It's time to face the ugly reality of face recognition

The use of A.I. to recognize faces is growing fast. Here's why you should be worried about your personal privacy.

By Mike Elgan
Contributing Columnist, Computerworld
MAR 18, 2017 4:01 AM PT

A hoax hit Facebook this week. Fake news about a fake app called Facezam claimed that the app could track down anyone by simply scanning their Facebook photos.

Thousands or millions of Facebook users fell for the hoax and freaked out. (A U.K. marketing agency created the hoax as a publicity stunt.)

The public reaction illustrates how confused people are about face recognition. In fact, everything the fake Facezam was said to do is easily done with real apps and sites.

The public is understandably hazy about the privacy and security risks of biometrics. Everybody knows biological features can be used to identify people. Police have been using fingerprints for decades, for example.

Technology has enabled a large number of new biometric identification systems that use fingerprints, iris scans, wrist vein scans, voice recognition and face recognition. But when it comes to the potential for privacy invasion, however, these various approaches are not equal.

Face recognition is 100 times more dangerous than all others

If you're concerned about biometric privacy violation, your concern should be focused heavily on face recognition.

There's a lot of public confusion, so I'm going to be extremely clear.

All biometric systems involve capturing biometric data, entering that data into a database, then capturing new data to run against the database looking for a match. They all work well for identifying individuals using computer analysis of their various body parts.

Most forms of biometric data are hard to capture. For example, explicit permission or knowledge is usually required to capture fingerprint, iris, vein and other biometric data. It's possible, for example, that your irises or veins have never been scanned even once.

Face recognition does not require permission or knowledge. Any photograph will do.

You have been photographed hundreds or thousands of times already. And with surveillance cameras, you're being photographed regularly. Every time you use an ATM, for example, you're having your picture taken, and that picture is associated in the bank's database with your name and bank account.

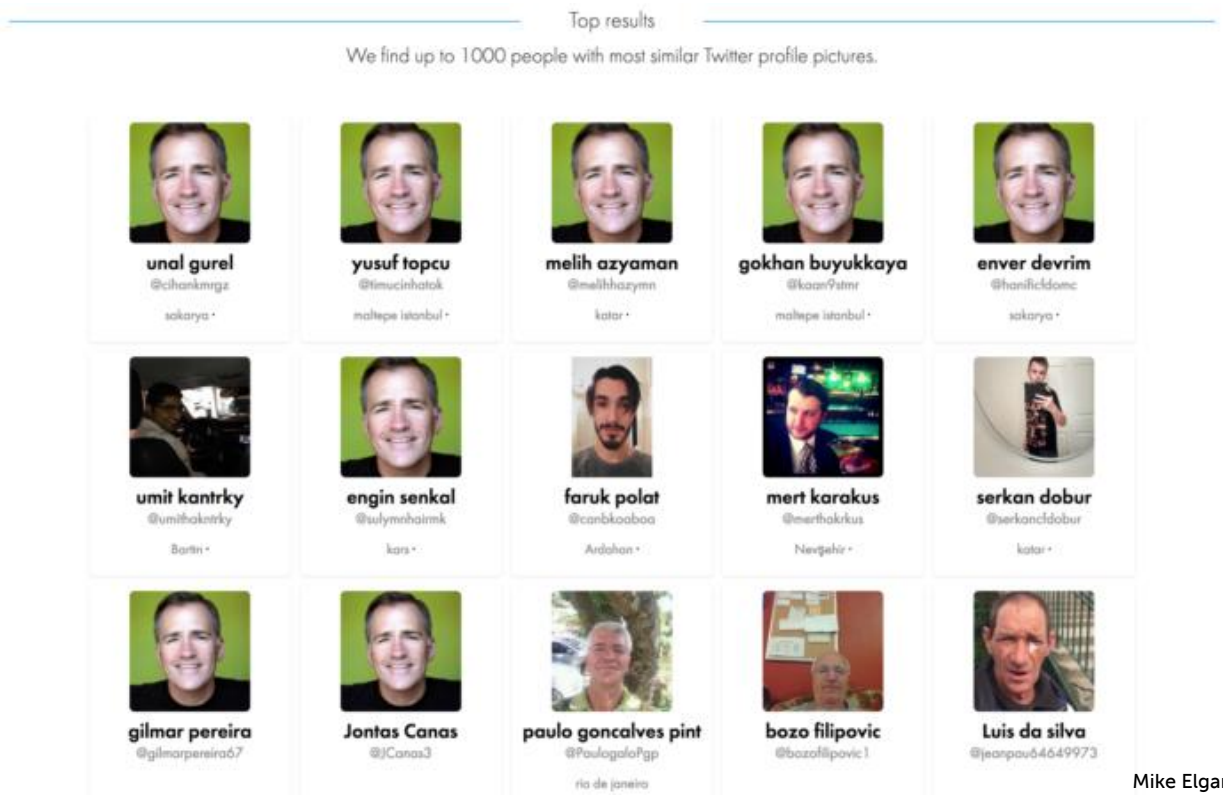
Photographs can be taken from a distance without the knowledge or permission of the target.

Other biometric data is private or more difficult to obtain without your knowledge or permission. For example, if you've been fingerprinted for a passport or by the police, you've agreed to it and those agencies will keep your data to themselves. If I provided you with somebody's fingerprints, you couldn't use that data unless you were a cop and had access to the database.

Pictures, on the other hand, are publicly available for anyone to access. Social networks, public picture sites and others make millions of people's biometric data (their snapshots) available to anyone in the world with an internet connection.

Pictures of faces are easy to connect to names. Once you have someone's name, you can usually find their home address, a list of their relatives, their phone number and other data.

This is what the fake Facezam claimed to be able to do. But I'll show you how to do it without Facezam. It takes less than three minutes and costs nothing to find a home address based on nothing but a photo.



Mike Elgan

The Russian face recognition site FindFace is a perfect tool for creepy stalkers. It's also useful for discovering that other people on Twitter are using your profile picture.

Here's how it's done:

1. Upload a picture of somebody's face to FindFace, a Russian face-recognition site.
2. FindFace will give you the search result of multiple Twitter accounts. Find the correct Twitter account, and it will tell you the person's name.
3. Copy and paste the name into a site called Family Tree Now. That will probably give you that person's home address, family members, age and other data.

You may now have a 100% positive ID on a person, which can be used to find out almost anything about them by searching government records, criminal records and the like.

Of course, this system isn't perfect. This trick might work less than half the time for a variety of reasons. (Some people don't have Twitter accounts, for example, or don't use their real photo or name on Twitter. And Family Tree Now may give you many people with the same name.)

But if you try this system with several photos of the same person, or for several people, you're certainly unlikely to work.

The solution, you might think, would be to delete or obscure your Twitter account. And given what I just told you, that would be a reasonable thing to do.

But I showed you this method only to bring home the reality of face recognition in a visceral way. FindFace represents a relatively minor risk compared to what's coming over the next few years.

Your face in photos

Another easy example is Google Photos. Just click here; this is the Google Photos "people" view. It demonstrates how Google automatically runs face recognition on all your photos, and groups pictures of people together. By clicking on any face, you'll see all the pictures of that person.

The most amazing fact about Google Photos is that anyone can add a name to each collection of photos.

That means anyone you know who has both taken your picture and who uses Google Photos can label that gallery of pictures with your name, thus telling Google's massive face recognition database who you are. (As someone with a tech-oriented family and who's active on Google+, I would guess that hundreds of people have connected my face to my name in Google's system.)

Just to be clear, it's not labeling specific photos as you. It's informing Google's A.I. that any or all the pictures of you are you, and so additional pictures will also get your name associated with them.

The same thing happens on Facebook. Users tag selfies and other photos, and tag their family and friends. This informs Facebook's industry-leading A.I. who's who. You'll notice that when you upload a picture of yourself, Facebook usually knows it's you.

Again, these are just available examples that are instantly accessible.

The truth is that your face is being constantly photographed for face recognition databases, and your face will be increasingly used for identification behind the scenes without your knowledge or permission.

Suddenly face recognition is everywhere

Rumors abound that best-selling smartphone lines will soon feature face recognition as their primary security scheme.

The Samsung Galaxy S8 and Galaxy S8+, which are expected to launch later this month, are rumored to include face recognition as part of their security systems. Face recognition could be used to unlock phones, verify Samsung Pay purchases, or both.

Other rumors suggest that Apple's upcoming iPhone 8 will also have face recognition. This outcome is less likely than the Samsung rumor. But Apple does have multiple patents for face recognition technology, including patents for using face recognition specifically for unlocking an iPhone.

A startup called Blue Line Technology offers face recognition for store security, and the technology is already being tested in several stores in Missouri, where the startup is located. It works by running face recognition on everyone coming toward the front door. If someone is wearing a mask, or if a recognized person is in the store's database as a known shoplifter, the doors won't open.

Airports in Japan, France, Canada, Australia and elsewhere are increasingly deploying face recognition systems. Most current programs hope to process all passengers at security checkpoints within the next few years.

Uber uses real-time face recognition in China and India. Drivers must scan their face before accepting any ride to verify that they aren't imposters or criminals looking to pick up unsuspecting passengers.

Cruise ships are embracing face recognition technology, too; it enables passengers to make purchases without carrying credit cards.

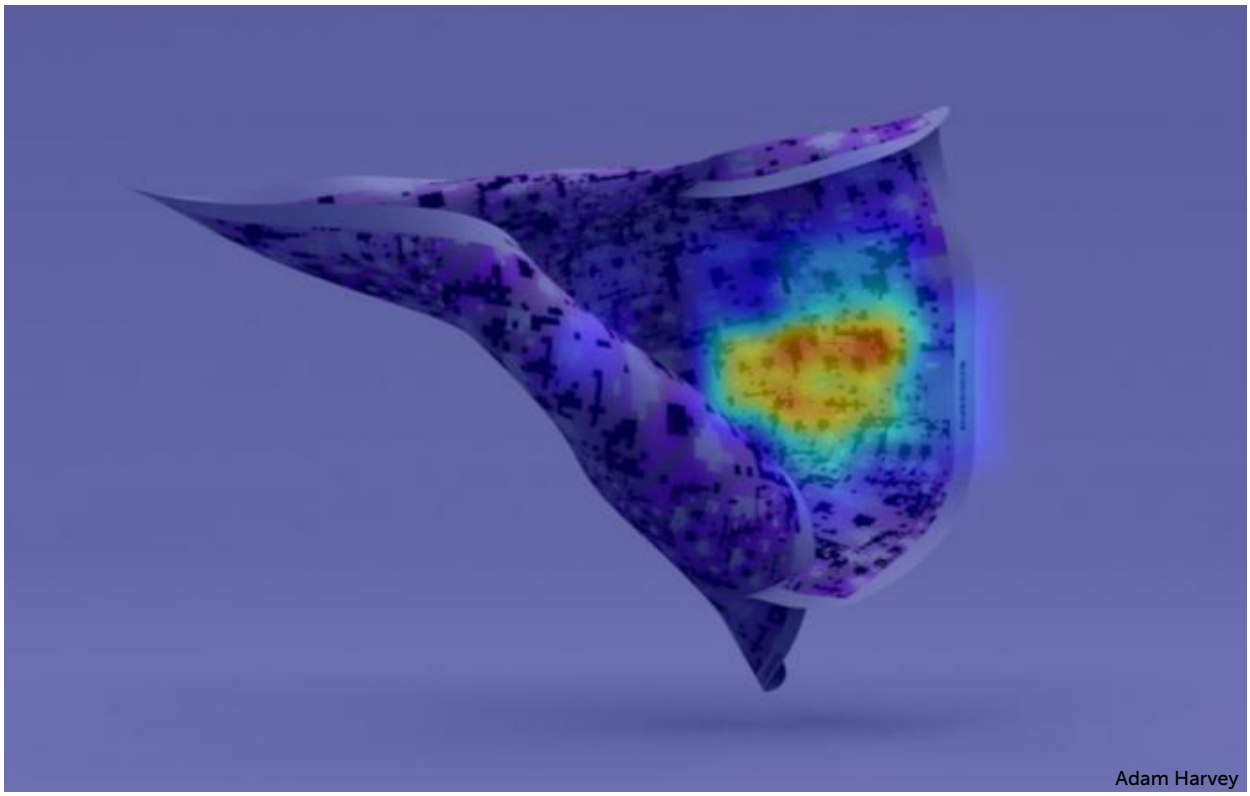
and U.S. states are increasingly using face recognition for driver's licenses and IDs. One next Hancock or Strawberry suspect claims to have no identification, a quick face photo will suffice.

In short, face recognition is going mainstream. The public is being led down a path where everybody accepts face recognition scanning as a normal part of everyday life.

You can foil face recognition (but you probably won't)

A character on the TV series *Minority Report* sports face tattoos designed to fool face recognition.

Is that really our future?



Designer Adam Harvey has created a fabric with a pattern designed to produce false positives in face-recognition systems.

A cottage industry of products designed to protect against face recognition is emerging. These products illustrate just how unlikely protection is.

For example, a designer named Adam Harvey invented a fabric that's supposed to fool face-recognition computers into thinking the cloth is covered with faces. As the system tries to recognize the multiple faces in the pattern, the confidence score of the match

should go down.

Harvey has also explored [illegible] styles and makeup that could fool face recognition technology.

A Kickstarter campaign for a product called ekō Glasses is designed to disrupt face recognition. The frames are highly reflective of both visible and infrared light, and therefore create a bright light in the middle of your face to confuse face-recognition A.I.

These schemes, while thought-provoking, aren't practical defenses against pervasive face scanning.

You can still opt out of face scanning whenever you're given the option -- for example while traveling or getting your driver's license. You can delete your social media and photo sharing accounts. And you can avoid using face recognition features and apps with your phone.

Beyond that, there's little you can do to protect yourself from the growing privacy threat of face recognition technology.

To express your thoughts on Computerworld content, visit Computerworld's Facebook page, LinkedIn page and Twitter stream.

Mike Elgan writes about technology and tech culture. Contact Mike and learn more about him at http://elgan.com/about.

Follow