

## Smart Grid and Smart Homes – Make Sure You Read the Fine Print

June 24, 2015 – It has been a while since we’ve written about the smart grid – smart utility meters that are connected to internet. These meters are supposed to provide consumers with a way to monitor their utility usage and add some conveniences such as being able to shut the lights off if you suddenly realize you left them on. But as we’ve mentioned before, there is a dark side to the smart grid. It has to do with the data that is being collected on you and who will have access to it. The smart grid will eventually expose virtually every American consumer to some radical changes associated with personal privacy while in the home. And as with any large-scale program connected to the internet, the smart-grid is database driving – meaning that it is a potential goldmine for hackers.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

So, you want the convenience of being able to turn up the thermostat, open your garage door and turn on your lights – all from your cell phone. There are already some systems available that can do that for you, but more are on the way.

To get those services now, you probably have to subscribe to a service. Eventually, many of these conveniences will be available directly through any appliance that you purchase. And therein lies a problem of huge proportions. The logical question is, who’s collecting all of that data and who does it belong to? Unfortunately, there is no real answer to that question yet, even though nearly 40 million smart meters have already been installed nationwide.

As of this writing, there are no real regulations regarding all of this ‘smart data’. The Department of Energy published voluntary standards earlier this year, but they are not enforceable. Combine that with the tremendous amount of money that utilities can make selling that data and you have a recipe for privacy Armageddon.

Just think about the information that the data can provide marketers. It can tell them when you are home and when you are away so that they can plan their telemarketing schedules accordingly. It can tell them how much electricity your AC uses. An enterprising entrepreneur might like to have that information to market a brand new air conditioner to you. These examples are just the tip of the iceberg.

In the hands of hackers, it’s an even gloomier picture. Hackers in possession of this information could compile a profile of the times that you are home and away and then sell that data to criminals over the internet. And if the utilities keep all of your usage data in the same database as all of your billing and payment information, they can also use or sell the data for identity theft.

An article in Politico may have said it best. “Exhaustive electricity consumption data is a holy grail, in many ways” for marketing analysts and consumer data aggregators, said Lee Tien, a senior attorney for the Electronic Frontier Foundation. “Few other types of data get inside the home the way that electrical usage data does.”

If you are thinking about signing up for a smart home service, make sure you read the fine print first. Who will own your data? Who will have access to your data? Can you opt out of sharing your data? Think long and hard about this. While these services may offer you some limited convenience, you may be opening a window on your life that you don’t want shared with everyone else in the world.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow me on Twitter:

Follow ACCESS