

Amazon's Alexa May Be Listening to Everything You Do

April 12, 2019 - Perhaps it should go without saying but if you bring a device into your home that has a microphone in it, you should probably expect that device to be listening to you. You may think it should only listen to you when you tell it to do so, but making the assumption that this is how it will work could prove to be wrong. You know what they say about assumptions.

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);
})();
```

Word has now leaked out that Amazon's family of products that employ Alexa "company's voice assistant, are recording people at random. Moreover, Amazon employees are listening to those recordings.

According to reports, Amazon's employees don't have a means to identify who they are listening to. And the reported purpose of this "listening" is to improve Alexa's voice recognition ability. All of this may be true, but it is still a little creepy to think that perfect strangers might be listening in on your conversations. It's also a little frightening.

To be fair to Amazon, they're not the only ones doing this. Google and Apple do it too. And all of these companies offer users a means to delete anything they have recorded. The problem is that in the cases of Google and Amazon, it's a manual process. Apple claims to do it automatically.

There are ways to set up these services so that they don't listen to you automatically, and if you are interested in personal privacy, that may be the best way to go. On the other hand, all of these services are becoming more and more integrated into our daily lives. They allow you to do a lot of things remotely and easily such as controlling the thermostat in your home or turning on your lights when you are away. Turning off automatic listening also impacts how these services work, so a lot of people aren't willing to do that.

Over the long term however, these convenience items could come at a very high price. It's only a matter of time before some of these services get hacked. And an industrious hacker might be able to write an algorithm to sort through recordings to isolate key words. Things like account numbers, investment decisions, or even private conversations entailing information that could be used to blackmail someone could become common fodder for crooks. If that sounds far fetched then just consider the fact that 20 years ago, almost nobody had ever considered the possibility of a massive data breach. Today, more than half of Americans have had their data included in a breach. Times change and so does technology.

If you are going to have smart devices in your home, then you need to learn about how they work, carefully consider where you place them and just as carefully consider what you say around them. For instance, announcing that youâ€™ll be out of town for the next month and that nobody will be watching your home may not be the best thing unless you want to have your home targeted for a burglary. Crooks may not have the ability to listen in on your conversations today, but give it a year or two. Now is the time to start thinking about the consequences of having these devices in your home or office, and conducting yourself accordingly.

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 ACCESS