



Smart Meters: How Will They Affect Your Privacy?

The American Civil Liberties Union of Hawaii is an organization with over 2000 members who care deeply about personal freedoms, especially privacy.

Of increasing concern is the collection and storage of data that reflect a person's individual actions, including the collection of electrical usage data through smart meters. This data is of great interest to law enforcement, for a variety of reasons.

To protect customers' privacy and give utilities an appropriate response to data requests from law enforcement or others:

- Law enforcement should not access Hawaii customers' smart meter data without a warrant.
- Any subpoenas or other court orders for a customer's smart meter data should be presented to the customer him/ herself, not to the utility. The customer deserves the opportunity to contest the subpoena.

Also of importance:

- Utility customers should decide for themselves whether they wish to have a smart meter installed at their home. Consent must be renewed every two years but can be revoked by the customer at any time.
- A utility should not charge extra fees if a customer decides not to opt in and have a smart meter installed at his/her home. The savings the customer foregoes because of his/her decision is already a penalty for nonparticipation. Additionally, extra fees could, because of the classes of people who might decline to opt in, lead to unintentional, and yet still illegal, discrimination.

Electrical usage data is of great interest to third parties other than law enforcement. Washing machine manufacturers, for example, may like to know who owns an older, energy-inefficient washing machine that is likely to be replaced soon. The sharing of such data, however, lies beyond the primary purpose of smart meter installation. Therefore:

- A customer's consent should be required anytime his/her data is being shared, sold, or given to a third-party not performing a primary purpose on behalf of the utility.

A utility should also be required to report yearly on a number of things:

- The number of times customer data has been sought without customer consent, with details of any access;
- The result of an independent audit of privacy and security practices;
- The number and identities of third-party access; and
- The number of breaches, and the number/percentage of customers affected by breaches.