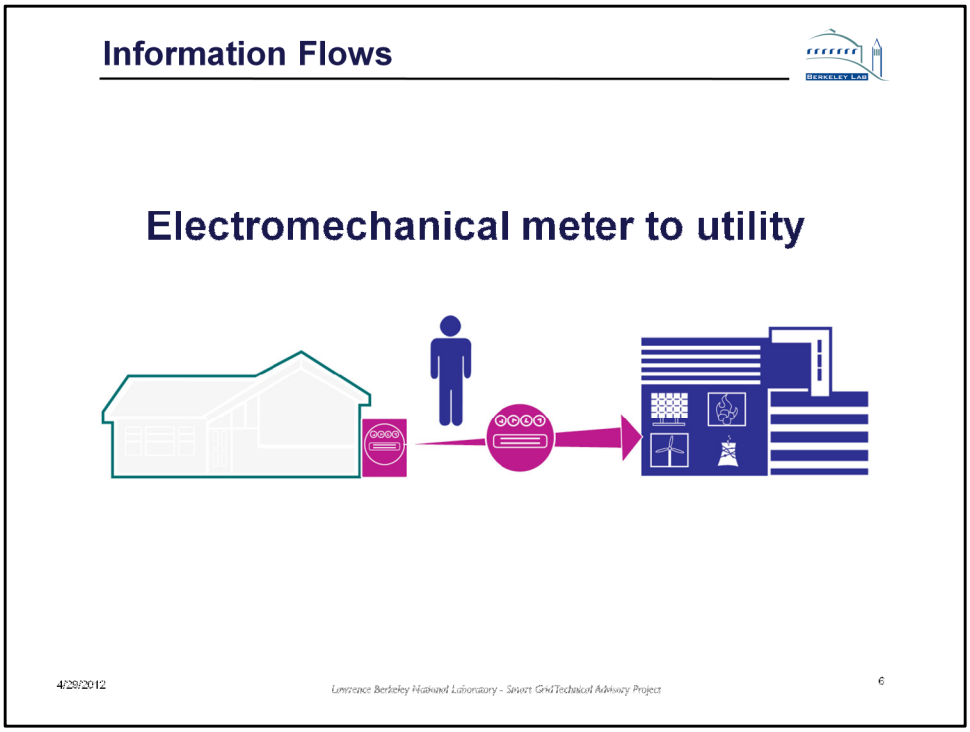
The smart grid may be viewed as an early instantiation of the Internet of 'things' where devices within the customer home will be individual addressable and designed to provide data and interact within the home and utility network.

There will be new recipients of this data that go beyond the utility.

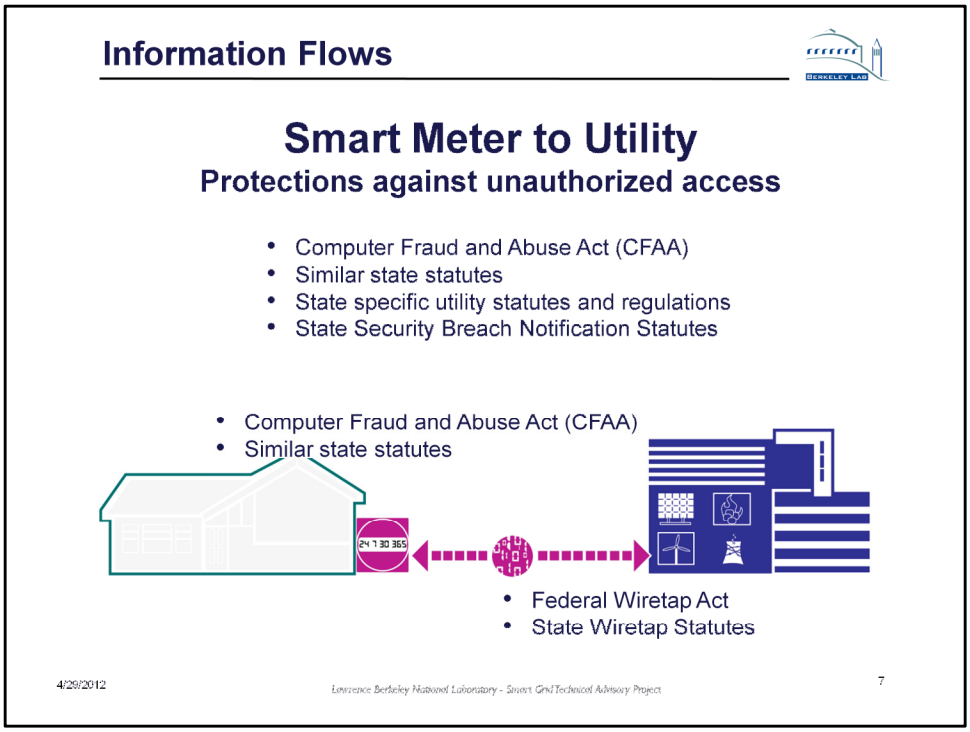
Uses of information will provide opportunities to make more and better uses of this data. However, there are also many other uses that may impact privacy.

Networking the home and grid will also impact the movement of data.

Finally, the nature of data is important. What can the data tell us at a meta level regarding energy use at a community as well as at the micro level regarding what this data can tell us for an individual customer or premise.



This graphic reflects the old world, where electro-mechanical meters require a person to physically visit (or come within close approximation) of each utility customer premise to read and then transmit meter readings back up to the utility.

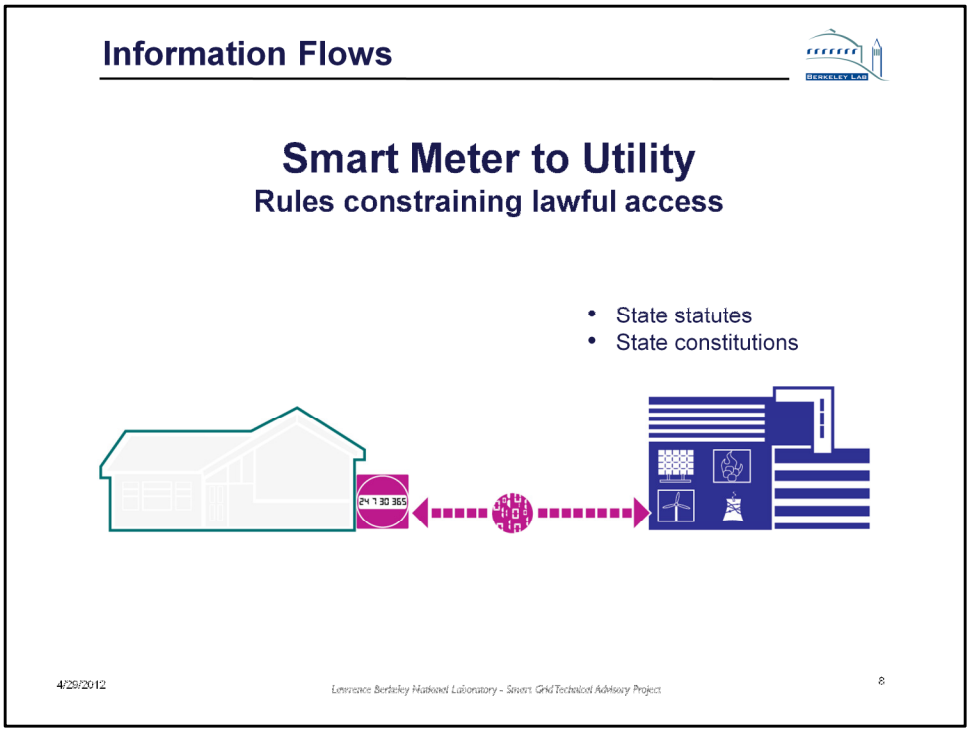


Protections against unauthorized access.

In the new smart grid world, meters include technology embedded with computing and communication capability that enables the collection, tracking, and periodic transmission of data back to the utility.

There are a host of protections to address authorized and unauthorized access, both of which may raise privacy concerns. There are a host of state statues and federal rules that already address privacy and security in the utility space regarding unauthorized access. At the meter, the Computer Fraud and Abuse Act and similar state statues that make it a criminal offense for people to access the information within those devices without authorization or to exceed authorization. Regarding the flow of information from the meter to the utility there are protections provided through the Federal Wiretap Act and state equivalents which make it a criminal offense to intercept data during the flow.

Finally back at the utility, protections are enabled by the Fraud and Abuse Act and similar state statutes. There are also individual state public utility acts that come into play. There are also notification statutes that create triggering events that require utility notify customers of breach events. In some cases encrypted information may be exempt from these notification statutes, which in an indirect way encourages companies that maintain customer account and other data to engage in data encryption and other security practices.



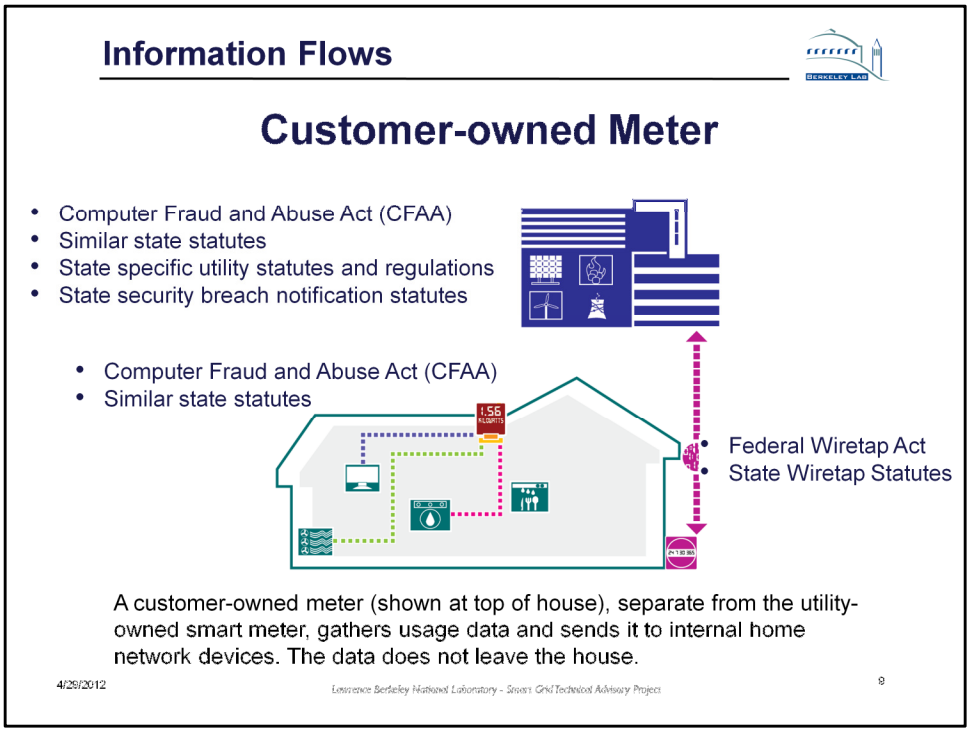
Rules Constraining Lawful Access.

One concern is regulatory gaps that may not sufficiently constrain illegal or unauthorized access to data. We are also concerned about situations that create a lack of parity due to the entrance of new players into the smart grid with respect to statues and constitutional provisions that limit lawful access to data.

Lawful access to data includes: (a) what are the procedural standards that regulate how data can be obtained, does it require court action, do you need to issue a subpena, and (b) substantive standards that consider relevance or is it provided under a clear and convincing evidentiary finding for law enforcement access to information. In addition what are the standards for third-party civil litigants or new business partners which may wan to share information.

For utilities there are state statues and public utility rules that govern how utilities store, use, and disclose data. These also frequently address how law enforcement gain access to data from public utilities.

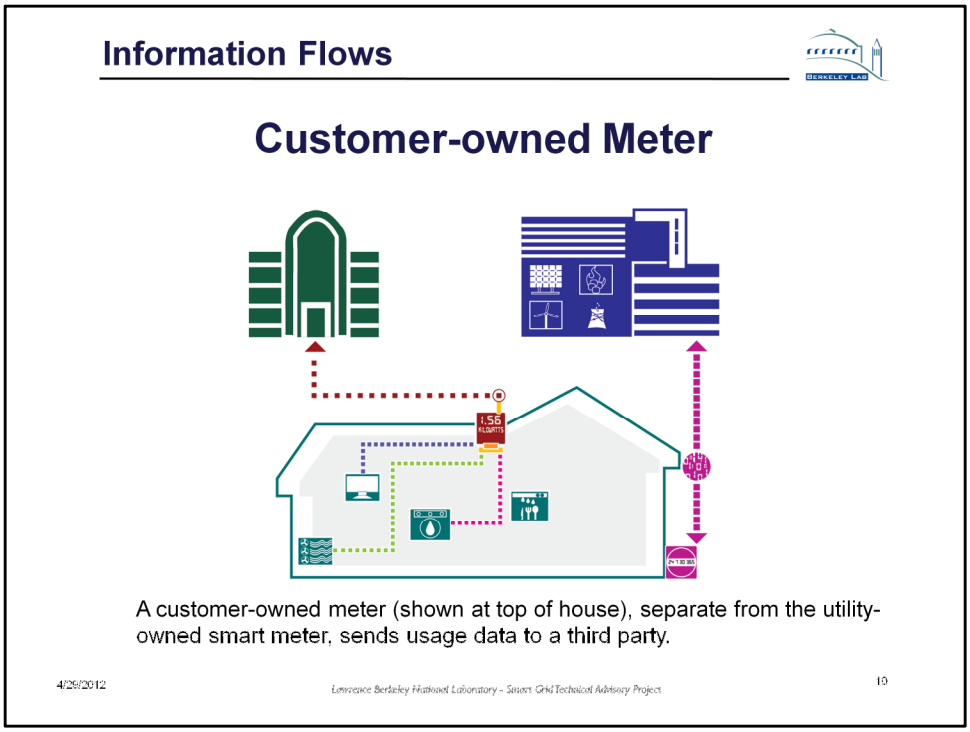
Many states have constitutional provision may provide a framework or may be interpreted to define specific rules for law enforcement access. These frameworks at the state level may or may not define the rules for third-party access to this data. Public utility rules that govern the extent to which utilities can disclose specific data about a particular account versus aggregate accounts are all rules that constrain lawful access, not unlawful access..



Customer Owned Meter

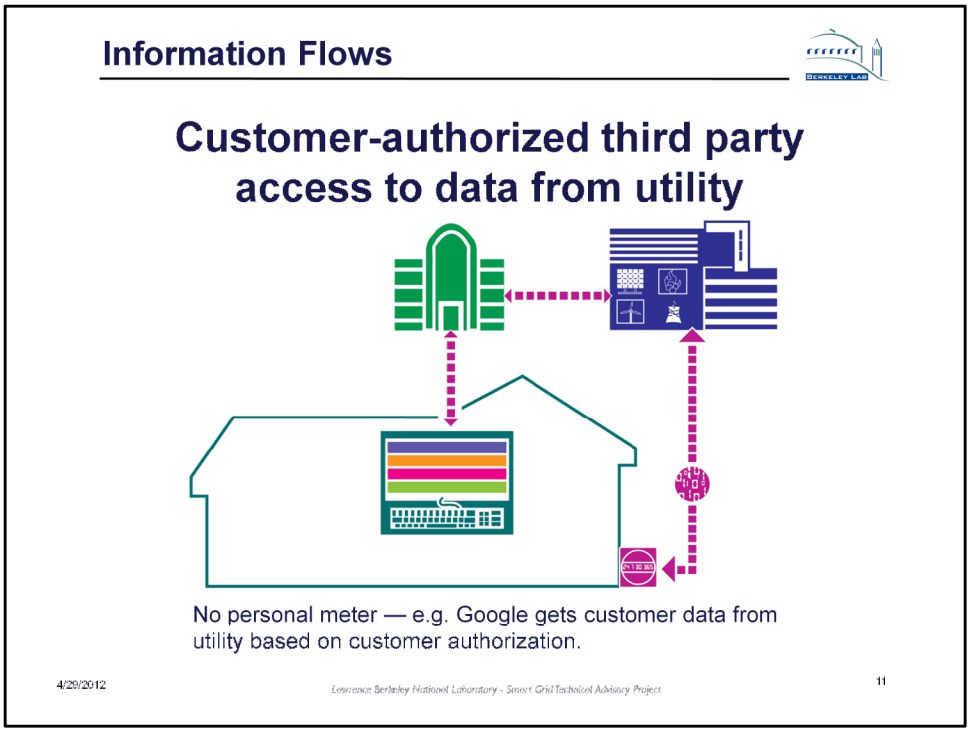
One of the new things being introduced by smart grid is the customer owned meter, in additional to the utility owned meter. The term customer owned meter is being used here in a general sense. This term could include something like a "TED" device that is wired into the customer service panel to provide access to information wirelessly to other customer owned devices. The same set of legal and illegal access statutes apply here. However, now we have data and identifiers relevant to specific devices, where in this case that information stay in the home. The flows of data within the home are covered by the Federal Wiretap Act . Retaining this information in the home means this information does not become a business record of a third-party which also means this information is still protected under the 4th Amendment protections.

Security of this information is also dependent upon whether this information is moved over a wired network or a wireless network restricted to operate only within the home. Wireless movement of this data over a public network may reduce privacy protections.



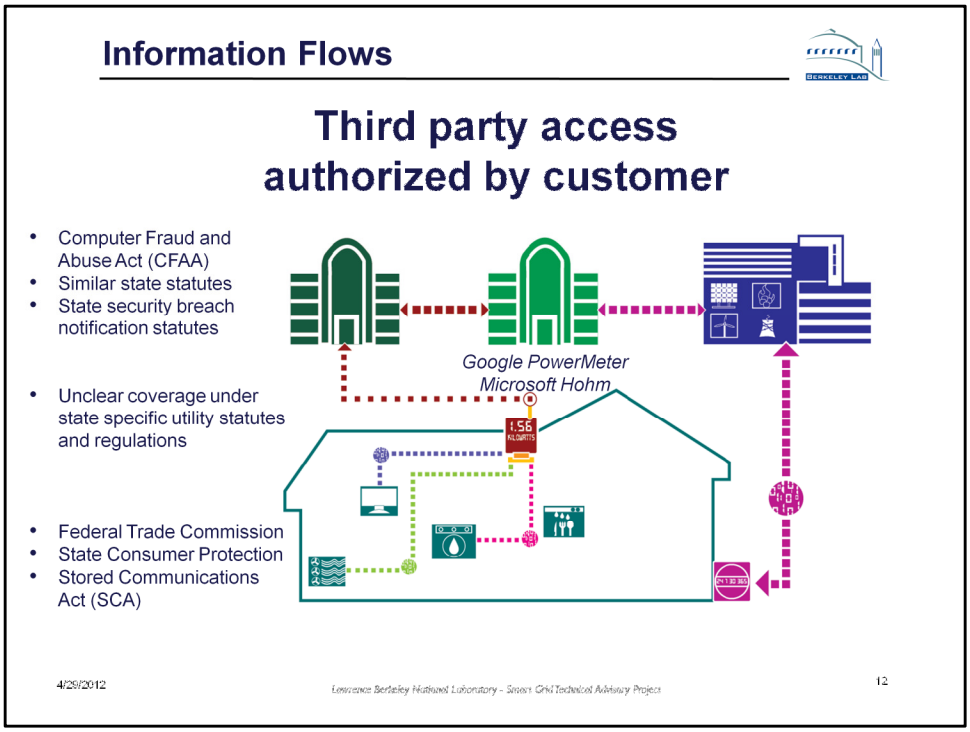
Customer Owned Meter

In this data flow there is a separate customer owned meter where the data flows out to a third-party, not to the utility. The next few slides will cover three different configurations or ways in which this customer owned meter data can flow between specific parties, each with slightly different legal and regulatory concerns.



<u>Customer Authorized Third-Party access to utility data</u>.

In this example there is no separate customer meter however there is an internal home area network. Customer usage data flows to the utility and independently the customer has authorized or provided permission to a third-party to access their data directly from the utility data.



<u>Third party access authorized by the customer</u>.

In this example the customer authorizes third-party access, however the data is coming both from the home through a separate metering infrastructure and from the utility.

In all of these options, the Computer Fraud and Abuse Act and similar state statutes to the extent we are dealing with third-party entrance into the smart grid are covered by state security breach statutes. The extent to which these third-party entities are covered under state specific utility statutes that provide privacy protections is unclear and will be have to be decided on a state-by-state basis.

Information flowing within the home that flows out of the home either through the customer owned meter or through the utility to third-party entities, there are state consumer protection laws and also potential protections that may be provided by the Federal Trade Commission. The FTC is looking at privacy protections and beginning to establish rules that obligates a standard of care. This may include putting programs in place to attend to security risks, stay updated on vulnerabilities, and provide mitigation .

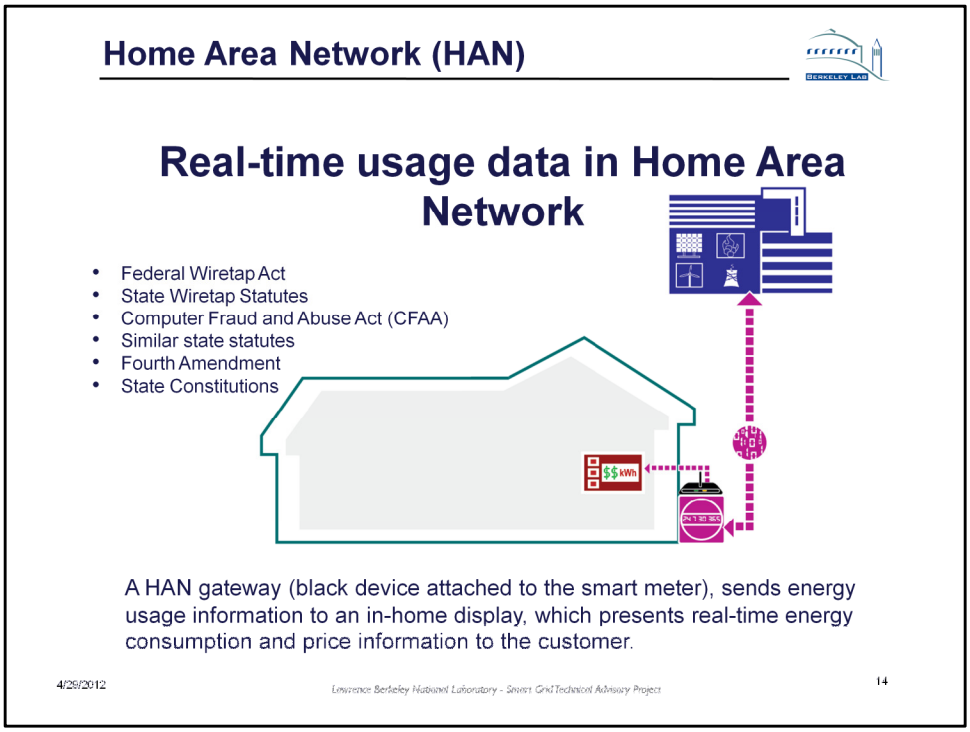
Finally, the Stored Communications Act (Federal) provides protections for access both against unauthorized access and authorized access to data stored in third-party sites.

Home Area Network (HAN)

- Privacy and Innovation
  - Tracking and Monitoring
  - Registration
  - Demand Response and Load Control
  - Pricing, Messaging, and Billing Information

4/29/2012 Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project 13

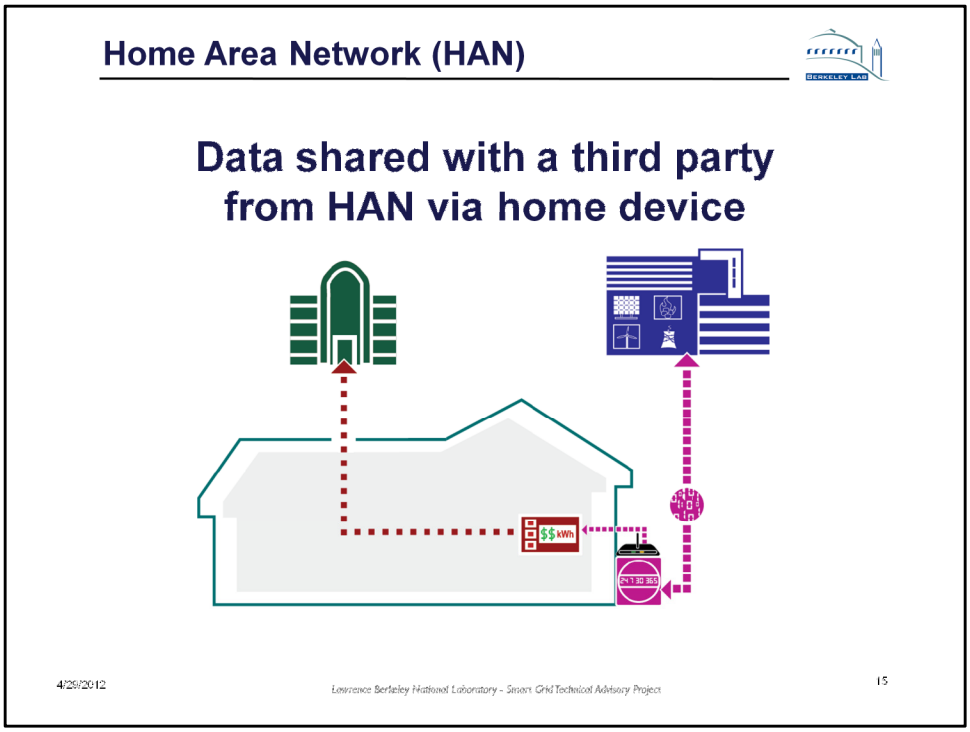
Home Area Network (HAN) – balancing privacy with innovation and competition



Home Area Networks (HAN)

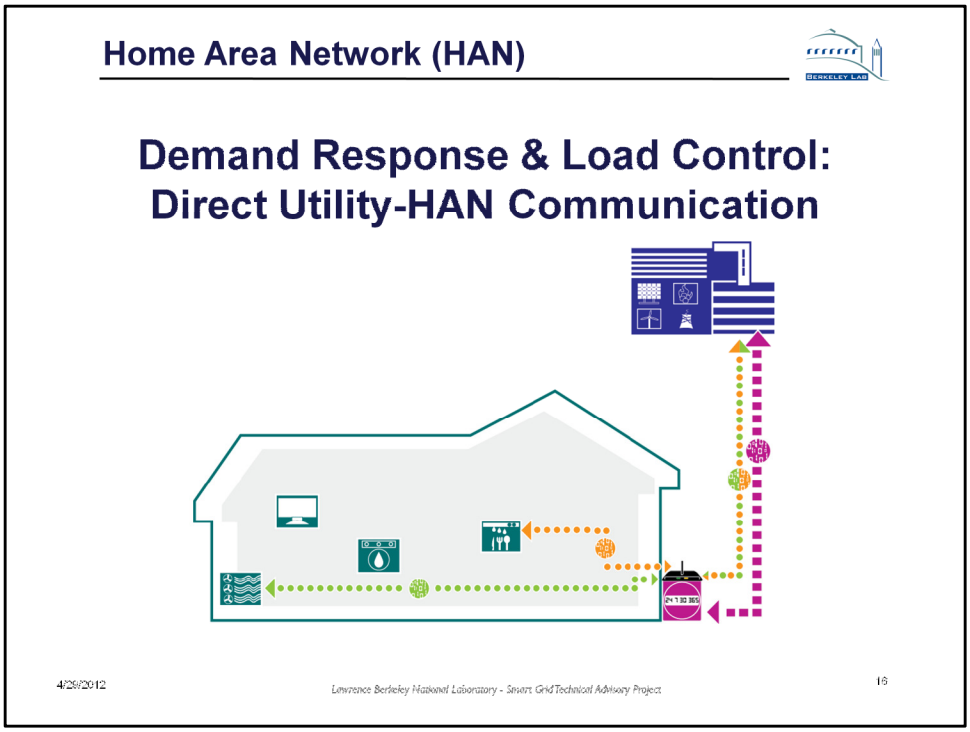
Tracking and Monitoring – the home is becoming populated by a number of smart devices that are interacting with a network. That network will use a gateway that acts to coordinate and manage these devices. Smart Meters may include a home area gateway designed and included in the meter. There is no reason why this gateway has to reside in the meter . The gateway is just an interface that is used to interface between the home devices and meter.

The gateway may provide the interface for managing price and other data passing to devices to regulate customer response. It may also be used to pass data from devices in the home back to the utility. Data that does not leave the home is covered by 4th Amendment protections against unauthorized access, however with data leaving the home and passing back to the utility the 4th Amendment has little relevance although these protections may change. There may be state constitutional protections to address this situation.



Home Area Networks (HAN)

Data Shared with a Third Party from a HAN - see slide #12.

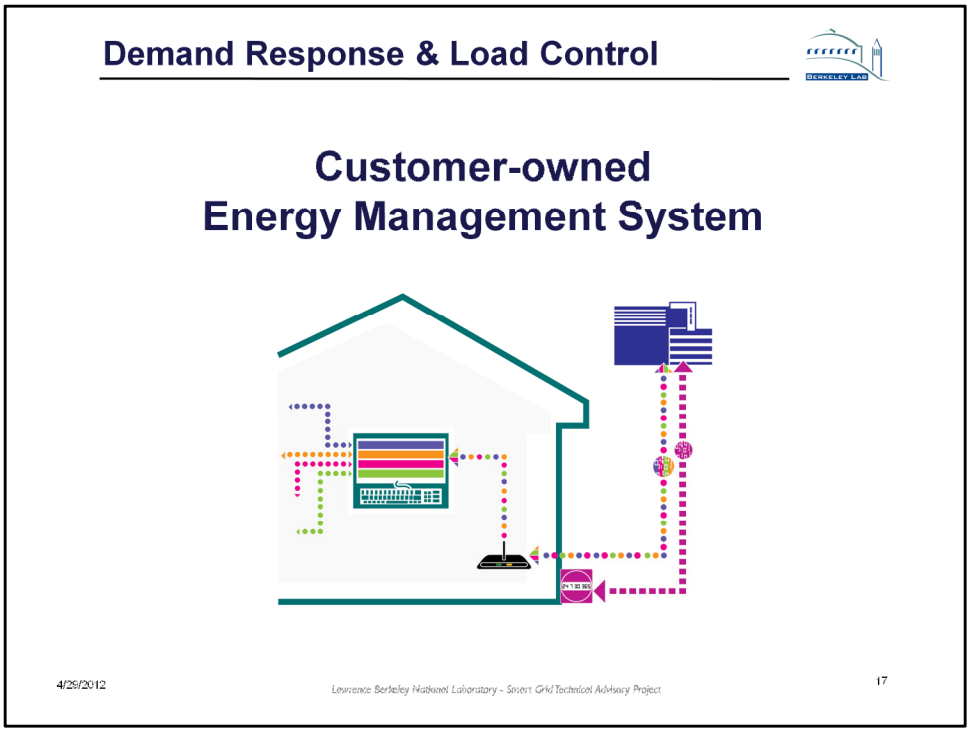


Home Area Networks (HAN)

Demand Response & Load Control: Direct Utility HAN Communication.

In this scenario the utility provides load control or pricing signals to the home through the meter, which passes this information to the HAN gateway to the customer energy management system/devices which control those devices based on customer decisions.

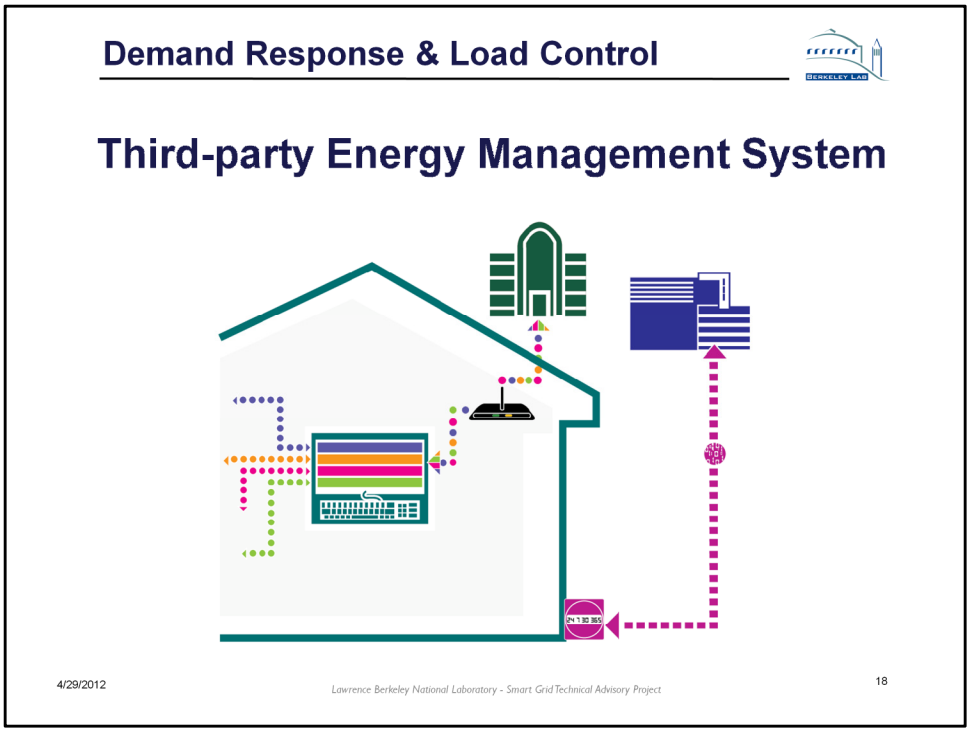
One option would be to provide a technical barrier around the home where all information about how the customer and devices respond is kept within the home. The decision regarding how the customer responds is shared with the utility based on meter data usage information, not specific information regarding particular premise devices.



Demand Response & Load Control:

Customer Owned Energy Management System

In this scenario a customer owned energy management system provides protection by shielding the devices and individual decisions from the interface with the meter.



Demand Response & Load Control

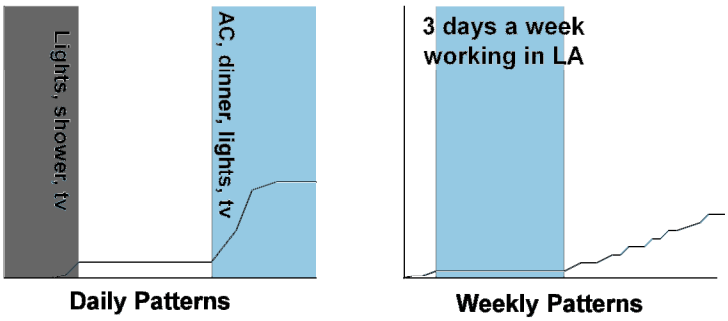
Third-Party Energy Management System.

In this scenario the utility is sending load control and pricing information into the home. The utility meter sends usage information back to the utility, however no customer device or specific decision information is provided back to the utility.

Where the customer uses a third-party energy management system, it may be sending information back to the third-party provider.

Interval Data

- 3000 data points per month for 15-minute intervals – vs. 1
- Virtual biography of household activity in near real-time
- Adding specific appliance data (e.g., smart dryers, PEVs) adds even more detail



Lawrence Berkeley National Laboratory - Smart Grid Technical Advisory Project

-Basic point - this data is not the same as it was before. 1 point of data a month is of a totally different character than is 3000 (every 15 minutes)
-More can be learned or inferred about the inhabitants of the home - when are they home, what are their occupancy patterns - this may be of interest to a variety of audiences

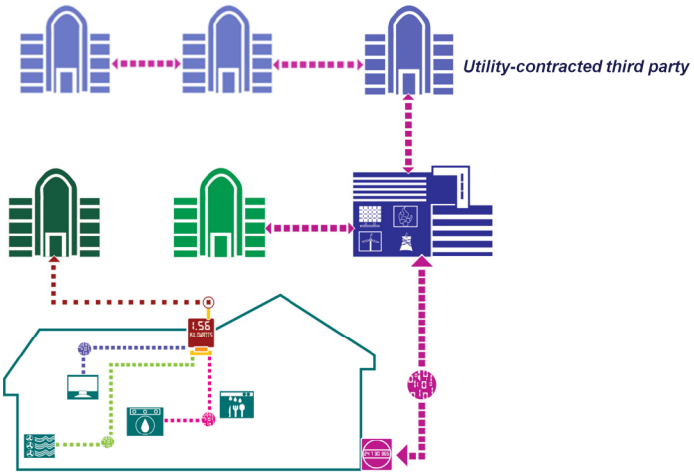
-Marketers - if you can determine particular things about inhabitants, then marketers may wish to buy data and mine it to sell to users with certain patterns
-Robbers - if you get your hands on data (especially in large amounts), can determine homes that have occupancy patterns making them easy to rob - data mining for targets
-Abusers/etc - may be able to determine activities remotely of a specific person, tell when is optimal time to harass them

-Advanced metering capabilities that are now being implemented will employ refurbished meters having a data collection module with hourly readings and transmission of raw data to the utility.75 Later meters may contain more internal processing and data storage capability. The data set the meter will send to the utility is expected to contain a unique meter identifier, a timestamp, hourly usage data, and some kind of time synchronization information.76

CPUC Proposed Decision
May, 2011

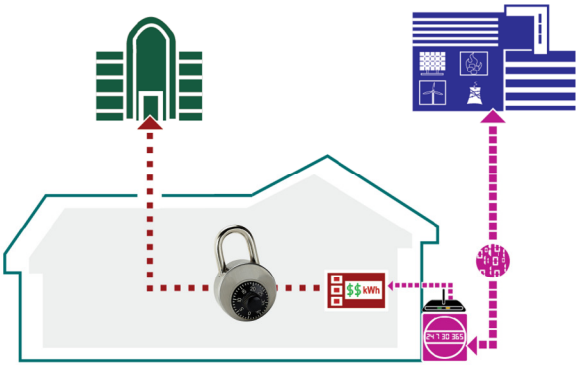
CPUC Decision

Data Flows



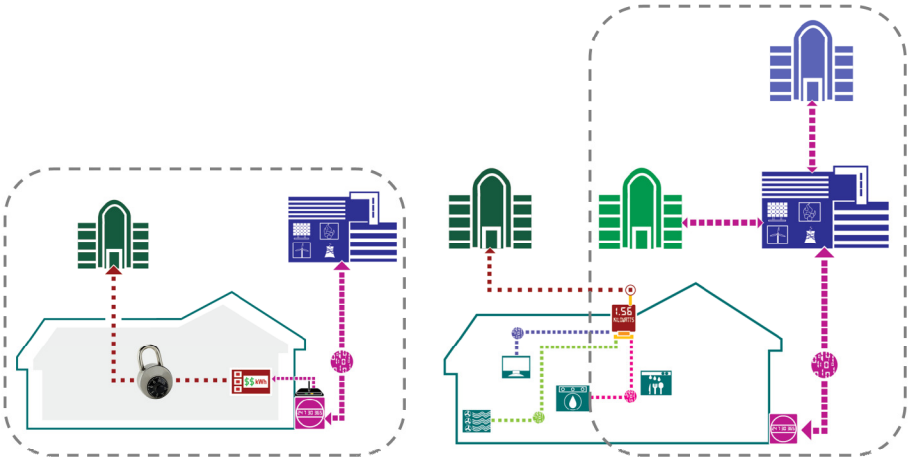
CPUC Decision

Data shared with a third party from HAN via "locked" device



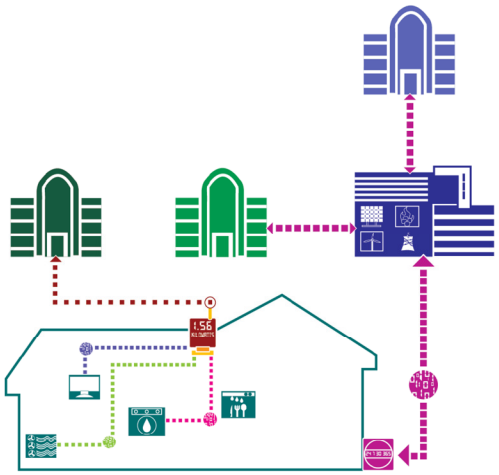
CPUC Decision

§1. Who Is Covered?



CPUC Decision

§1. Definitions



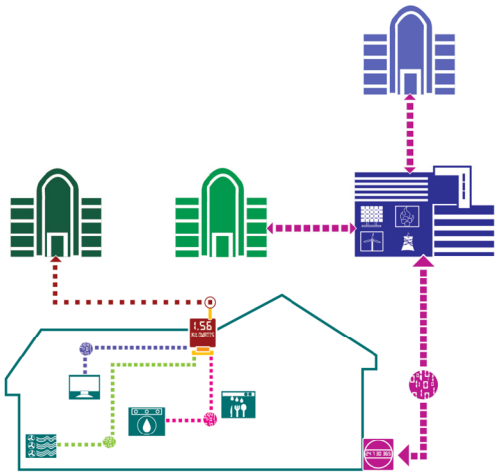
(a): **Covered Entity:** electrical corporations and third parties who obtain information via the utility or a "locked" device.

((b) **Customer**: Recipient of retail generation, distribution or transmission service (ongoing discussion re "entity").

(c): **Covered Information**: usage information obtained through AMI *if* it is associated with any information that can reasonably be used to identify a customer; does not cover information that cannot be reasonably identified or re-identified.

CPUC Decision

§2. Transparency

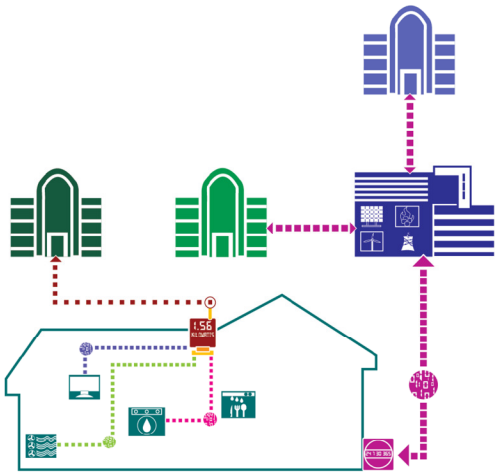


(a): Must provide customers with "clear, accurate, and specific notice regarding the collection, storage, use, and disclosure of covered information."

There are requirements for when notice must be provided and, notably, what must be included in the notice

CPUC Decision

§3. Purpose Specification



Must provide

(a)(1): What categories of information are information stored and reasonably specific purposes for why it is stored

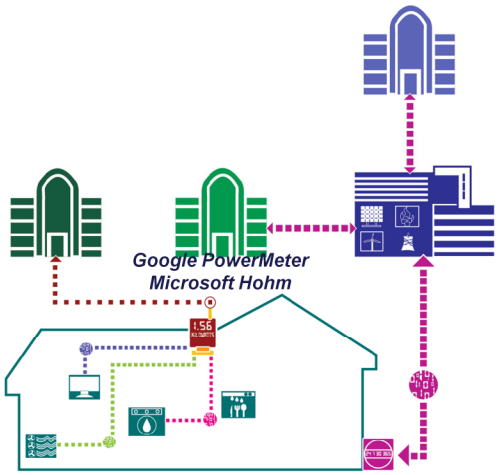
(a)(2): What categories of information are provided to third parties and purpose; some information about third parties

(b): How long information is retained

(c) Information on means or dispute or minimization by customer

CPUC Decision

§4. Individual Participation



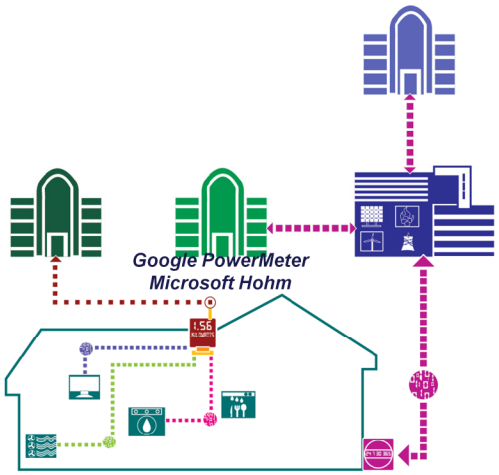
(a) Customers have access to their covered information

(b)(1): Customers have the right to grant or revoke secondary uses of covered information, to dispute accuracy, and request corrections

(c) Rules for Legal Process

CPUC Decision

§5. Data Minimization

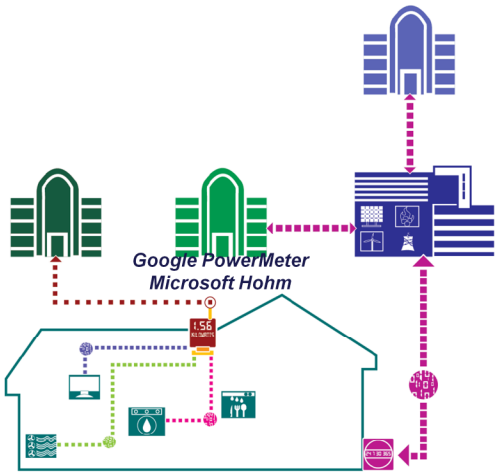


(a): "collect, store, use, and disclose only as much covered information as is reasonably necessary"

(b): "maintain covered information only for as long as reasonably necessary"

CPUC Decision

§6. Use & Disclosure Limitation

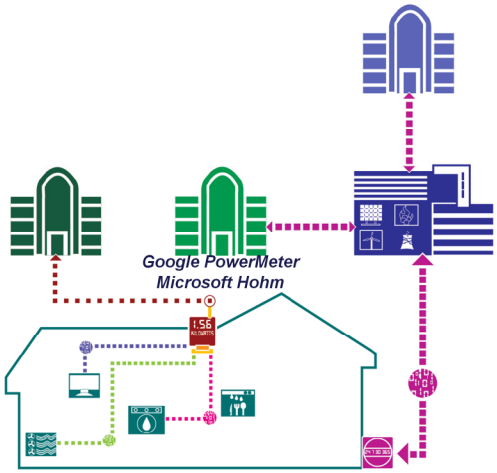


(b): Utilities "may collect, store and use covered information for primary purposes without customer consent."

(b): Third parties "may collect, store and use covered information only with prior customer consent. *Exception*: utilities may disclose info when ordered to do so by the Commission or for a primary purpose being carried by contract on behalf of the utility

CPUC Decision

§6. Use & Disclosure Limitation

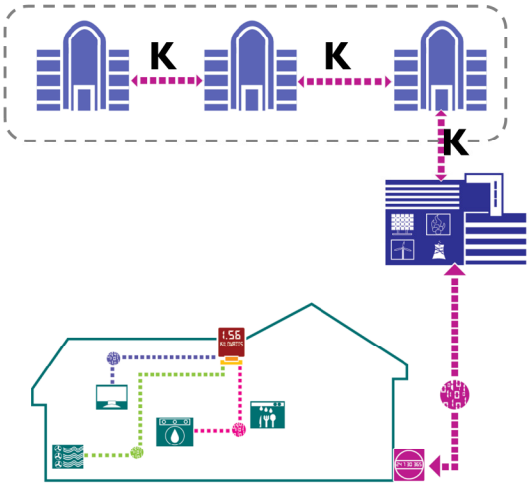


(c)(1): No customer consent required "for a primary purpose being carried out under contract with and on behalf of the entity disclosing the data."

Contractor (light blue building) must adhere to CPUC policies.

CPUC Decision

§6. Use & Disclosure Limitation

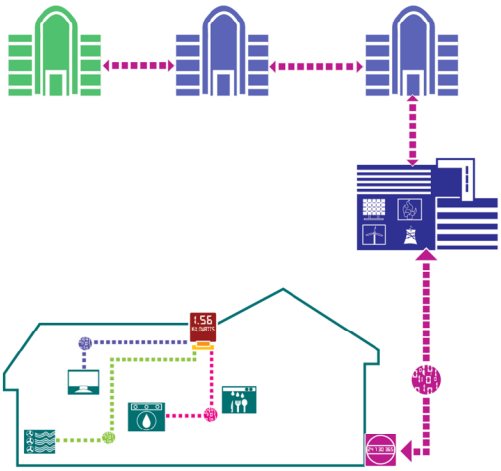


Contract chain

(c)(2): "Any entity that receives covered information derived initially from a covered entity" may share data without customer consent for primary purposes. All must adhere to CPUC's policies via contract.

CPUC Decision

§6. Use & Disclosure Limitation

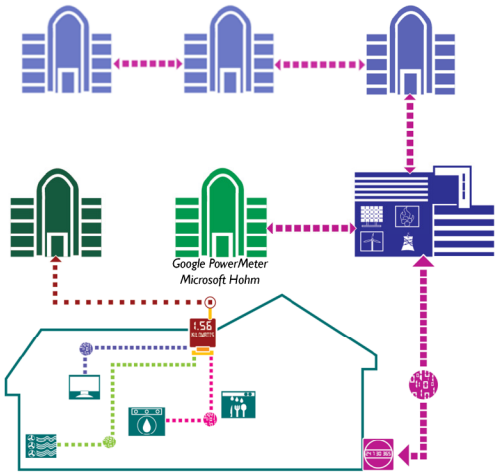


(d): Customer consent is always required to disclose covered information for any secondary purpose.

(e): Customers can revoke authorization at any time.

CPUC Decision

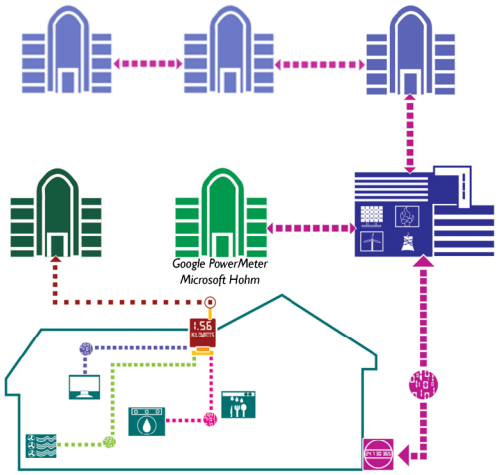
§7. Data Quality & Integrity



Must ensure "covered information [...] is reasonably accurate and complete."

CPUC Decision

§8. Data Security

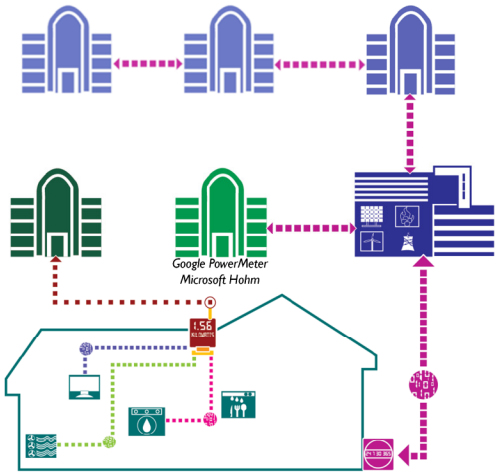


(a): "reasonable administrative, technical, and physical safeguards to protect covered information."

(b) Required to provide notification of breach

CPUC Decision

§9. Accountability & Auditing



(a): must make available to the Commission:

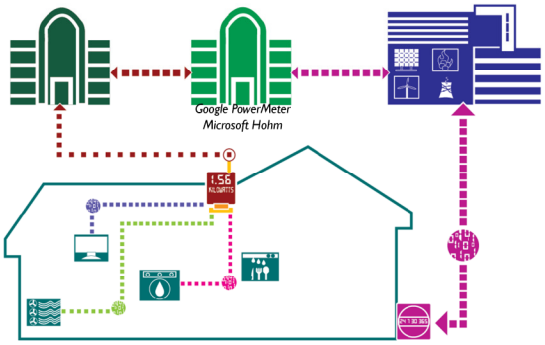
(1) privacy notices

(2) their internal privacy and data security policies

(3) third parties to which they disclose covered information, the purposes for which that information is disclosed

CPUC Decision

§9. Accountability & Auditing



(d): Electrical corporations must do audits.

(e)(1): Must report "the number of authorized third parties accessing covered information."

Overarching Policy Issues

- Privacy in the home
- Jurisdictional Issues
- Engagement with other State and Federal Actors
- Relationship between privacy rules and innovation
- Technical Implementations of DR and LC can make privacy easier or harder to address

References

	Title	Link
1	Mulligan, Deirdre K., Wang, Longhao and Burstein, Aaron J., Privacy in the Smart Grid: An Information Flow Analysis, On behalf of California Energy Commission, Public Interest Energy Research Group, March 1, 2011. Available at SSRN:	http://ssrn.com/abstract=1815605
2	P.A. Subrahmanyam, D. K. Mulligan, D. Wagner, U. Shankar, E. Jones, J. Lerner, "Network Security Architecture for Demand Response/Sensor Networks". Technical report, On behalf of California Energy Commission, Public Interest Energy Research Group, January, 2005.	• http://sites.energetics.com/MADRI/toolbox/pdfs/standards/network_security_final_report.pdf • http://www.law.berkeley.edu/4727.htm
3	Lerner, Jack I. and Mulligan, Deirdre K., Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home. Stanford Technology Law Review (STLR), Vol. 3, 2008. Available at SSRN:	http://ssrn.com/abstract=1099121
4	Proposed Decision Adopting Rules to Protect the Privacy and Security of Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company, *in* Rulemaking 08-12-009, California Public Utilities Commission, filed May 6, 2011	http://docs.cpuc.ca.gov/EFILE/PD/134875.pdf
5	Comments of the Center for Democracy & Technology, on Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security and Requirements, National Institute of Standards and Technology, Dec. 1, 2009	http://www.cdt.org/content/cdt-comments-nist-smart-grid

Graphics Credit: Brian P Miller Photo & Design, http://www.brianpmillerphotography.com/