

## Smart Devices Continue to Raise Privacy Issues

January 3, 2017 - Last week we wrote about police in Arkansas trying to get their hands on Amazon Alexa recordings that may have inadvertently recorded information associated with a murder case there. It turns out that Amazon didn't have the only smart device in the home where the murder occurred. The house also had a "smart" water meter and the police are now saying that the suspect in the case used hundreds of gallons of water in the middle of the night according to that meter. They seem to think that the water use was an effort to clean up blood. But the suspect is saying that the clock on the water meter was incorrectâ€ meaning that the water was used but not in the middle of the night so there was nothing unusual about his water consumption.

The fact that these "smart" pieces of information are associated with a murder makes them sensational. But that doesn't alter the fact that smart devices are changing privacyâ€ especially in the homeâ€ in ways never before contemplated. It's a brave new world out there and consumers really need to think about what they are doing before they bring one of these devices into their home.

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);  
})();
```

In the case of the smart water meter, the homeowner and murder suspect in the Arkansas case may not have had any choice. It really depends on local laws. If utility companies don't need your permission to install a smart meter, they're going to do it. It cuts their cost for meter reading, is far more accurate than a manual reading and it gives them a lot of information about their customers that they wouldn't otherwise have.

But in the case of the Amazon device, a choice was made to bring it into the home. And that's true with most smart devices—including TV's, phones, refrigerators, appliances, etc—including

If you have a smartphone, it is tracking you. In many cases, it is tracking your every move. Google actually provides a way that Android users can take a look at their movements. Just go to Google and while you are logged in, search "my activity". If you go through the items there, you can see which YouTube videos you've watched and where you have traveled. It will even show you the routes that you used in your journey. Fortunately, Google will also allow you to turn off some of the tracking—something that everyone should seriously consider.

Smart TV can track what you are watching and when. Smart refrigerators can tell when you access their systems remotely, potentially providing information on when and where you shop. All of this information can help you establish or destroy an alibi if you ever really need one.

And of course the smart electrical grid that is being implemented at the behest of the federal government will have the ability to look at all of this information. What will emerge is a digital fingerprint that is likely to be able to identify you just as accurately as your actual fingerprint.

I'll probably never own a smart refrigerator. First of all, I don't see the need. A written list works just fine. Secondly, having a computer included with something that dispenses water and ice just sounds like a very bad idea. That doesn't alter the fact that a lot of consumers are buying these devices already. Most of them will never think twice about the privacy ramifications of their purchase—that is, they won't think about those ramifications until it is too late for them to protect their privacy.

In many cases, the information generated by smart devices is stored in the cloud. That means that it can be accessed with a simple subpoena rather than through a search warrant. This also means that if any of the information stored by these smart devices ever becomes relevant in a civil case—meaning a lawsuit against you—anyone trying to access the information will almost certainly be able to access it.

Anyone who already owns or who is considering the purchase of any smart device would be well served to learn how it works first. There may be things you can do to protect your privacy while still getting the benefits provided by the device. And if you can't protect your privacy, but you still decide to move forward with your purchase, at least you'll be an informed consumer and know exactly what convenience you are trading your privacy for.

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