The Privacy Perils of Smart Phones

January 29, 2019 - If you have a smart phone and you're concerned about privacy, then you really need to pay attention to the applications you use on it. Take Apple's Face Time app for instance. Yesterday it was revealed that a bug in the software could allow people to listen in on your off-line conversations even if you refused to take a call from them. Since that revelation, Apple has disabled group-call capability in Face Time and has stated publically that they know what the problem is and that they will release an update this week to fix it. That said, some people may have already suffered damage as a result of the software bug. And Face Time is far from the only app that can cause a privacy breach.

Unless you learn how to turn certain features of you smart phone on and off, the idea of having a smart phone and personal privacy is nothing more than a myth. That's because smart phones track pretty much everything you do on them.

Apps - including the phones actual operating systems - track your movements every place you go. It doesn't matter if your phone uses Android, IOS or Microsoft. Location services are built in. In the United States, GPS is government mandated in smart phones. You can turn it off, but you need to know how. And once you do turn it off, some other apps on your phone may not work. For instance, if you want use turn-by-turn directions to find a particular store that you searched for on Google, that feature won't work if location services are turned off.

Your phone could also be listening to you. There are downloadable apps for Alexa (Amazon) and Cortana (Microsoft) that can be setup to be activated when you speak a key-word or phrase. And Google has built in voice recognition to the Android operating system; much like what Apple has done on IOS. The problem is that voice recognition for these systems isn't perfect. If you've ever been surprised to hear you phone talking to you like it is attempting to answer a question that you didn't ask it, that's because you said something the phone has mistaken for your key-word. It then woke up and started listening to what you were saying. And whatever you said was recorded and probably stored in the cloud somewhere.

Every key stroke you make is also recorded. And your browsing history is stored in whatever internet browser you use.

There is nothing inherently evil about smart phone. The fact is, they really arenâ€™t that smart yet. If they were, they wouldn't wake up and start recording you without warning.

But smart phones do pose a real threat to personal privacy. And because most of us are lazy and never read the operating instructions for our phones or the applications on them thoroughly, that threat is even greater. Every time you download a new app, it increases your privacy risk.

If you value your privacy, you need to learn how to use your device and manage its settings. And when you aren't using it, turn it off. Nobody is so important that they need to be accessible 24 hours a day, 7 days a week.
byJim 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