

Your Picture Is Now The Only Thing Needed To Find You

January 21, 2020 - What if someone could take a picture of you and learn your name, address and other personal details about you in just a few seconds? For years, that has been a question that government, law enforcement agencies, corporations and academics have contemplated but done little else. Now the time for contemplation is over. A company by the name of Clearview AI has made the scenario above a reality and they are now providing their services to more than 600 law enforcement agencies around the country. And other commercial applications of their service are almost certain to follow.

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);  
})();
```

Facial recognition is nothing new. Law enforcement agencies have used it for many years, but with limits. For instance, when hunting for a criminal it has typically been used by taking a photo of the criminal in action and then comparing that photo to a database of mug shots. In this scenario, if the criminal in question is a first-time offender, there won't be a mug shot to compare his picture to. And facial recognition won't be too useful.

But Clearview AI has taken facial recognition to a new level. They did this by going out to social media websites and scraping the pictures and other data off of them. They then put all of that information in a database. At present, they have around 3 billion pictures stored. You have to figure, if you've put a picture of yourself online, then you're probably in their database.

All of that data is sorted using a neural network - meaning artificial intelligence. This allows the company to take a mundane photo and turn it into real data. Anyone using their system can find out the name, address and other details of the person in the photo as long as that information is on their network.

While all of this may be a little frightening to those of us who are privacy conscious, a system like Clearview's also has the potential to do a lot of good. One scenario that comes to mind has to do with identity theft. Just think about some criminal who has stolen your data and who decides to use it to apply for instant credit at some department store. The store takes a picture of them, matches it against the Clearview database and finds out that the person submitting the application has a different name and address, and all of that information is provided to the store in real time.

What Clearview is really doing here is turning biometric data into something that can be useful in the real world. It is a tool. But like any tool, it can be used for good or it can be weaponized and used for bad.

Unfortunately, even though we've known that this day was coming for years, our elected officials have done little to prepare for it. There are almost no regulations out there that regulate the collection and use of this type of data. Data breach laws wouldn't apply unless someone was able to obtain access to Clearview's database. Privacy laws may not apply either because the company is just collecting data that other people have already put on the internet; in most case, about themselves.

This lack of regulation has the potential to trigger a knee-jerk reaction from politicians. And that reaction could do more damage than good. Some will certainly start screaming to make this sort of thing illegal and at the same time they will ignore the benefits that can be derived from such a system. Others will try to prevent regulation at all costs, but that ignores the damage that such a system can create in the wrong hands. Just think of what stalkers or sexual predators could do with such a system.

We believe that regulations need to be well thought out before they are enacted, but that there certainly need to be some. And they really need to start with who can access databases like this, and what that data can be used for. For starters, should law enforcement be required to get a warrant in order to use the system? Should such a requirement have an exception when time is critical, such as to catch a child abductor or someone fleeing a crime scene? Should commercial entities be able to access the system to prevent fraud? Should those same commercial entities be barred from using the system to prevent identification of customers simply window browsing or walking through their establishments?

All of these are critical questions and they need to be addressed soon, but thoughtfully.

One thing is certain. This genie can't be forced back into the bottle. That means we need to make it work for good and regulate out any potential bad side effects.

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