

# Will the smart grid protect consumer privacy?

Jay Cline

November 17, 2009 ([Computerworld](#))

A big shot of stimulus money awarded last month is sure to accelerate the transformation of the U.S. power grid into a massive network capturing data about much of what we do inside our homes. But will we trust this new "[smart](#)" [grid](#) with our data? I think the answer to that question will depend on the first impressions we get from the privacy and security offered by our power companies. Up until now, however, it hasn't been obvious to the average consumer what those protections are.

As [announced by President Obama](#) on Oct. 27, the Department of Energy has awarded \$3.4 billion in stimulus money to 100 smart-grid projects. Each project had to drum up its own matching funds, meaning the overall investment will top \$6 billion. According to [the department's estimates](#), the awards will result within three years in 18 million homes -- or 13% of all U.S. households -- getting the smart meters necessary to convert to the smart grid.

Why the [government interest in this new power network](#)? It's all about saving energy, reducing American dependence on foreign oil and [securing the grid against terrorists](#), according to supporters. And I couldn't find any opponents, other than those opposed on principle to government-industrial subsidies.

Here's how it will probably look to you and me.

If we live in Austin, Boulder, Baltimore or one of the other cities that won an award, at some point in the near future we'll receive an invitation from our power company to allow it to install an advanced-metering infrastructure (AMI) meter at our home. The AMI will wirelessly transmit its data back to headquarters.

If we live in a rural area, this invitation may also come along with an offer to sign up for [broadband-over-power-line \(BPL\)](#) -- to get Internet access through our power outlets.

Next, we'll receive instructions to log in and create an account on our power company's Web site. Through our account, we'll be able to view our energy usage, outlet by outlet, in 15-minute increments. We'll also be able to see the associated rates charged for the different time periods. It won't take much review of our accounts to conclude that avoiding the peak hours of energy usage -- 3 p.m. to 8 p.m., when rates are correspondingly high -- for doing things like running a load of laundry will be money on the table for our taking.

Strategizing on when to run power-heavy activities will become especially important to owners of electric cars. Recharging an electric vehicle can consume half of a home's daily use of power. A whole neighborhood of homes recharging their cars at the same time could crash the local power grid. With a smart-grid account, however, you and I will be able to program our cars to recharge at 2 in the morning.

But this is where it gets interesting.

Power companies will be able to reach inside homes and turn off certain outlets -- for example, one recharging a car, supporting an air conditioner or water heater, or charging a laptop that has been on screensaver for hours. Power companies will need to be able to do this to avert [grid crashes](#) and also help us meet our power-use objectives.

This outlet-specific control will remind us that power companies will be receiving a lot of data about us -- when we come and go, what kinds of appliances are plugged in and how much of our energy use could be classified as waste. There will perhaps be no richer profile of who we and our families are.

That data profile will only become richer with the introduction of smart appliances. These remotely programmable appliances will be able to track,

record and optimize usage and send data to each other. And quite possibly, their data could feed back to the power company.

For example, manufacturers say a smart dishwasher could tell a smart clothes washer to wait until it gets done, or a smart oven could tell a smart refrigerator to hold off on defrosting until after dinner in order to optimize energy use.

GE is even building a smart refrigerator that will be able to read the bar codes of food containers. It'll be able to keep track of what's been bought, what recipes can be made from the food it contains and what should be on next week's grocery list. The same technology could be applied to a medicine cabinet to keep track of prescriptions.

So it's possible that your power company could become your Internet service provider; know your daily rhythm, carbon footprint, eating and medicine habits, and relative income level; and be able to micromanage your outlets. Just about every appliance maker, manufacturer, clinical-research organization and service provider is going to be knocking on the door of your power company to buy this data.

Landlords may also be very interested in keeping tabs on what's happening inside their properties. Litigants, law-enforcement entities and defense agencies are also certainly going to be pursuing this data on a regular basis.

Privacy consultant Rebecca Herold, writing in the September 2009 document by the National Institute of Standards and Technology (NIST), [Smart Grid Cyber Security Strategy and Requirements](#), outlined the key privacy risks needing to be managed by smart-grid operators. Among them:

- **Personal profiling** -- Accumulating massive data files on people that eventually become used for purposes beyond delivering them energy.
- **Identity theft and home invasions** -- Not sufficiently protecting these rich data profiles from criminals who could harm individual consumers.
- **Activity censorship** -- Determining what energy uses are not acceptable or should be taxed at a higher rate.

- **Decisions based on inaccurate data** -- Turning off power to an outlet that is providing a health-sustaining appliance or device, or providing inaccurate data to credit-reporting agencies and government agencies.

How can grid operators manage these risks and win consumer trust?

I think the [National Association of Regulatory Utility Commissioners \(NARUC\) had great foresight in 2000 when it resolved](#) that "unless a customer grants explicit, affirmative informed consent, customer-specific information about his or her utility service should only be used in connection with rendering or billing for that service or other services requested by the customer, and that such information should not be otherwise available to affiliates or third-parties."

NARUC will be taking it one step further this week at its annual meeting in Chicago. Members there will vote on [new smart-grid-privacy resolutions](#) that include minimizing the personal data collected by the smart grid.

Minneapolis-based [Xcel Energy](#) got this right this year when it took an opt-in approach toward loading the data of its 3.4 million customers into [Microsoft's Hohm personal-energy tracker](#). And [Ontario's Ministry of Energy and Infrastructure](#) got it right by engaging the province's privacy commissioner, Ann Cavoukian, early in the process of deploying smart meters to all Ontario homes by the end of 2010.

What kind of privacy requirements should they be building into the smart grid? I think the [seven Safe Harbor privacy principles](#) point the way. Here they are, applied to the smart-grid world:

1. **Notice.** Prior to hooking up a smart meter, give consumers a detailed privacy notice that lists all the potential data that will be collected, all the potential uses, all the potential parties who could get access to it, and how long the power company will retain this information.
2. **Choice.** Obtain opt-in consent from consumers for any collection and use of their data that is not strictly required to provide and bill for energy service.

3. **Access.** Give consumers the ability to review all of the data that has been collected about them.
4. **Data integrity.** Give consumers a way to correct mistakes in their data, especially regarding outlets and appliances that, if turned off, could harm them.
5. **Security.** Certify against the NIST standards for smart-grid security.
6. **Onward transfer.** Hold business partners and service providers who may access consumer data contractually accountable to these same terms. If consumer data has been subpoenaed, immediately notify affected consumers so that they can exercise their rights.
7. **Enforcement.** Maintain an independent dispute-resolution process of the likes managed by Truste to expediently resolve consumer-privacy complaints. Regularly conduct privacy and security audits and report the findings to the appropriate regulator.

An upgrade of America's power grid is long overdue. Steps taken in the next 12 months to build privacy into the upgrade will determine whether the most innovative aspects of the smart grid will be accepted by the public.

**Jay Cline** is a former chief privacy officer at a Fortune 500 company and is now president of Minnesota Privacy Consultants. You can reach him at [cwprivacy@computerworld.com](mailto:cwprivacy@computerworld.com).