Biometric Data - Once Lost, Your Troubles Are Just Beginning

October 15, 2019 - Using biometric data in place of passwords has become all the range in the information technology industry. Want to lock your phone? Use a fingerprint or facial scan. Want to access a secure facility? Use a retinal scan. Even scans of human ears... which are supposedly as good as fingerprints... are being used as for biometric security. Unfortunately the cavalier use of this type of data may create more problems than it actually solves, but few people are talking about that.

Frankly, using biometric data to secure your phone is a very bad idea. Phone manufacturers, eager to give users new bells and whistles on smart phones, have been pushing its use. But there are significant problems with it. In the first place, if you are trying to keep your device secure from the prying eyes of the government, using biometric data to lock any device is the worst thing you can do.

That's because the courts have held that law enforcement can force you to unlock a device using a facial scan or a fingerprint. But they can't force you to reveal a password. You may think that's ridiculous but it is the law. It is based on the idea that law enforcement can already force you to give up your fingerprints and provide other visual details, such as taking a mug shot. But a password is something that you possess in your mind. And the Constitution says you can't be forced to provide information against yourself; which is essentially the same thing as forcing someone to reveal a password. The law on this is pretty clear.

But the government's ability to force you to unlock your phone is probably not the most troubling aspect of storing biometric data on a computerized device. The real issues start to come up when you consider the possibility of data breaches, the fact that companies regularly share data without telling us, and the rapid advancement of artificial intelligence (AI). The first two issues here are fairly easy to understand. The last issue is one that is only beginning to emerge. All of these issues should make you think long and hard before willingly giving anyone access to your biometric data.

All data is stored electronically in the form of numbers; "ones" and "zeros" to be precise. Biometric data is no different. That makes sharing it very easy. Even encrypted data is stored this way; the numbers are just all mixed up and an algorithm is needed to unscramble them.

Once you provide your data to someone, there is little to keep them from sharing it. Since biometric data is considered to

be the current Holy Grail for security, it is also becoming quite valuable to both companies and thieves. If it falls into the wrong hands, it isn't a stretch to say that anything you have attempted to secure with it is now vulnerable. But unlike a breached password which can easily be changed, we're all stuck with our biometric data. Once breached, the chances are that you will be severely limited in the ways you can use it in the future.

That situation is only going to get worse because there are now programs out there that allow for the creation of what are known as "deep fakes." These are falsified pictures that are nearly impossible to distinguish from the real thing. They are assembled using AI. Until recently, they have mostly been used to harass people. One of the more common forms of abuse has been to put the face of a known person on a picture of the body of a porn actor and then distribute the pictures widely. A lot of Hollywood celebrities have had this happen to them and it is easy to see how this could damage reputations and relationships.

Deep fakes are advancing rapidly however, and can now be placed in video. Not only that, these images can be manipulated to say anything and the voices can be faked electronically to the point that even voice recognition can't tell the difference between a real video and a deep fake. These developments have frightening implications. They mean that we will no longer be able to trust video evidence. Just think of that in terms of what it means in politics or crime fighting. Again, all of this is now possible because of the rapid advancement of AI.

Governments around the world are now scrambling to figure out how to deal with these issues but it is important for all of us to realize they impact us at a much more personal level. We're now at a point where a data breach of biometric information could allow someone to assemble a deep fake picture or video of you. It may show you doing something you've never done, in a place that you've never been. What do you think people will believe. Will they believe you saying," That isn't me!"? Or will they believe their own eyes when they watch the video? By now, I'm sure you can see the problem here.

Today, we're being encouraged to unlock phones, computers, safes, offices and even homes with biometric data. There are even guns and gun safes that are setup to recognize biometrics. For these systems to work, that data needs to be stored somewhere; making it vulnerable to theft or simple incompetent data security practices. Either way, once the data is out there, there is very little that you can do to protect yourself.

For now... and probably forever... passwords are a much better option for the average person. Just something to keep in mind the next time your phone asks you to secure it with a fingerprint.

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