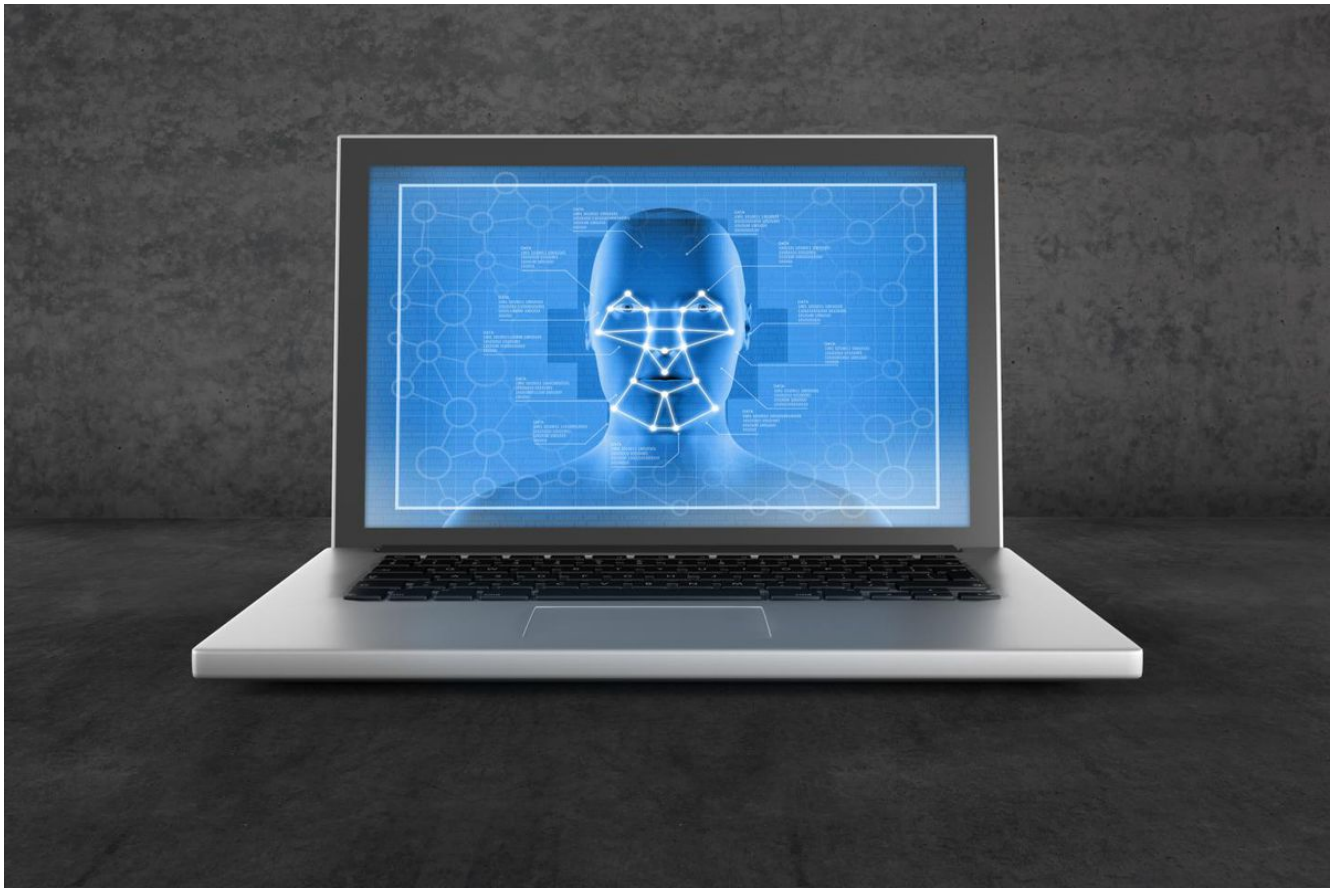
OPINION

You don't own your own face: Ever-more-sophisticated technology will allow the likes of Facebook to locate you, and profit from it

By JOSEPH J. ATICK
NEW YORK DAILY NEWS | AUG 27, 2017



Face it (Maxiphoto/Getty Images/iStockphoto)

Have you been tagged in a Facebook photo lately? Think this is a harmless or fun act? In reality, you are feeding one of the scariest beasts in the technological forest: You are accelerating the development of a massive face recognition engine that has the potential to recognize every man, woman and child on this planet.

Not only in airports, but on city sidewalks. In stores. In hospitals. We could be hurtling toward a future where anonymity as we know it is no longer possible.

While face recognition was invented in the early 1990s by a handful of pioneers, it is the hundreds of millions of social media users today who are unconsciously perfecting a technology with the power to end privacy, not just online but in the physical world.

This technology is now growing with a speed and sophistication few imaged possible. We, the people - who own our faces - have lost control over how they are used.

But we don't have to surrender. We can and must pass laws to guide the industry and guard against the abuse of face recognition. And we must do it soon. As someone who was part of the handful pioneers that invented face recognition, I feel it is my responsibility to warn against a creepy side that could emerge.

There's nothing new about the basic technology here. Computers have been able to automatically detect faces in photographs or from video and identify who they are for some time. You saw it in James Bond films nearly two decades before the technology was actually invented; and over the last 15 years, the technology, propelled by legitimate security needs in the aftermath of 9/11, evolved dramatically from those fictional depictions to become very real.

Even more recently, it received major boosts from the mainstream IT industry and has become familiar to the consumer through applications from Facebook, Google, Apple, Microsoft as well as from a myriad of mobile, payment and banking applications. It is even rumored that the next iPhone will rely on face recognition as the primary method for controlling access.

Many of these applications are perfectly welcome, especially those that help defeat ID theft and other crimes.

Today, along with technologies that measure patterns of fingerprints and the iris of the eye, face recognition represents a cornerstone in the ensemble of modern biometrics which aim to establish individual identity based on the uniqueness of measurable physical characteristics of the human body, such as the geometry of the human face.

Programs that use biometrics - to uniquely identify individuals to combat identity fraud, identify criminals from surveillance photos, secure mobile transactions, expedite border crossings or dispense social services - are now very common worldwide and their scope continues to grow.

For example, New York Police Department has one of the world's most advanced face recognition programs for forensic investigation, only matched in capabilities by the so-called Next Generation Identification program of the FBI.

But when used for large-scale identification, as opposed to simple authentication that you are who you say you are, facial recognition raises some serious concerns. Unlike DNA analysis, fingerprints and other biometrics, it and only it can be surreptitiously performed from a distance, without a subject's cooperation or consent. And it works from ordinary photographs without the need for special scanners or cameras.

These concerns are not new; they immediately came up as the technology began to be commercialized back in the 1990s within the context of law enforcement applications.

But, today, we are in a different era and the problem is much larger. The simplistic self-regulations that worked back then will not work now. The technology has escaped the orbit of control.

What changed everything is the abundance of face photographs on social media. Face recognition systems are as good as their reference databases of known faces, against which they perform the recognition. This is the gallery of faces. Without it, the system is said to be face-blind.

Back when face recognition was invented, building a face gallery was a big challenge. Most photographs had to be scanned one by one and added to the database manually. This meant that galleries were limited in size and the impact of these early systems was limited.

For example, for law enforcement applications, all we had to make sure is that the gallery contained faces that were legitimate targets for law enforcement such as individuals with warrants or felony convictions, or who are part of active investigations. For the other 99% of the population, face recognition systems would be blind.

Anonymity and privacy would still be enjoyed by the clear majority. At the time when we invented face recognition, we did not imagine that the day would come when this clear majority would be voluntarily feeding images of their faces into massive databases such as Facebook.

Social media users today get the credit for having built the world's largest and highest quality face galleries, orders of magnitude larger than those maintained by the FBI. This is crowdsourcing at its best.

In addition to serving as reference galleries, the massive abundance of face images allows the deployment of a class of intelligent algorithms called "deep learning." These powerful data processing methods automatically learn to classify image content through examples. Software developers do not have to code the classifiers needed to tell a computer what a face is in an image and who it belongs to (eye, mouth, nose and other feature detectors).

All they have to do is show computers a large number of examples of photos of faces, and deep learning takes care of the rest. The result is a software engine that learns what makes a face a face and not a car or an animal, and that can distinguish billions of faces, in countless settings and at countless different angles, from one another.

This class of face recognition engines has already surpassed the accuracy of the old systems and has even exceeded human performance, as demonstrated by the Facebook

research and development team.

As users upload more and more images, for example to Facebook, each image is processed automatically to detect faces and each detected face is converted to specialized mathematical codes the so called faceprints. These highly compact codes, which don't even take that much computer memory to store, capture the uniqueness of our faces, as, in principle, no two faceprints are alike (except for identical twins).

Today it is estimated that Facebook maintains a database of over 1 billion faceprints. Thousands of processors are involved, distributed over thousands of servers in multiple computing farms - just to deal with faceprints.

Facebook justifies this massive undertaking by the need to support a popular feature. While this is all well and good - it's neat to see photos tagged automatically - it sidesteps what should be serious user concerns.

By default, everyone is in opt-in mode, submitting to the face recognition, and one would have to consciously take action to opt-out, which is an effort that requires some sophistication to navigate the complex privacy policy.

It makes one wonder, if Facebook were required to put a disclaimer or a warning (similar to that on cigarette packs) that would say something like "faceprints can be used to recognize you among billions of others, and they can be used almost anywhere. Give consent at your own risk," how many users would opt-in in reality?

And while it may be true that Facebook is answering a consumer need today, that says nothing about how they might use the data they're collecting tomorrow. This ready-made database can be used to achieve the unthinkable: the linking of online and offline personas of billions of people in a manner that would kill privacy and anonymity forever.

It can allow you to be identified offline and linked to the massive amount of information that is known about you online from your social footprint. That data can be

used to help companies sell their products or services, or for who knows what other purposes.

Would it be acceptable to live in a world where you can be recognized or stalked by strangers in public places, or by marketers or retailers who would hound you to buy specific products based on your pattern of purchases and your likes on your user profile, thanks to offline behavioral advertising linked to online profiling?

Would you be willing to be tracked even when you have done nothing to warrant being tracked?

Should private companies be allowed to have such massive identity databases and such potential power over the entire population, especially in a country such as the U.S. that prides itself in not having a national ID because of fears of being tracked by the government?

All these surveillance applications by the private sector would be for the most part perfectly legal in the United States, apart from in a handful of states such as Illinois that have adopted some biometric data protection laws.

The technology is clearly moving much faster than the law. Politicians appear to be hesitant to tackle this issue.

I had hoped that the industry giants, such as Facebook, Google, Apple and Microsoft, working with the biometrics industry, would adopt a new code of conduct to protect faceprints, and to treat them and other biometric data with the same sensitivity as one should treat medical and financial records.

Unfortunately, there does not appear to be any initiative in that direction. The industry sees no incentive nor need to act, as they are not compelled to do so. In fact, the health and financial industry would have been less careful as well if it were not for the fact there are already strong federal laws requiring data protection in these domains.

I now believe that a federal law is also needed to do the same for faceprints. The industry tech giants assure us they have no plans to turn on privacy-invading applications already developed in their shops, but can we afford to take them at their word, when there is a significant economic incentive to do otherwise down the line? In fact, records and interviews with lawmakers show that industry giants such as Facebook are stepping up their lobbying activity in opposition to such legislation.

Core to such legislation needs to be the issue of consent, which would affirm the basic principle that faceprints are owned by the faces they were extracted from, and that explicit and informed consent should be required before they are exploited for specific ends. That may sound simple, but it's essential - and it runs contrary to the industry's current assumption.

Such a federal law should be welcomed by an enlightened industry since it would eliminate the need to deal with the confusing patchwork of state legislation regarding biometric data that is emerging right now in the absence of federal law.

This is not a difficult undertaking. Europe has adopted an omnibus legislation called General Data Protection Regulation, which will become enforceable in May 2018, to strengthen and unify personal data protection for all individuals within the EU. Something similar is needed in the U.S.

As someone who witnessed the birth of face recognition and accompanied it through its formative years, it is my dream to see it mature, adding safety, security and convenience to the consumer without taking away their control of their own privacy or their personal data. It can be done if there is the right political will.

Atick, one of the inventors of face recognition in the early 1990s, is chairman of the Identity Counsel and ID4Africa, movements to give legal identity for all around the world by 2030.

Topics: facebook, technology, featured opinion

CONNECT

TRIBUNE PUBLISHING

Chicago Tribune

Orlando Sentinel

The Morning Call of Pa.

Daily Press of Va.

The Daily Meal

The Baltimore Sun

Sun Sentinel of Fla.

Hartford Courant

The Virginian-Pilot

Studio 1847

COMPANY INFO

Careers

Help Center

Manage Web Notifications

Place an Ad

Media Kit

Privacy Policy

Terms of Service

Contact Us

Site Map

Manage Subscription

Contests

Special Sections

Daily News archives

About Us