UNMASKED

Facial recognition software could soon ID you in any photo

By **John Bohannon**

IMAGE: WILLIAM DUKE

Appear in a photo taken at a protest march, a gay bar, or an abortion clinic, and your friends might recognize you. But a machine probably won't—at least for now. Unless a computer has been tasked to look for you, has trained on dozens of photos of your face, and has high-quality images to examine, your anonymity is safe. Nor is it yet possible for a computer to scour the Internet and find you in random, uncaptioned photos. But within the walled garden of Facebook, which contains by far the largest collection of personal photographs in the world, the technology for doing all that is beginning to blossom.

Catapulting the California-based company beyond other corporate players in the field, Facebook's DeepFace system is now as accurate as a human being at a few constrained facial recognition tasks. The intention is not to invade the privacy of Facebook's more than 1.3 billion active users, insists Yann LeCun, a computer scientist at New York University in New York City who directs Facebook's artificial intelligence research, but rather to protect it. Once DeepFace identifies your face in one of the 400 million new photos that users upload every day, "you will get an alert from Facebook telling you that you appear in the picture," he explains. "You can then choose to blur out your face from the picture to protect your privacy." Many people, however, are troubled by the prospect of being identified at all—especially in strangers' photographs. Facebook is already using the system, although its face-tagging system only reveals to you the identities of your "friends."

DeepFace isn't the only horse in the race. The U.S. government has poured funding into university-based facial recognition research. And in the private sector, Google and other companies are pursuing their own projects to automatically identify people who appear in photos and videos.

Exactly how automated facial recognition will be used—and how the law may limit it—is unclear. But once the technology matures, it is bound to create as many privacy problems as it solves. "The genie

Corrected 2 February 2015; see full text.

Published by AAAS

is, or soon will be, out of the bottle," says Brian Mennecke, an information systems researcher at Iowa State University in Ames who studies privacy. "There will be no going back."

SIMPLY DETECTING FACES is easy for a computer, at least compared with detecting common objects like flowers, blankets, and lamps. Nearly all faces have the same features—eyes, ears, nose, and mouth—in the same relative positions. This consistency provides such an efficient computational shortcut that "we've been able to detect faces in images for about 2 decades," LeCun says. Even the puny computers in cheap consumer cameras have long been able to detect and focus on faces.

But "identifying a face is a much harder problem than detecting it," LeCun says. Your face uniquely identifies you. But unlike your fingerprints, it is constantly changing. Just smile and your face is transformed. The corners of your eyes wrinkle, your nostrils flare, and your teeth show. Throw your head back with laughter and the apparent shape of your face contorts. Even when you wear the same expression, your hair varies from photo to photo, all the more so after a visit to the hairdresser. And yet most people can spot you effortlessly in a series of photos, even if they've seen you in just one.

In terms of perceiving the world around us, facial recognition may be "the single most impressive thing that the human brain can do," says Erik Learned-Miller, a computer scientist at the University of Massachusetts, Amherst. By contrast, computers struggle with what researchers call the problem of A-PIE: aging, pose, illumination, and expression. These sources of noise drown out the subtle differences that distinguish one person's face from another.

Thanks to an approach called deep learning, computers are gaining ground fast. Like all machine learning techniques, deep learning begins with a set of training data—in this case, massive data sets of labeled faces, ideally including multiple photos of each person. Learned-Miller helped create one such library, called Labeled Faces in the Wild (LFW), which is like the ultimate tabloid magazine: 13,000 photographs scraped from the Web containing the faces of 5749 celebrities, some appearing in just a few photos and others in dozens. Because it is online and free to use, LFW has become the most popular benchmark for machine vision researchers honing facial recognition algorithms.

To a computer, faces are nothing more than collections of lighter and darker pixels. The training of a deep learning system begins by letting the system compare faces and discover features on its own: eyes and noses, for instance, as well as statistical features that make no intuitive sense to humans. "You let the machine and data speak," says Yaniv Taigman, DeepFace's lead engineer, who's based at Facebook's Menlo Park headquarters. The system first clusters the pixels of a face into elements such as edges that define contours. Subsequent layers of processing combine elements into nonintuitive, statistical features that faces have in common but are different enough to discriminate them.

This is the "deep" in deep learning: The input for each processing layer is the output of the layer beneath. The end result of the training is a representational model of the human face: a statistical machine that compares images of faces and guesses whether they belong to the same person. The more faces the system trains on, the more accurate the guesses.

The DeepFace team created a buzz in the machine vision community when they described their creation in a paper published last March on Facebook's website. One benchmark for facial recognition is identifying whether faces in two photographs from the LFW data set belong to the same celebrity. Humans get it right about 98% of the time. The DeepFace team reported an accuracy of 97.35%—a full 27% better than the rest of the field.

Some of DeepFace's advantages are from its clever programming. For example, it overcomes part of the A-PIE problem by accounting for a face's 3D shape. If photos show people from the side, the program uses what it can see of the faces to reconstruct the likely face-forward visage. This "alignment" step makes DeepFace far more efficient, Taigman says. "We're able to focus most of the [system's] capacity on the subtle differences."

"The method runs in a fraction of a second on a single [computer] core," Taigman says. That's efficient enough for DeepFace to work on a smart phone. And it's lean, representing each face as a string of code called a 256-bit hash. That unique representation is as compact as this very sentence. In principle, a database of the facial identities of 1 billion people could fit on a thumb drive.

But DeepFace's greatest advantage—and the aspect of the project that has sparked the most rancor—is its training data. The DeepFace paper breezily mentions the existence of a data set called SFC, for Social Face Classification, a library of 4.4 million labeled faces harvested from the Facebook pages of 4030 users. Although users give Facebook permission to use their personal data when they sign up for the website, the DeepFace research paper makes no mention of the consent of the photos' owners.

"JUST AS CREEPY as it sounds," blared the headline of an article in *The Huffington Post* describing DeepFace a week after it came out. Commenting on *The Huffington Post*'s piece, one reader wrote: "It is obvious that police and other law enforcement authorities will use this technology and search through our photos without us even knowing." Facebook has confirmed that it provides law enforcement with access

Is that really you?

Just glance at these photos and it is immediately obvious that you're looking at the same person (computer scientist Erik Learned-Miller). To a computer, however, almost every parameter that can be measured varies from image to image, stymieing its ability to identify a face. A technique called deep learning squelches noise to reveal statistical features that these visages have in common, allowing a computer to predict correctly that they all belong to the same individual.

PHOTOS: COURTESY OF ERIK LEARNED-MILLER

Corrected 2 February 2015; see full text.

to user data when it is compelled by a judge's order.

"People are very scared," Learned-Miller says. But he believes the fears are misplaced. "If a company like Facebook really oversteps the bounds of what is ruled as acceptable by society … they could go out of business. If they break laws, then they can be shut down and people can be arrested." He says that the suspicion stems from the lack of transparency. Whereas academic researchers must obtain explicit consent from people to use private data for research, those who click "agree" on Facebook's end-user license agreement (EULA) grant the company permission to use their data with few strings attached. Such online contracts "are the antithesis of transparency," Learned-Miller says. "No one really knows what they're getting into." Last year, the company introduced a friendly looking dinosaur cartoon that pops up on the screen and occasionally reminds users of their privacy settings, and it boiled down the EULA language from 9000 words to 2700.

There is already a bustling trade in private data—some legal, others not—and facial identity will become another hot commodity, Iowa State's Mennecke predicts. For example, facial IDs could allow advertisers to follow and profile you wherever there's a camera—enabling them to cater to your preferences or even offer different prices depending on what they know about your shopping habits or demographics. But what "freaks people out," Mennecke says, "is the idea that some stranger on the street can pick you out of a crowd. … [You] can't realistically evade facial recognition." FacialNetwork, a U.S. company, is using its own deep learning system to develop an app called NameTag that identifies faces with a smart phone or a wearable device like Google Glass. NameTag reveals not only a person's name, but also whatever else can be discovered from social media, dating websites, and criminal databases. Facebook moved fast to contain the scandal; it sent FacialNetwork a cease and desist letter to stop it from harvesting user information. "We don't provide this kind of information to other companies, and we don't have any plans to do so in the future," a Facebook representative told *Science* by e-mail.

The potential commercial applications of better facial recognition are "troublesome," Learned-Miller says, but he worries more about how governments could abuse the technology. "I'm 100% pro–Edward Snowden," Learned-Miller says, referring to the former National Security Agency contractor who in 2013 divulged the U.S. government's massive surveillance of e-mail and phone records of U.S. citizens (see p. 495). "We have to be vigilant," he says.

Learned-Miller's sentiment is striking, considering that he is funded in part by the U.S. Intelligence Advanced Research Projects Activity to develop a facial recognition project called Janus. Perhaps that's all the more reason to take his warning seriously. ■

IMAGE: WILLIAM DUKE

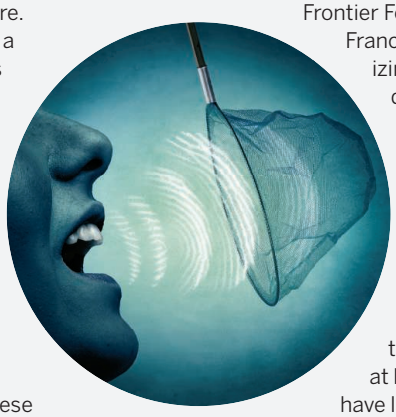
THE PRIVACY ARMS RACE

When your voice betrays you

By **David Shultz**

"My voice is my password." You may soon find yourself saying that—or perhaps you already do—when you call your bank or credit card company. Like a fingerprint or an iris scan, every voice is unique, and security companies have embraced voice recognition as a convenient new layer of authentication. But experts worry that voiceprints could be used to identify speakers without their consent, infringing on their privacy and freedom of speech.

Voiceprints are created by recording a segment of speech and analyzing the frequencies at which the sound is concentrated. Physical traits like the length of a speaker's vocal tract or a missing tooth leave their mark on a voice, creating a unique spectral signature.



Unlike a fingerprint, a voiceprint incorporates behavioral elements as well; traits like cadence, dialect, and accent easily distinguish, say, Christopher Walken from Morgan Freeman. Speech recognition systems, which aim to understand what is being said, minimize these differences, normalizing pitch and overlooking pauses and accents. But for identifying a unique individual, the disparities are crucial.

Because voiceprint systems typically have the user repeat a standard phrase, identity thieves could theoretically record such phrases and play them back to fool the technology. The systems are designed to detect recordings or synthesized speech, however. An even safer alternative is to ask the customer to repeat a randomly chosen bit of text. "The system will prompt the user, 'Now say this phrase,'" says Vlad Sejnoha, the chief technology officer at Nuance Communications Inc. in Burlington, Massachusetts, an industry leader in voice recognition technology. "It's hard to come prepared with all possible recordings." Some systems require no pass phrase at all but rather analyze a person's voice by listening in the background—for instance, as they talk to a sales representative—and compare it with a stored voiceprint.

Demand for voiceprint authentication is skyrocketing. Nuance Director Brett Beranek says the company has logged more than 35 million unique voiceprints in the past 24 months, compared with only 10 million over the previous 10 years. But massive voiceprint databases could make anonymity a scarcer commodity.

"Like other biometrics, voiceprint technology does raise privacy issues, because it gives companies and the government the ability to identify people even without their knowledge," says Jennifer Lynch, an attorney at the Electronic Frontier Foundation in San Francisco, California, specializing in biometrics. "That does create a challenge to anonymous speech protection" as enshrined in the United States' First Amendment, she says.

How and when voiceprints can be captured legally is murky at best. Many countries have legislation regulating wiretapping, but voice recognition adds a major new dimension that most lawmakers have yet to consider, Lynch says. If the past is any guide, companies have massive financial incentives to track consumers' movements and habits. Recognizing someone as soon as they pick up the phone or approach a cashier will open up marketing opportunities—as well as ease transactions for the consumer. As with many new authentication technologies, the balance between convenience and privacy has yet to be struck. ■

Corrected 2 February 2015; see full text.

Published by AAAS