When The Hunter Has Become The Hunted - An Ironic Data Breach

February 27, 2020 - It's been a little over a month since we first reported on a company named Clearview AI. In short, they are a facial recognition software company, and they are very controversial. That's because they have gone out to social media platforms and taken just about every face-shot they can find; placing those pictures in their own proprietary database and matching the pictures with other identifying data. Right now, that tallies up to be around 3 Billion pictures which they are marketing to law enforcement agencies around the globe. So we find it a little ironic that a company whose primary market is law enforcement is now a data breach target and the victims are the law enforcement agencies themselves. The company just announced that their entire customer database was stolen.

Clearview AI is marketing its services to the security conscious. To law enforcement agencies. In my mind, that means that they should have some of the best computer security in the world. You know, James Bond, state of the art computer security developed in some super-secret dungeon lab hidden underground. After all, they need to protect their reputation with their customer base, or so you would think. And by the way, their customer base doesn't want to be identified. That's been made abundantly clear because Clearview AI has refused to name their customers. And I mean, any of their customers.

But that cat appears to be out of the bag now. That's because, of all the things that hackers could have stolen from the company, they wound up with their entire base of customers. In fact, the company has said their picture database wasn't impacted.

Now the question is, what will the hackers do with this information? If I was a betting person - and I am - my guess would be that they are going to release it. And that's likely to cause some issues.

The general public is becoming less and less enamored with the idea that you can be identified by the highest bidder when you are simply standing on a street corner minding your own business. But that's the brave new world being pedaled by Clearview AI and others. Releasing information on how this technology is being used is likely to get the unwanted attention of both the public and of some attorneys. It even has the potential to disrupt cases that are already moving through the justice system where defendants were negatively impacted by the company's services. In the end, it could lead to a much smaller database of customers for the company.

Clearview AI is just one player in the field of biometric identification. The real issue here is that congress has yet to

address the proper use of biometrics in law enforcement or, perhaps even more importantly, for commercial entities. It's now time for them to pick up this ball and run with it.

As it stands right now, Clearview is only marketing their database to law enforcement. But what if they released an app to the public? Or to employers? Or to private investigators? You get the idea. The very concept of "anonymity" could vanish overnight.

There is no doubt that what Clearview is doing has some very positive applications. One example of a good use might be to find a suspect wanted in an Amber Alert. Just ask the public to take out their phones and start videoing. You might be able to catch the culprit in a matter of a few minutes and long before he can do any harm to the person he's taken. But the flip side to that is very dark. Just imagine a stalker using the same application to track down a victim who is in hiding. Right now, there are no regulations for either scenario.

We've been telling our readers for years that technology advancements are outpacing our regulatory laws. And nothing that we've seen recently leads us to change that opinion. If lawmakers don't take up this issue relatively soon, then privacy is likely to become an antiquated concept. Maybe this breach will get the public's attention and lead some politicians to take some legislative action. We certainly hope that's the case.
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