The Privacy Implications of a Smart Grid Electrical System

The emerging Smart Grid electricity system will allow utilities to collect and possibly distribute detailed information about household electricity consumption habits - ice makers will operate only when the washing machine isn't, TVs will shut off when viewers leave the room, air conditioner and heater levels will be operated more efficiently based on time of day and climate.

Home gadgets and appliances will be wirelessly connected to the Internet so consumers can access detailed information about their electricity use, and reduce their carbon footprint appropriately. The potential benefits of such a system are self evident, including: Reducing energy use and CO2 emissions (maybe 20% per home), preventing blackouts, spurring development of renewable energy sources, and improving customer service by locating trouble spots and dispatching maintenance teams to fix the problem.

The Consumer Federation of California supports these goals. But the paradox of a smart grid system is that what will ostensibly make it an effective tool in reducing energy usage and improving our electric grid – our information - is precisely what makes it a threat to privacy: our information.

Soon this technology will be near ubiquitous: Up to three-fourths of the homes in the United States are expected to be placed on the “Smart Grid” in the next decade, and there will be nearly 50 million by 2012. Some foresee it becoming 100 to 1000 times larger than the internet.

The sheer volume of data provided by Smart Grid technologies will make it a prospective goldmine for numerous parties other than the utilities themselves, for reasons other than energy efficiency, and used for purposes that do not benefit the consumer: advertisers and marketers will seek to create and utilize increasingly detailed behavioral profiles, law enforcement and the government will seek to monitor our homes, and criminals will seek to steal identities and rob homes – made all the more easy by the wireless transmittal of the data.

As such, without proper safeguards and ironclad rules in place, a myriad of new privacy threats could eventually find their way into every home in America.

Activities that might be revealed through analysis of home appliance use include personal sleep and work habits, cooking and eating schedules, the presence of certain medical equipment and other specialized devices, presence or absence of persons in the home, and activities that might seem to signal illegal behavior.
Personal privacy issues routinely arise when data collected is harmless in isolation, but becomes a threat when combined with other data, or examined by a third party for patterns. In other words, what are the potential “unintended consequences” of such an electrical system? And more importantly, what must we do to ensure that those unintended consequences are never realized?

Such interest in our private data by third parties begs some important questions: How much information should we give up to the grid? Should it be up to the customer to decide? Who stores all that information and for what reasons? How will this information be managed and how long will it be stored? Who will come asking for that information, for what purposes and under what rules? And will there be proper and enforceable accountability for those that abuse our data?

Specific examples of such “unintended consequences” might include:

- Travel agencies might start sending you brochures right when your annual family vacation approaches.

- Financial institutions making home mortgage loans might also be interested in their customers’ energy usage records to verify whether the customers are actually living in those houses.

- Law enforcement officials might use our information against us. Consider the predictable desire of police to locate in-home marijuana growers by monitoring household power usage? What about increasingly intrusive surveillance of proclaimed suspects homes?

- Lawyers might seek to subpoena your data in a divorce trial, "Have you ever left your child home alone? If so, how often, and for how long?"

- Insurance companies, always seeking to maximize profits by denying coverage or jacking up premiums, might start developing connections between energy use patterns – like eating late at night - and unhealthy tendencies.
• Soon RFID tagged labels – read by smart meters – will be found on more and more of the food and prescription drugs that fill our refrigerators and cabinets. Could our health insurance go up because we eat too much unhealthy food? Might we start receiving mailers trying to sell us new prescription drugs that their detailed behavioral profile has led them to conclude we need?

• Hackers and criminals might seek to falsify power usage, pass on their charges to a neighbor, take down the grid entirely, disconnect others, and plan burglaries with an unprecedented degree of accuracy.

• Some consumers are already getting statements that compare their use to their neighbors. Could we see a system develop in which some are penalized for more “wasteful” usage? What if the comparisons aren't fair? Will details such as the number of occupants be properly taken into account?

• Landlords might be interested in know more about what's happening inside their properties.

• If recent revelations regarding warrantless wiretapping, Patriot Act abuses and increasingly intrusive surveillance techniques are an indicator, we should also expect government agencies to come seeking our data.

Such privacy implications strike at the heart of the Fourth Amendment, the California Constitution, and a core American value: our right to keep private what goes on in our homes, and the inherent freedom that that right provides us.

The challenge that now stands before us is how to both protect consumer privacy while simultaneously empowering customers with the ability to access their data in near real time and potentially share it with entities other than the utility.

It is paramount then that our state’s transition to a smart grid system addresses the potential privacy pitfalls while we are in the early stages of its implementation; because once that genie is out of the bottle it’s difficult to put him back in.

A few principles we should keep in mind as we develop a regulatory framework will be consumer control, informed consent, transparency, security and accountability - including strict limits on the amount of data collected, its use, and the length of time it’s stored.
Such privacy safeguards will increase, not decrease, the long-term viability of, and consumer confidence in, the system itself.

The only real conflict I foresee in implementing such a system isn’t between privacy advocates and environmentalists, but rather, between those that want to protect their personal data versus those that seek to access and profit off it….as well as the expected public policy rush to get the system up and running before it’s truly ready.

The endless accumulation of our personal data – combined with the outlandish profits being made off it and growing government demand for it – represents a direct assault on our right to privacy. We would do well to contemplate the steady erosion of this right and its long-term implications.

Corporations, by definition, care about profit, not solving the climate crisis or reducing energy usage, and certainly not protecting privacy. Governments, by definition, care far more about power and control, than individual liberty.

Evidence of this abounds: Social networking sites store and publicly share unprecedented private details about their users without telling them what they are doing with that information. A recent study found that the 43 leading sites made privacy control settings difficult to find and to understand; and the defaults were almost always set to allow maximum dispersal of data.

Google’s CEO, Steve Schmidt recently stated "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."

As you let that sink in, he also said:

"... the reality is that search engines including Google do retain this information for some time, and it's important, for example that we are all subject in the United States to the Patriot Act. It is possible that that information could be made available to the authorities."

The facts bear witness to Mr. Schmidt’s worldview, as one Google product after another – from Google Buzz to Google Books - has been a virtual privacy train wreck. The company’s refusal to make public how often information about their users is demanded by, or disclosed to the government, is all the more disconcerting.
Facebook reportedly receives up to 100 demands from the government each week for information about its users. AOL reportedly receives 1,000 demands a month. In 2006, a U.S. Attorney demanded book purchase records of 24,000 Amazon.com customers. Sprint recently disclosed that law enforcement made 8 million requests in 2008 alone for its customer’s cell phone GPS data for purposes of locational tracking.

It wasn’t long ago that the idea of our government wiretapping American citizens without warrants for purposes other than national security would have been revolting. Now its official Government policy – and the telecom companies that participated in these crimes have been given retroactive immunity while continuing to make billions off overcharging the same customers they betrayed.

Nor was it long ago that we would have been rightly outraged by Patriot Act provisions – recently renewed – that allow for broad warrants to be issued by a secretive court for any type of record, without the government having to declare that the information sought is connected to a terrorism investigation; or that allow a secret court to issue warrants for the electronic monitoring of a person for whatever reason — even without showing that the suspect is an agent of a foreign power or a terrorist; and of course, that allow the government to search your home as long as it doesn't tell you it did.

As for the Smart Grid, just this week the FCC went on record as saying, “the federal government should be granted limited access to utility bills from homes receiving federal energy efficiency funds...”

The trend line is all too clear. More concerning than any single threat posed by any single technology – including Smart Grid – is this larger pattern indicating that privacy as both a right and an idea is under siege. As young people grow up with so much of their information so public and accessible to all, including government, I fear their sense, appreciation and understanding of privacy will continue to fade away. The consequences of such a loss would be profound.

As noted privacy expert Bruce Schneier recently stated:

“...lack of privacy shifts power from people to businesses or governments that control their information. If you give an individual privacy, he gets more power...laws protecting digital data that is routinely gathered about people are needed. The only lever that works is the legal lever...Privacy is a basic human need...The real choice then is liberty versus control.”
Rapid technological advancement - without the requisite regulatory safeguards – will only add to the increasing disintegration of privacy rights in this country - something the Smart Grid could come to epitomize if we allow ourselves to be seduced by arguments that claim we have no time to spare or to just “trust” those with inherent conflicts of interest.

Elias Quinn, Sr. Policy Analyst of the University of Colorado Law School’s Center for Energy and Environmental Security recently summed up the challenge and responsibility before us: “In the final analysis, the privacy problem posed by smart metering is only a difficult one if the data gets unleashed before consequences are fully considered, or ignored once unfortunate consequences are realized. But to ignore the potential for privacy invasion embodied by the collection of this information is an invitation to tragedy.”

I urge the Public Utilities Commission and the State Legislature if necessary, to provide an example to the rest of the nation by recognizing privacy as the Constitutional right that it is, and integrating at every point of the Smart Grid network ironclad protections. Now I want to turn it over to Jim Dempsey who will describe in detail how this can be done.