It's time to face the 'reverse side' of face recognition technology

The use of artificial intelligence AI identifies faces growing quickly. This is why you should feel anxious about your personal privacy and it's time to face the flip side of face recognition technology.

The use of artificial intelligence AI identifies faces growing quickly. This is why you should feel anxious about your personal privacy.

A scam has just been posted on Facebook last week. Fake news about a fake application called **Facezam** , the app that helps you search a **passer's** Facebook, just by taking a picture.

Thousands and millions of Facebook users believe in hoaxes and feel extremely worried. (*An English businessman has just developed a face recognition application that can recognize strangers through a photo*). However, it turned out that this was just a prank of a marketing company to create a certain buzz.

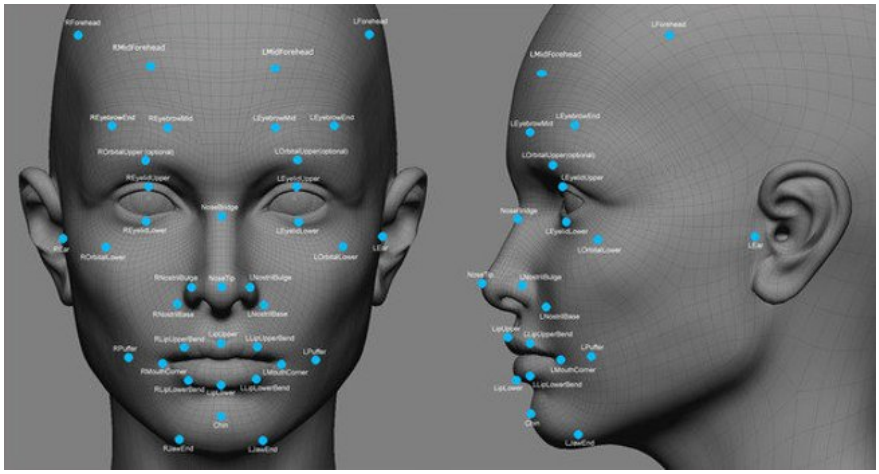


Photo source: EndTheLie.com
The online community understands ambiguity about privacy and security risks of **biometric technology** . Everyone knows that each individual's biological characteristics can be used to identify. For example, for decades, police have used hand question marks to identify many people.

Modern technology has enabled a large number of biometric identification systems to use the physical attributes of each individual such as fingerprints, iris, face and voice to identified. But when it comes to this, it can pose a threat to personal privacy, but there are still many other approaches.

Face detection is 100 times more dangerous than other things.

If you are concerned about biometric privacy violations, your concern should focus on face recognition. All biometric systems involve collecting biometric data, entering data into a database, then collecting new data to combat the appropriate search databases. All of them work very well to identify individuals who use computer analysis data of different body parts.

Most forms of biometric data are elusive. For example, it is clear that permission or knowledge is often required for fingerprint, iris, vein and other biometric data. However, your iris or veins may never be scanned, even once.

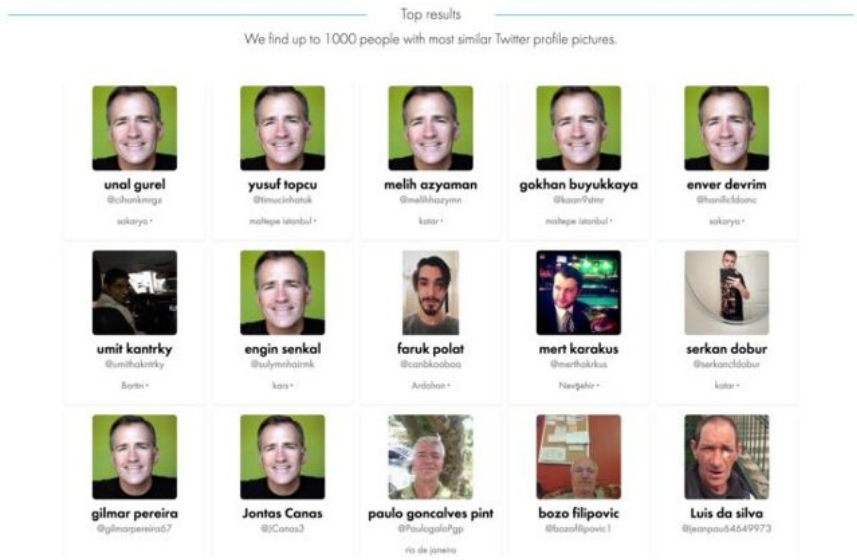
Face recognition does not require permission or knowledge. Any photo can do that.

In fact, each of us has already taken hundreds or thousands of photos. With surveillance cameras, we are often photographed. Every time we use ATM withdrawals, we can easily catch our images taken and the images associated with the bank's internal database will show the bank's name and bank account. friend. The captured image can be taken from a long distance.

Other biometrics data is more difficult to verify privacy without your knowledge or permission. For example, if you get fingerprints when you are a passport or police station, you have agreed to give your fingerprints and these agencies will retain your data. Suppose, if I give you someone's fingerprint, you cannot use that data unless you are a police officer and have access to the database.

On the other hand, publicly available images are available online to make it accessible to anyone. Social networking sites, brand image websites and others make millions of people's biometric data (*their snapshots*) available to anyone in the world when connected to the Internet. .

Face images are easily connected to names. Once you know someone's name, you can identify their home address, relative list, phone number and other data. This is what the fake **Facezam** app claims to be able to do. However, this article will show you how to do it without Facezam application. Just spending at least three minutes and not having to pay any expense can find a home address based on a single photo.



Similarly, **FindFace's** face **recognition app** , which sparked controversy in Russia in 2016 after its feature was used to identify and humiliate pornographic actors and sex workers. via personal accounts on Vkontakte social network (*VK*). VK has taken many measures to combat abuse but the FindFace application still exists. Therefore, it is not an exaggeration to say that an application like Facezam or FindFace gives people the tools to attack others online. However, FindFace is useful in discovering people on Twitter who are using your profile picture.

You can follow the steps below:

1. Upload someone's face image to FindFace, a Russian face-recognition website.

2. FindFace will give you multiple search results for Twitter accounts. Then, find the correct Twitter account and it will tell you the person's name.

3. Copy and paste the person's name into a website called Family Tree Now that will give you the address of the person, family members, age and other data.

Now, you can have 100% accurate information about a person, which can use find out almost anything about them by searching government records, criminal records and what you want. .

Of course, this system is not always perfect. This trick can work less effectively than half for a variety of reasons, such as: some people don't have a Twitter account, don't use real photos or real names on Twitter. And especially the Family Tree Now page can provide you with many people with the same name. However, if you try to test this system with some images of a person or a group of people, some of them will likely be identified.

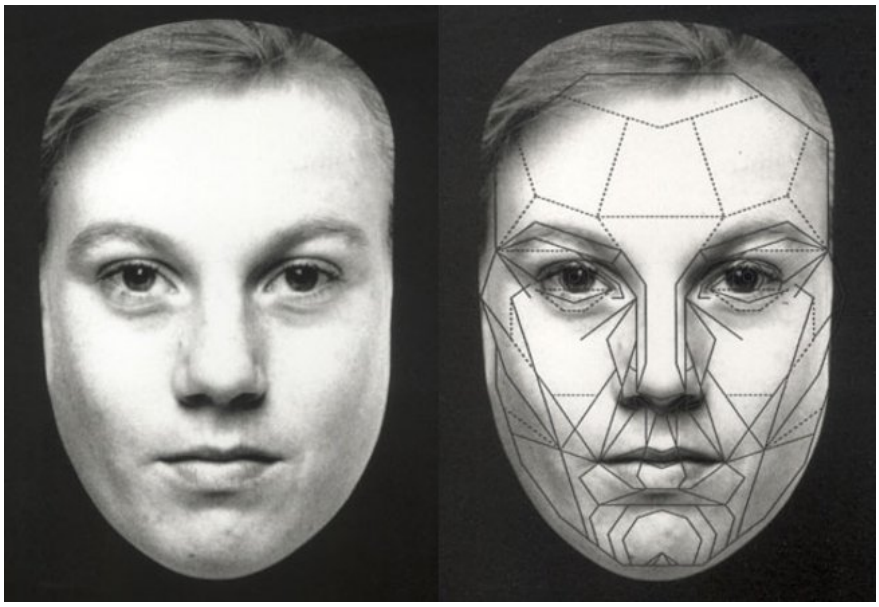
You may think that the solution will be deleted or blurred your Twitter account. And for that what I tell you is just a " *reasonable* " thing to do. But I show you that only this method instinctively brings facial recognition. And FindFace represents only a relatively small risk compared to what happens in the next few years.

Face in photo

Another simple example is that **Google Photos** just needs to click that Google " *viewer* " image will automatically run face recognition on all your photos and groups of images of that person together. By clicking

on any face, you will see all images of that person.

Google Photos automatically organizes your uploaded photos by location and by date. Using advanced image recognition and Google's large information database can easily identify topics for photos. Search for quick photos at any time according to such standards: wedding photos taken last month, photos taken during holidays, pet photos, dishes you cook and more.



In addition, the Google Photos application uses a number of complex image processing techniques for group photos. The group photos are automatically displayed in the main search interface. The categories you will see here depend on what you take. These groups can be places where you go, a friend or objects like food, cars, bicycles and more.

Google Photos models the faces in your photos to synthesize similarly shaped faces into a group. This way, you can search the image gallery for a specific object's image. If someone appears in multiple groups, you can combine them. Moreover, you can create a sticker with a name for that person.

The best fact about Google Photos is that anyone can add a name for each photo gallery. That means anyone who knows, who has taken your photos and Google Photos users can label them with images with your name. So tell Google's huge face recognition database who you are.

Just be shown clearly, do not label specific images like you. It is Google's AI notification that any or all of your images are you and additional images will also receive your name, then link to them.

The same thing happens on Facebook. Selfie of users with their personal cards, family cards and friends. This announces the leading AI industry of Facebook who is who. You'll notice that when you upload an image of yourself, Facebook often knows it's you.

The truth is that your face is being photographed continuously for your face and face recognition database that will be used more to determine the things behind that don't involve permission and knowledge. yours.

Face detection technology appears everywhere

Many rumors suggest that the best-selling smartphone line will soon have facial recognition, like their top security security program. Samsung Galaxy S8 and Galaxy S8 +, expected to be released later this month, are spread including face recognition technology as part of a security security system.

Another rumor suggests that the upcoming Apple 8 iPhone also has facial recognition software. This result is less likely to happen than Samsung's rumors. However, Apple does not have many patents on face recognition technology, including using face detection to unlock.

A startup project called **Blue Line Technology** provides face-recognition technology for security stores and the technology is being tested at several stores in Missouri, where the startup is located. This technology works by running face recognition everyone is walking in front of the door. If someone wears a mask or is confirmed in the store database as a thief, that door will not open.

Airports in Japan, France, Canada, Australia and other countries are gradually implementing face recognition systems. Most of the current programs hope to handle identifying all passengers at security checkpoints within the next few years.

Uber uses real-time face recognition in China and India. Drivers must scan their faces before accepting any trip to verify that they are not impostors or criminals who seek to pick up customers.

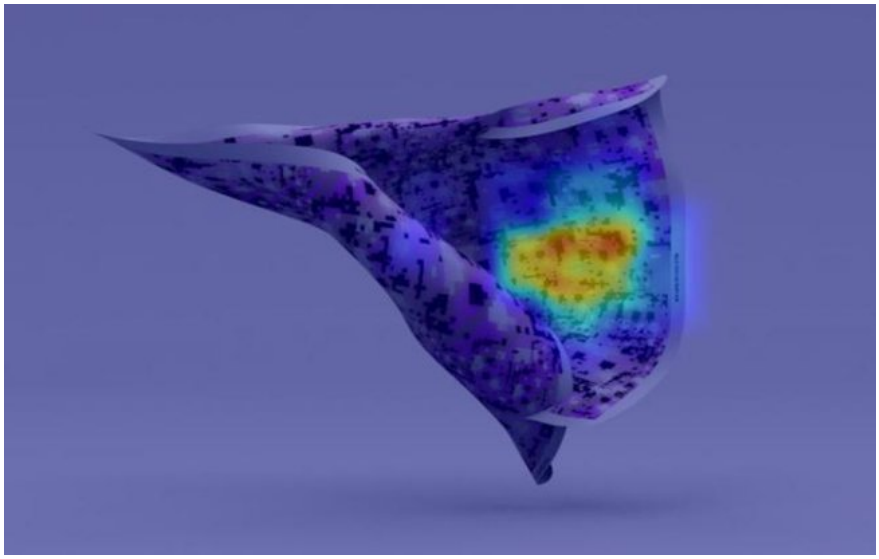
Cruise ships are also catching up with facial recognition technology, allowing passengers to buy items without carrying a credit card. And the United States is also working to use face recognition instead of driver's licenses and IDs.

In the short term, face recognition technology will be the mainstream. People are gradually getting used to a road, where everyone accepts " *scanning recognition* " as a normal part of everyday life.

Can highlight face recognition (maybe not)

A Tv Series " *Minority Report" character* - adapted from a fascinating Steven Spielberg work on the prospect of future people with facial tattoos is designed to trick face recognition technology.

Is that really our future?



Designer Adam Harvey has created a patterned fabric designed to help actively in the face recognition system. The designer created a fabric that tricked computers into identifying faces by covering the face with a cloth. When the system tries to identify facial recognition points, proper accuracy will be significantly reduced. In addition, Harvey also discovered hairstyles and makeup to trick face recognition technology.

Kickstarter campaign for a product called **ek? Glasses** is designed to " *break* " face recognition. The frames reflect the observed light and infrared rays, thus creating a light in the middle of the face to confuse AI face detection

You can still choose not to participate in face scanning functions whenever the option is offered - for example when traveling or getting a driver's license. In addition, you can delete your social media and photo sharing accounts, avoid using face recognition features and phone apps.

However, there is little you can do to protect yourself from the growing security threats of face recognition technology.

Refer to some more articles:

1. Image of a test run by Hyperloop One in the Nevada desert
2. See the wonderful images of the world's first computer layout
3. Libratus - artificial intelligence has just defeated 4 players in poker games

Having fun!