The **Dangers** of
FACIAL
RECOGNITION TECHNOLOGY

SELFDEFENSEFUND.COM

SDF

[MATCH]

John Doe

AGE	35	HEIGHT	5'11"
Occupation			Manager
Interests			Technology, VR, Travel
Location			London

ID 34593457834 HASHCODE 2AB4 CF23 EF98 DA57
CHECKSUM 893428657843578265785 DB GeneralPublic2A

MATCH 99%

THE DANGERS OF FACIAL RECOGNITION TECHNOLOGY

The facial recognition technology has been gaining traction in the market lately. Whether it is, biometric authentication, identifying shoplifters, adding to home security, or automatically being tagged on social media platforms, the technology is driving innovation across almost every sector. But, is the technology safe?

The data that is gathered and mined for facial recognition to work is people's information. For instance, Facebook's auto-tag feature on the photos uploaded has attracted a lot of criticism for the social media giant. The problem was that Facebook never sought permission from its users to activate the new feature for their profiles, in turn, jeopardizing their privacy and security. And, consequently, they had to also pay for it after settling the lawsuit against them in the form of $550 million.

There is no doubt that technology brings humongous opportunities to the table and makes lives easier, but what it asks in return, concludes into a complicated technology-human relationship.

WORKING ON FACIAL RECOGNITION TECHNOLOGY

Facial Recognition technology is a programmed system that analyzes digital images or video footage for identifying and verifying an individual's identity. It does so by mapping the user data across databases avail-able. And, that is not it! The technology also analyzes the personal data of the identified person, which brings a threat to society.
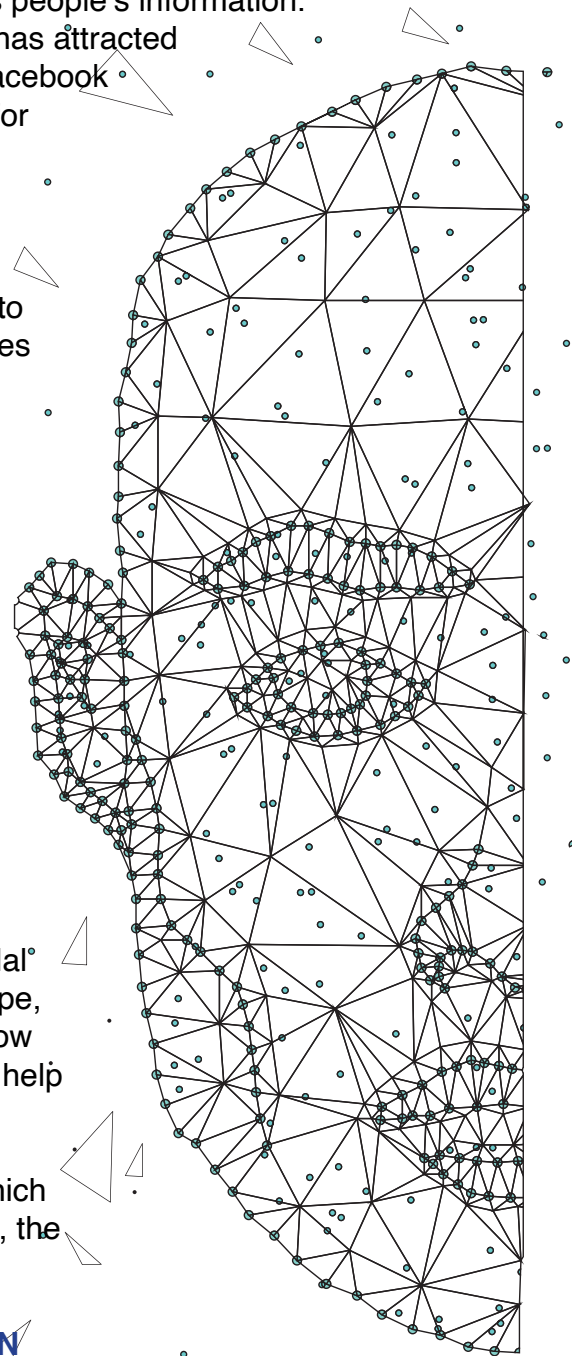
The process of recognizing the identity of an individual, through this technology is as follows: The system captures the images or video stills for scrutiny. The system works at its best when the person is looking right into the camera at a 90-degree angle.

The system reads and analyzes the geometry of the face using nodal points, i.e., the distance between eyes, nose width, cheekbone shape, eye socket depth, and jawline length. You would be surprised to know that a human face includes about 80 such nodal points, which then help in defining the facial signature.

The facial signature exists in the form of a mathematical formula which is then mapped across the data-bases available. If there is a match, the identity of a person gets verified along with other supporting data.

HERE ARE THE HARMFUL EFFECTS OF FACIAL RECOGNITION TECHNOLOGY

Now that you understand the working of a facial recognition system, here are some of the risks of using the technology.

1. THREAT TO PRIVACY

Data collection and its ongoing accessibility by the facial recognition system is conducted by businesses without the user's permission. It is similar to a stranger clicking your photographs on a street without you even knowing it. Doesn't that sound bizarre?

To worsen the situation, the data and facial signature would be stored across databases for any future references. Just like what Facebook does, as already mentioned above. The funny part is that these systems are not even 100 percent accurate. Imagine two people with familiar face geometries and features being misinterpreted by the system. It would be an identity hoax that would lead to confusion down the line.

2. THE SECURITY ISSUE

The introduction of the facial recognition system is certainly good technological progress as it is adding to ease of identifying criminals who tend to pose several identities. Not only the public security sector, but other sectors across the globe are gaining advantage from the technology too. But, that doesn't mean that one needs to overlook the bigger picture.

The databases that accommodate the A-Z of data of an individual are stored in virtual Cloud servers. This would mean that the data is vulnerable as it can be possibly breached
By hackers. This isn't an ideal scenario at all!

Analyze the worst-case scenarios – Information can be accessed illegally, data can be stolen, data can be replaced with inaccurate data, data can be erased from the databases, data can be used for conducting illegal activities, and data can be sold inappropriately on the dark web. All of the dangers are equally intense and add to anxiety and fear. So again, do you think facial technology is worth all of it?

3. THE IDENTITY HOAX

Assume this scenario – John committed a crime and is currently running from being penalized in the court of law. He has a doppelganger, Liam, with almost the same facial features. Liam is a banker and lives a reputed life. Liam is heading on a holiday with his family members to Miami, and authorities stop him at the airport for investigation.

Liam did not do anything, so what exactly went wrong? The facial recognition system at the airport mapped him incorrectly and concluded him to be John. The actual criminal runs away and a reputed gentle-man pays for the price. Now, that is called an identity hoax.

Facial recognition system is still an evolving technology, which should not be relied on completely. This could even pose a threat to the technology holders. Because later, people like Liam can file lawsuits against the misidentification and are highly likely to win. Indeed, a scary situation both ways.

4. INTENSIFYING CRIMINAL OFFENSES

People have a right to live their lives the way they want, and the same applies to their occupational preferences and lifestyle. Nobody gets the right to use the destructive power of technology to stalk a person and harass them for their life choices.

It seems that facial recognition systems have been contributing to such offenses lately. A Russian face recognition app, "Find Face," identified women and also harassed them, as the system claimed them to be working for pornography websites. This dark part of the technology was totally uncalled for.

The above situation also gives an idea of how technology can be manipulated for triggering criminal activities. If you come to think of it, facial recognition can be used by serial killers or obsessed individuals for tracking information illegally.

5. SEXUAL & RACIAL DISCRIMINATION
That may sound obnoxious in the present times, but facial recognition apps have been differentiating people based on their color and gender.

The report even stated that the results of facial recognition are 99% accurate if the individual is a white male. The darker the skin tone, the harder it is to identify a person. This biasing by the system is making this world an unfair place to live.

Do you know Google once apologized for this in 2015? Google's facial recognition system recognized Africans as "Gorillas," in Google Photos. This mis-categorization led to several debates and controversies down the line. A representative was quoted as saying, "Image labeling technology is still early and unfortunately it's nowhere near perfect."

But, such imperfect instances might become the reason for people trusting these organizations less.

What can be done to fight the Dangers of Facial Recognition Systems?
Boycotting facial recognition systems completely should not be the conclusion as the possibilities of the technologies are immense. But, there certainly needs to be protocols and regulations around how the people's data, security, privacy, and other concerns are handled.

THE CONSTITUTION OF THE UNITED STATES

WE THE PEOPLE

· THE SECOND AMENDMENT ·

"The right of the people to keep and bear arms shall not be infringed."

SINCE 1791

MISSION STATEMENT

The SDF is a fund sponsored by membership in the Association For Legal Gun Defense, with litigation "junk yard dog" attorneys in all 50 states providing our members with an aggressive attack-dog style criminal or civil defense for the use of any weapon in self-defense.

CONTACT INFORMATION

Mail Office Number: 682-238-8161 | Email: sdfmembers@gmail.com

How to submit an article for publication

Submit an Article or Cartoon
We accept articles or cartoons related to self-defense, gun review topics, patriotic, as well as submissions on any related aspect of the law.

Where to submit
E-mail submissions (Word documents (.doc, .docx, attached to your e-mail message) submit to **sdfmembers@gmail.com**

Word count and specifics
Submit 1,000 words or less, unless other arrangements are made with the editor. Include a brief bio at the end of every submission, describing who you are and how you can be contacted. Include your name, mailing address and phone with all submissions. Include a photo of yourself for use online with your bio. We do not guarantee your submission will be published. Cartoon 3.625" X 4.75" PDF File.

Deadlines
Submissions are due on the 10th day of the month two months prior to the month of publication (January 10 for the March edition, for example).

Letters to The Editor
We welcome feedback from our readers via e-mail to sdfmembers@gmail.com. Include your name, address and phone number. Letters may be edited for clarity or length. We do not guarantee their pulication.

The Fine Print
By submitting your article or cartoon, you certify that you wrote the subject matter and that it does not contain content shared without the permission of another author. Submitting an article or cartoon does not guarantee publication. SDF reserves the right to edit article text submissions. All copyrights remain with the author. The publisher assumes no liability for unsolicited art, photos, manuscripts or other material. There is no remuneration paid for any submitted or published cartoon or article.

Articles vs. Advertising
Many of our articles are written by professional practitioners about their own field of practice. We hope that an engaging well-written piece will encourage readers to naturally want to find out more and the way to do this may be through visiting their website etc. We discourage you from using an article to heavily promote your own work or events.