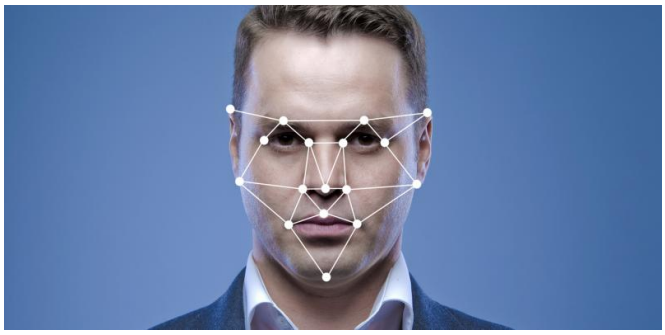
Facial recognition is increasingly common, but how does it work?

5 April 2017, by Jessica Gabel Cino



Mapping a face is the starting point. Credit: Anton Watman/shutterstock.com

The Trump administration's efforts to impose new immigration rules drew attention – and legal fire – for its restrictions on the ability of people born in certain majority Muslim countries to enter the U.S. In the frenzy of concern, an obscure piece of the executive orders did not get scrutinized, or even noticed, very much: its expansion of facial recognition systems in major U.S. airports to monitor people leaving the U.S., in hopes of catching people who have overstayed their visas or are wanted in criminal investigations.

It's a much more powerful version of the method your phone or computer might use to identify friends in your photos. Using computers to recognize people's faces and validate their identities can streamline access control for secure corporate and government buildings or devices. Some systems can identify known or suspected criminals. Businesses can analyze their customers' faces to help tailor marketing strategies to people of different genders, ages and ethnic backgrounds. There are even consumer services that take advantage of facial recognition, like virtual eyeglass fitting and virtual makeovers.

There are also serious privacy concerns as government agencies and companies are more able to track individuals through their communities, and even around the world. The facial recognition market is worth approximately US$3 billion and is expected to grow to $6 billion by 2021. Surveillance is a large reason for growth; government entities are the primary consumers. The FBI has a database with images of approximately half the U.S. population. There are also fears of people using facial recognition to engage in online harassment or even real-world stalking.

As facial recognition becomes more common, we must know how it works. As someone who studies and researches the legal implications of new technology in criminal investigations, I believe it's important to understand what it can and can't do, and how the technology is progressing. Only then can we have informed discussions about when and how to use computers to recognize that most human of features – our faces.

How it works

As one of several methods of what are called "biometric" identification systems, facial recognition examines physical features of a person's body in an attempt to uniquely distinguish one person from all the others. Other forms of this type of work include the very common fingerprint matching, retina scanning, iris scanning (using a more readily observable part of the eye) and even voice recognition.

All of these systems take in data – often an image – from an unknown person, analyze the data in that input, and attempt to match them to existing entries in an database of known people's faces or voices. Facial recognition does this in three steps: detection, faceprint creation, and verification or identification.

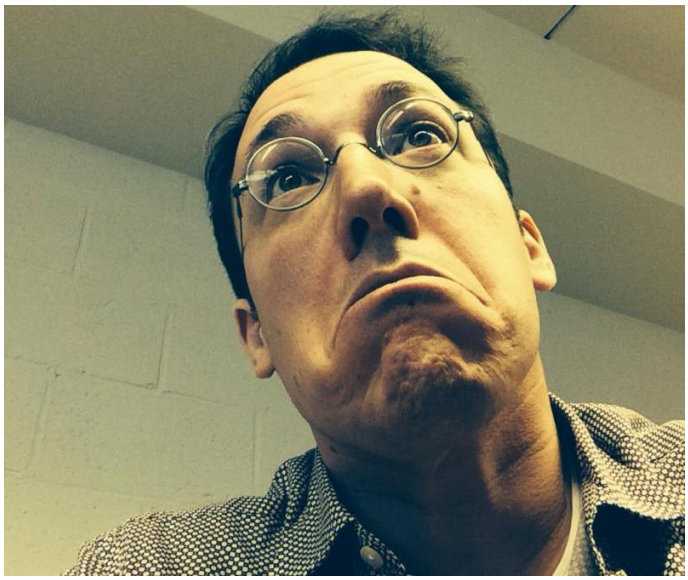
When an image is captured, computer software analyzes it to identify where the faces are in, say, a

crowd of people. In a mall, for example, security cameras will feed into a computer with facial recognition software to identify faces in the video feed.

Once the system has identified any potential faces in an image, it looks more closely at each one. Sometimes the image needs to be reoriented or resized. A face very close to the camera may seem tilted or stretched slightly; someone farther back from the camera may appear smaller or even partially hidden from view.

When the software has arrived at a proper size and orientation for the face, it looks even more closely, seeking to create what is called a "faceprint." Much like a fingerprint record, a faceprint is a set of characteristics that, taken together, uniquely identify one person's particular face. Elements of a faceprint include the relative locations of facial features, like eyes, eyebrows and nose shape. A person who has small eyes, thick eyebrows and a long narrow nose will have a very different faceprint from someone with large eyes, thin eyebrows and a wide nose. Eyes are a key factor in accuracy. Large dark sunglasses are more likely to reduce the accuracy of the software than facial hair or regular prescription glasses.

A faceprint can be compared with a single photo to verify the identity of a known person, say an employee seeking to enter a secure area. Faceprints can also be compared to databases of many images in hopes of identifying an unknown person.



Uneven light, a bad angle and a strange expression can cause facial recognition to fail. Credit: rouadec/flickr, CC BY

It's not always easy

A key factor affecting how well facial recognition works is lighting. An evenly lit face seen directly from the front, with no shadows and nothing blocking the camera's view, is the best. In addition, whether an image of a face contrasts well with its background, and how far away it is from the camera, can help or hurt the facial recognition process.

Another very important challenge to successful facial recognition is the degree to which the person being identified cooperates with – or is even aware of – the process. People who know they are using facial recognition, such as that employee trying to get into a restricted room, are relatively easy to work with. They are able to look directly at the camera in proper lighting, to make things optimal for the software analysis.

Other people don't know their faces are being analyzed – and may not even know they're being surveilled by these systems at all. Images of their faces are trickier to analyze; a face picked out of a crowd shot may have to be digitally transformed and zoomed in before it can generate a faceprint.

That leaves more room for the system to misidentify the person.

Potential problems

When a facial recognition system incorrectly identifies a person, that can cause a number of potential problems, depending on what kind of error it is. A system restricting access to a specific location could wrongly admit an unauthorized person – if, say, she was wearing a disguise or even just looked similar enough to someone who should be allowed in. Or it could block the entry of an authorized person by failing to correctly identify her.

In law enforcement, surveillance cameras aren't always able to get very good images of a suspect's face. That could mean identifying an innocent person as a suspect – or even failing to recognize that a known criminal just ran afoul of the law again.

Regardless of how accurate it appears to be on TV crime dramas, there is room for error, though the technology is improving. The National Institute of Standards and Technology has estimated that stated error rates are declining 50 percent every two years, and are currently around 0.8 percent. That's better than voice recognition, which has error rates above 6 percent. But facial recognition may still be more error-prone than iris scanning and fingerprint scanning.

Privacy concerns

Even if it's accurate, though – and perhaps even more so as accuracy improves – facial recognition raises privacy concerns. One of the chief worries is that, much like the rise of DNA databases, facial features and photos are being warehoused by government agencies, which will become able to track people and erase any notion of privacy or anonymity.

New privacy problems are cropping up all the time, too. A new smartphone app, FindFace, allows people to take a person's photo and use facial recognition to find their social media accounts. Ostensibly a convenient way to connect with friends and co-workers, the app invites misuse. People can use it to expose identities and harass others.

These new capabilities are also raising concern about other malicious uses of publicly available images. For example, when police issue alerts about missing children, they often include a photograph of the child's face. There is little regulation or oversight, so nobody knows whether those images are also being entered into facial recognition systems.

This, of course, doesn't even touch on using facial recognition tools along with other technologies like police body cameras, geolocation software and machine learning to assist in real-time tracking. That goes beyond simple identification and into the realm of where someone has been, and where the software predicts they will go. Combining technologies offers attractive options for crime fighting, and deepens the fissures in our privacy.

Technology provides powerful tools, and the law is often ill-equipped to keep pace with new developments. But if we're going to be using facial recognition in immigration and law enforcement decisions, we must engage with its possibilities and its detriments, and understand the issues of accuracy, privacy and ethics this new capability raises.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation