Bias in Facial Recognition Technology

By: Maxwell Yearwood and Christine Marra
CSCI 77800 Ethics
Fall 2022

Overview

In this paper we will discuss:

- History of Facial Recognition
- Modern Facial Recognition Technology
- Current Uses of Facial Recognition Technology
- Shortcomings Facial Recognition Technology
- Recommendations to Improve Facial Recognition Technology
- Legislative Measures to Ensure the Ethical and Transparent Use of FRT

History Facial Recognition

Each person has certain biological features, a.k.a. biometrics, that are unique to them alone. A person's face is one of several unique biometric identifiers; others being fingerprints, voice and vein patterns in the eye and palm. The earliest known use of biometrics to identify a person dates back to the Qin Dynasty in China 221B.C. by using a clay finger imprint.

The first use of facial recognition, the ability to identify an individual by their face, as a tool dates back to the late 19th century. England introduced a regular system of prison photography to make prisoners easier to find in the event of a successful escape and to enable record-sharing with other police stations. The first use of facial recognition as a tool in the United States is credited to the Pinkerton National Detective Agency. Before the establishment of a national law enforcement agency (i.e.FBI), the Pinkerton National Detective Agency investigated interstate crimes involving train and bank robberies. In 1895 they published Criminal Mug Shot & Information Book, an accumulation of 300 mugshots of known thieves. At the time, it was a “must have” for all members of The American Bankers Association.

As Alan Turing, is considered the father of computer science, Woodrow Bledsoe can be considered the father of facial recognition technology (FRT). In the mid 1960’s Bledsoe and two colleagues at Panoramic Research, Inc. (PRI), developed a process of comparing a photo to a database of photos to find a match. They referred to their project as “man-machine” because the process of identifying facial “landmarks,” which

is now referred to as measurement and extraction and done by computers, was done by humans.

The next generation of FRT using algorithms was created in 1991 by MIT researchers Matthew Turk and Alex Pentland. Building upon the idea of Sirovich and Kirby, which was based on the the idea that all pictures of the human face to be a weighted sum of a few “key pictures” they coined “eigenpictures.” In a study by Turk and Pentland they laid out a memory-efficient way to compute the eigenpictures. They also proposed an algorithm on how the face recognition system can operate, including how to update the system to include new faces and how to combine it with a video capture system. SOURCE

Modern Facial Recognition Technology

Fast forward to the 21st century and the use of facial recognition as a tool has expanded in scope and sophistication. Today, the process of identifying someone by their face is exclusively digital. At the highest level, facial recognition technology relies on artificial intelligence (AI) to learn the patterns of a human face. AI systems use machine learning models to learn from a dataset of human faces. These datasets, (i.e. photos) are compiled using various sources including, but not limited to, social media platforms, DMV records and police files.

The process of identifying a person using facial recognition technology (FRT), takes the following steps: detection, alignment, measurement/extraction, recognition and verification.

Detection and Alignment
All FRT programs must first detect or identify the face in an image or video.

Unfortunately, in most photos, the face is not squarely centered. This poses a problem because to a computer, faces that are turned away from the focal point appear completely different. Bledsoe’s FTR fell short because he was unable to account for rotations or tilts of the face in photos. Today, an algorithm aligns or centers the face to make it consistent with the faces in the database. During this process a variety of generic face “landmarks” such as the bottom of the chin to the top of the nose, the outsides of the eyes, and different places surrounding the eyes and lips are used. The next step is to then train a deep learning (AI) system to locate these spots on any face and turn them towards the center. This makes the face detection process possible.

Measurement and Extraction

Every face has numerous, distinguishable “landmarks”, the different peaks and valleys that make up facial features. FaceIt defines these landmarks as nodal points. Each human face has approximately 80 nodal points. Some of these measured by the software are:

- Distance between the eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

A deep learning (AI) system then measures the curves of the face and creates a template.

Recognition

Using the unique measurements just generated, AI algorithms then compare them to the measurements of each face in the given database/dataset. The match will be whichever face in the database comes closest to the measurements of the face in question.

Verification

The last step, also performed by deep learning algorithms, is to match the face with other faces in the database. If the face matches then it is said to be verified, and if unmatched it remains unverified. This verification process can sometimes be complex. The facial images created during the measurement and extraction process are 3-D. Problems arise when the images in the dataset are 2-D.

Current Uses of Facial Recognition Technology

Most people are unaware of the extent to which facial recognition technology pervades their everyday lives. Many of us use FTR to safeguard and access our personal devices. Our phones and tablets come with FRT already installed, so whether knowingly or unwittingly, we use FRT everytime we share and store photos. Many “techies” and “early adopters,” of FRT will have the ability to speed though lines at airports, hotels and grocery stores.

Facial recognition technology is currently being used in many public spaces where large groups of people gather and security is a concern, especially airports and stadiums. The trade-off for this convenience and security is a lack of privacy. The use of security cameras in public places is a source of photos for a potential dataset.

The most controversial use of FRT is in law enforcement and community policing. Law enforcement agencies ranging from local police departments to the U.S. Customs and Border Dep't. use FRT to identify and apprehend criminals. Although there are many success stories and enhanced public safety resulting from this technology, it is still imperfect and needs to be used in conjunction with other tools. When used exclusively, without proper checks and balances the results can be devastating. Nijeer Parks and Robert Williams highlight when law enforcement officers used FRT irresponsibility.

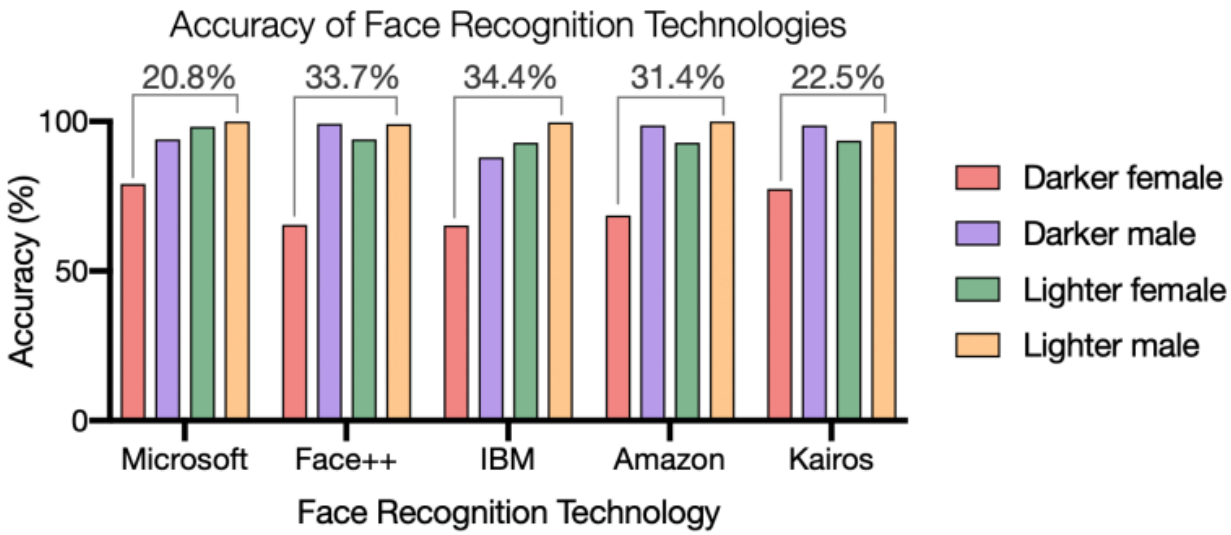
Facial Recognition Technology Shortcomings

Given our highly partisan and divided society, one thing most of us can agree upon is that the major drawback of facial recognition technology is the occurrence of false positive results. The range of false positive error rates in one study was between 3 errors out of 100,000 queries (0.003 percent) in optimal conditions to 3 errors out of every 1,000 queries (0.3 percent). Although those error rates are very low, they can have a significant impact when applied to an entire entire population. Given the population of the U.S., a .3% error rate would equate to over 1 million false results. Source

Factors to Consider resulting in false results:

- Quality of photo
- Performance of the algorithm
- Size of database
- Type of comparison; one-to-one or one-to many

The existence of false positive results is referred to as implicit bias because it happens most often to women of color.



SOURCE

Recommendations to Improve Facial Recognition Technology

There are a few ways to improve the use of facial recognition technology. One action that can be taken to improve the verification results is to improve the datasets used FRT algorithms. Underexposed and poor quality photos should be removed from datasets as it makes the performance of the results of the facial extraction and measurement process less reliable. More varied photos need to be added to the datasets in the AI algorithms. It is noteworthy to mention that China does not experience the same level of inaccuracy in their FR systems as we do here in the U.S. One possible conclusion that can be drawn is that since the Chinese population is more homogeneous than that of the U.S., all of the photos in their datasets will have darker skin tones. Therefore, since the FR algorithms use machine learning, the more datasets, the more accurate the results.

Algorithms and machine learning (AI) form the foundation Facial Recognition Technology. There are currently hundreds of biometric authentication recognition algorithms functional and patented within the USA. Therefore, improved FRT, will need to come from improved algorithms.

Legislative Measures to Ensure the Ethical and Transparent Use of Facial Recognition Technology

Most people agree that FRT is an important tool used for public safety and many individuals enjoy the convenience it provides. For those reasons, it is safe to say that the use of FRT is only going to expand in the future. Fortunately, FRT is improving rapidly. In order to balance the need for security and convenience against the need and desire for privacy, all stakeholders must stay engaged in public discussion of FRT.

Although there is a lot of discussion surrounding FRT, there are no federal laws regulating its use. This has led to a “patchwork”of various laws addressed at the state and local levels. A good starting point for public discourse and future legislation should involve data, privacy and civil liberties, safeguards and reporting. Some topics to discuss should include:

- FRT should only be used in a manner consistent with constitutional protections for civil liberties and civil rights.
- Use of FRT should be transparent; the public should be notified that FRT is being used as well as to when, where and for how long the images can be stored and under what conditions they can be used or shared.

- Use of FRT should be at the consent of the subject. This could be implied consent, as when you enter a store that is transparent about FRT use and be given the option to “opt out.”
- To hold uses of FRT accountable, an oversight mechanism at each level of government that authorizes its use will be required.
- With regard to oversight agencies, lawmakers should enact transparency laws regarding algorithms and consider establishing accuracy thresholds.

SOURCE, SOURCE

New York’s Legislative Measures

Bill	Description
NYS Assembly Bill A6787D	Bans the use of biometric surveillance technology in schools **until** the New York State Education Department (NYSED) issues a report on the risks and benefits of this technology in schools and the Commissioner of Education authorizes its use.
NYS Senate Bill S1933A	Establishes the biometric privacy act requiring private entities in possession of biometric identifiers or biometric information to develop a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with the private entity, whichever occurs later.
NYS Senate Bill S675	Establishes the "protect our privacy (POP) act" to impose limitations on the use of drones for law enforcement purposes by prohibiting the use of drones by law enforcement at concerts, protests, demonstrations, or other actions protected by the first amendment and requires a search warrant prior to using a drone for law enforcement purposes.
NYS Senate Bill S1076	Prohibits facial recognition technology to be used in connection with an officer camera used by both local and state police including the storage of biometric data.
NYS Assembly Bill A4352	Prohibits the use of a facial recognition system by a landlord on any residential premises.
NYS Assembly Bill A768	Prohibits the use of facial recognition and biometric information as the sole factor in determining the existence of probable cause to place in custody or arrest an individual.

NYS Assembly Bill A4916	Prohibits the state, state agencies and departments and contractors doing business with the state, its agencies or departments from retaining facial recognition images or sharing such images with third parties without legal authorization by a court.

Code Portion of Final Project

How does facial recognition work?

Facial recognition technology takes place in two main ways: facial detection and facial identification. Facial detection is an essential first step in facial recognition. In this step, the software uses a mathematical formula to reduce the many features of your face into tiny bits of information. Some algorithms use cascades to repeatedly scan the features of a face.This step constitutes one's facial signature. Once the face is detected it is then compared to a known database of faces. The unknown face is then matched to a known face. This completes the identification phase and thus facial recognition is complete. These steps are illustrated in our code in Appendix A and B.

Our simulations of facial recognition are illustrated in two ways. The code in appendix A illustrates facial recognition by comparing a known database of faces housed on a hard drive against an unknown face housed in another folder on the same hard drive. The code in appendix B illustrates facial recognition technology in real-time by using a webcam and a phone. An unknown image on the cell phone is held up against the webcam at various distances and angles. The known images are stored in a folder on the computer's hard drive. Once a face is detected a rectangle is drawn around the face along with the name(s) that match the image shown on the phone. The code displays "unknown" if there is no match or an error message if no image is detected. This completes the facial recognition process.

We used images of Keanu Reeves, Will Ferrel, and Idris Elba in this simulation. Our simulations confirm that this technology detects and identifies male caucasoid faces accurately but often fails to do so for some known dark skinned male images. These findings are in accordance with the literature on facial recognition technology.

Appendix A

```
import cv2
import face_recognition
```

```
#This algorithm detects all images for Keanu Reeves and Will Ferrel in my database
# but could not detect some of Idris Elba's images. Instead it
# displays the error: " IndexError: list index out of range error"
# Why is this so? According to Stackoverflow
#
(https://stackoverflow.com/questions/59919993/indexerror-list-index-out-of-range-face-recognitio
n)
# this algorithm displays the error: " IndexError: list index out of range error"
# because it could not detect a given image. Hence one ethics issue in facial recognition.
#Some experts claim that facial recognition technology (sometimes) misidentifies dark skinned
people

# Accessing and encoding known image
known_image = cv2.imread("C:/Users/Tashema Bholanath/Documents/images/Idris_Elba.jpg ")
rgb_img = cv2.cvtColor(known_image,cv2.COLOR_BGR2RGB)
img_encoding = face_recognition.face_encodings(rgb_img)[0]

#Accessing and encoding unknown image
unknown_image = cv2.imread("C:/Users/Tashema Bholanath/Documents/images/Idris
Elba_2.jpg ")
rgb_img_2 = cv2.cvtColor(unknown_image,cv2.COLOR_BGR2RGB)
img_encoding_2 = face_recognition.face_encodings(rgb_img_2)[0]

# Comparing images to test if known and unknown images represent the same person.Returns
true if images are the same person.
image_recognition = face_recognition.compare_faces([img_encoding],img_encoding_2)
print("Image Recognized:", image_recognition)

# Displays known and unknown images
cv2.imshow("Img",known_image)
cv2.imshow("Img_2",unknown_image)

# Image is displayed until user presses a key on keyboard
cv2.waitKey(0)
```

Appendix B

```
# This algorithm works by using your webcam and phone to provide real-time facial recognition
# to simulate real-time facial recognition used in practice.

#Note Findings: Algorithms normally works fine but either fails to detect or name
# an unknown face if the phone being held to the Webcam is either held too far
# away or if the phone showing the unknown face is held at an angle. Hence an ethical
```

```
# issue of misidentification of some unknown faces



import cv2
import face_recognition
from simple_facerec_import_SimpleFacerec

# Encode all faces in folder

sfr = SimpleFacerec()
sfr.load_encoding_images("C:/Users/Tashema Bholanath/Documents/images/ ")

# Take Webcam Stream
# Load Camera
cap = cv2.VideoCapture(0)


while True:
    ret, frame = cap.read()

    # Face Location and face detection of known faces
    face_locations, face_names = sfr.detect_known_faces(frame)
    for face_loc, name in zip(face_locations,face_names):
        y1, x1, y2, x2 = face_loc[0], face_loc[1],face_loc[2],face_loc[3]
        #print(face_loc)
    #Show names and  rectangle around face identified
        cv2.putText(frame,name,(x1, y1-10),cv2.FONT_HERSHEY_DUPLEX,1,(0,0, 0),2)
        cv2.rectangle(frame,(x1,y1), (x2,y2), (0,0,200),2)

    cv2.imshow("Frame", frame)


    key = cv2.waitKey(1)
    if key == 27:
      break


cap.release()
cv2.destroyAllWindows()
```

Sources

https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/

https://www.smithsonianmag.com/history/first-case-where-fingerprints-were-used-evidence-180970883/

https://leg.mt.gov/content/Committees/Interim/2021-2022/Economic%20Affairs/Meetings/September%202021/facial-recognition-technology.pdf

Legal concerns
https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape

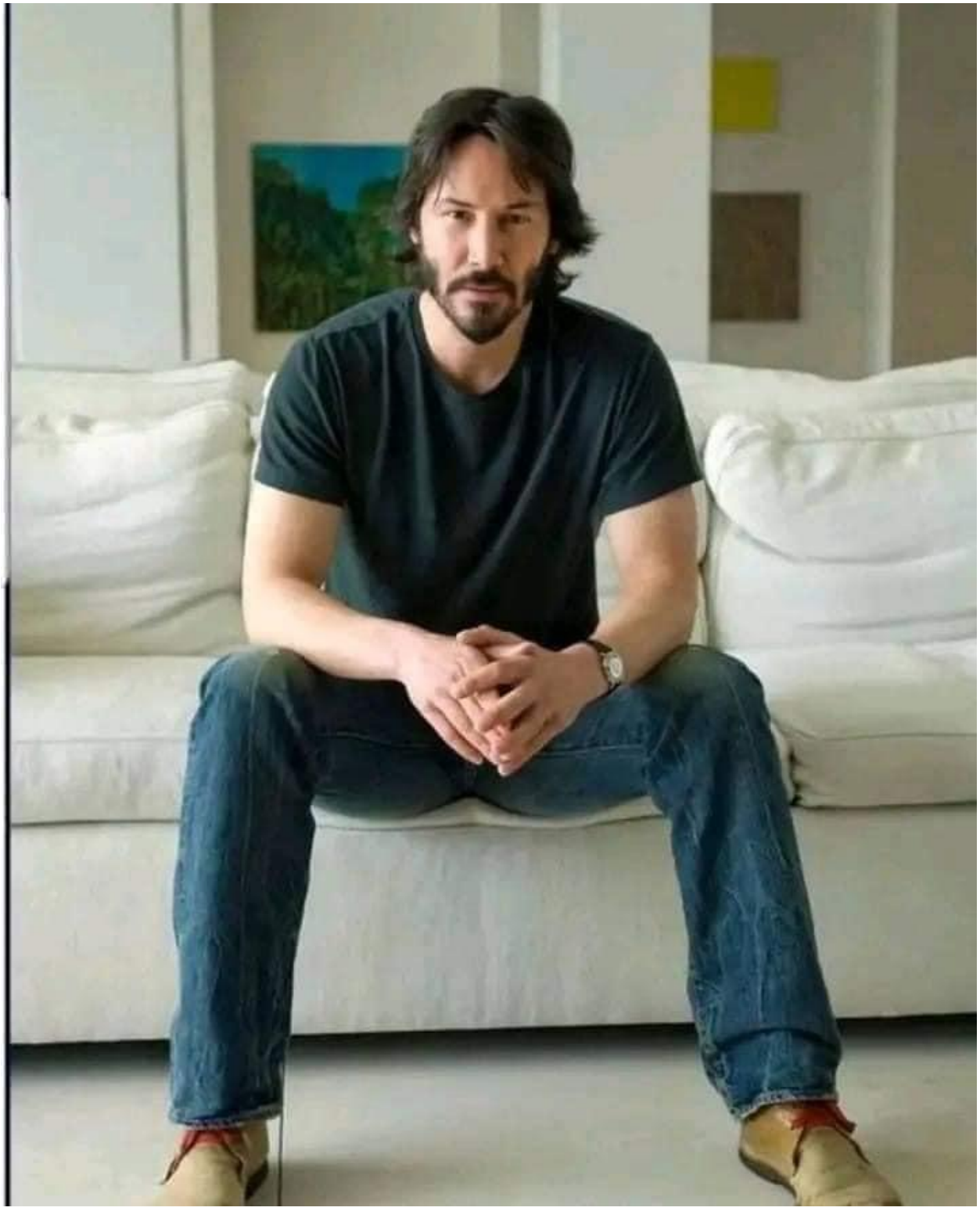
https://www.mitre.org/sites/default/files/2021-11/biometric-face-recognition-references-policymakers.pdf

How does Facial Recognition work?
https://www.csis.org/analysis/how-does-facial-recognition-work

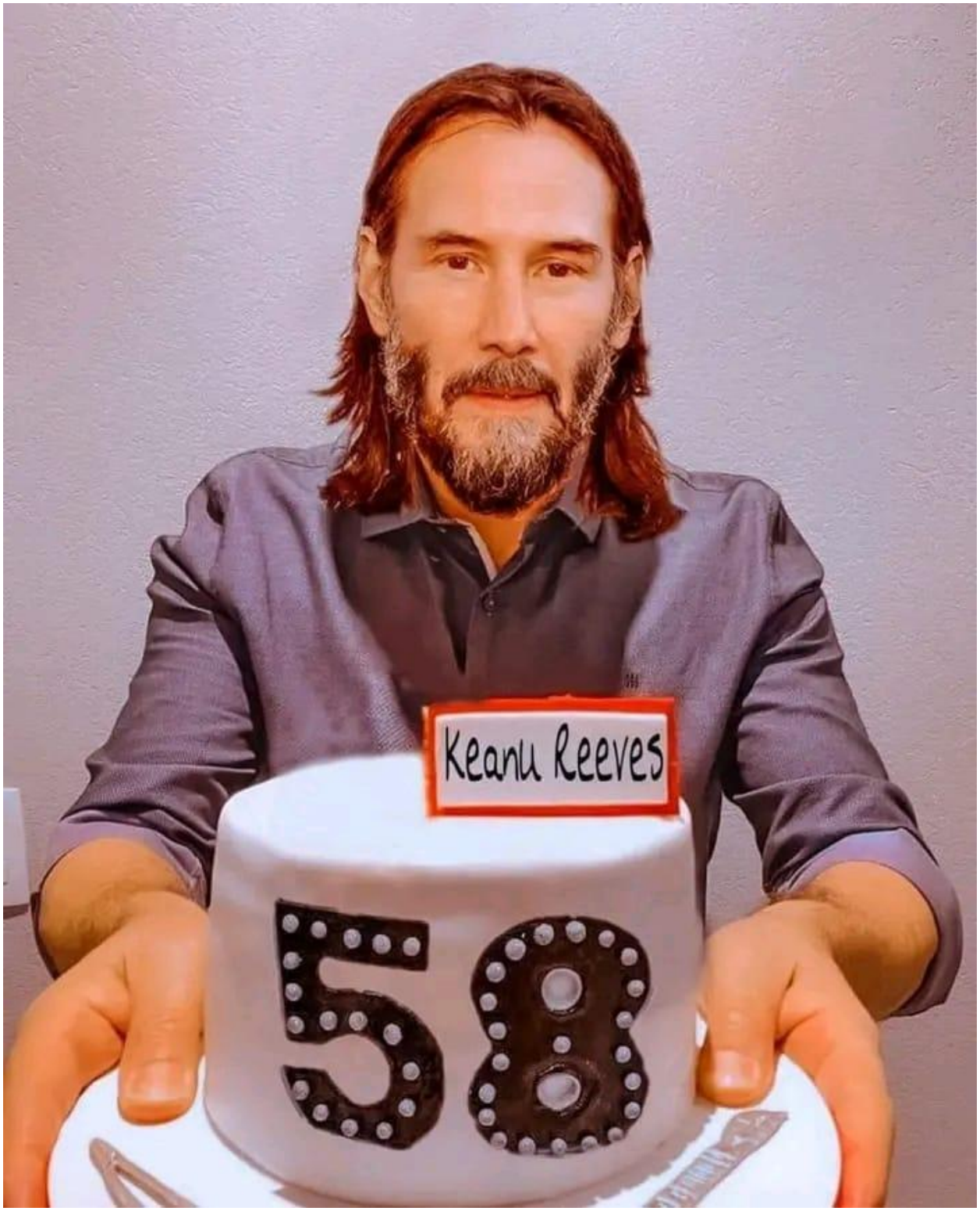
https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

Facial Recognition is everywhere.
https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/

Safety of Facial Recognition
https://www.electronicid.eu/en/blog/post/face-recognition/en



Keanu_Reeves

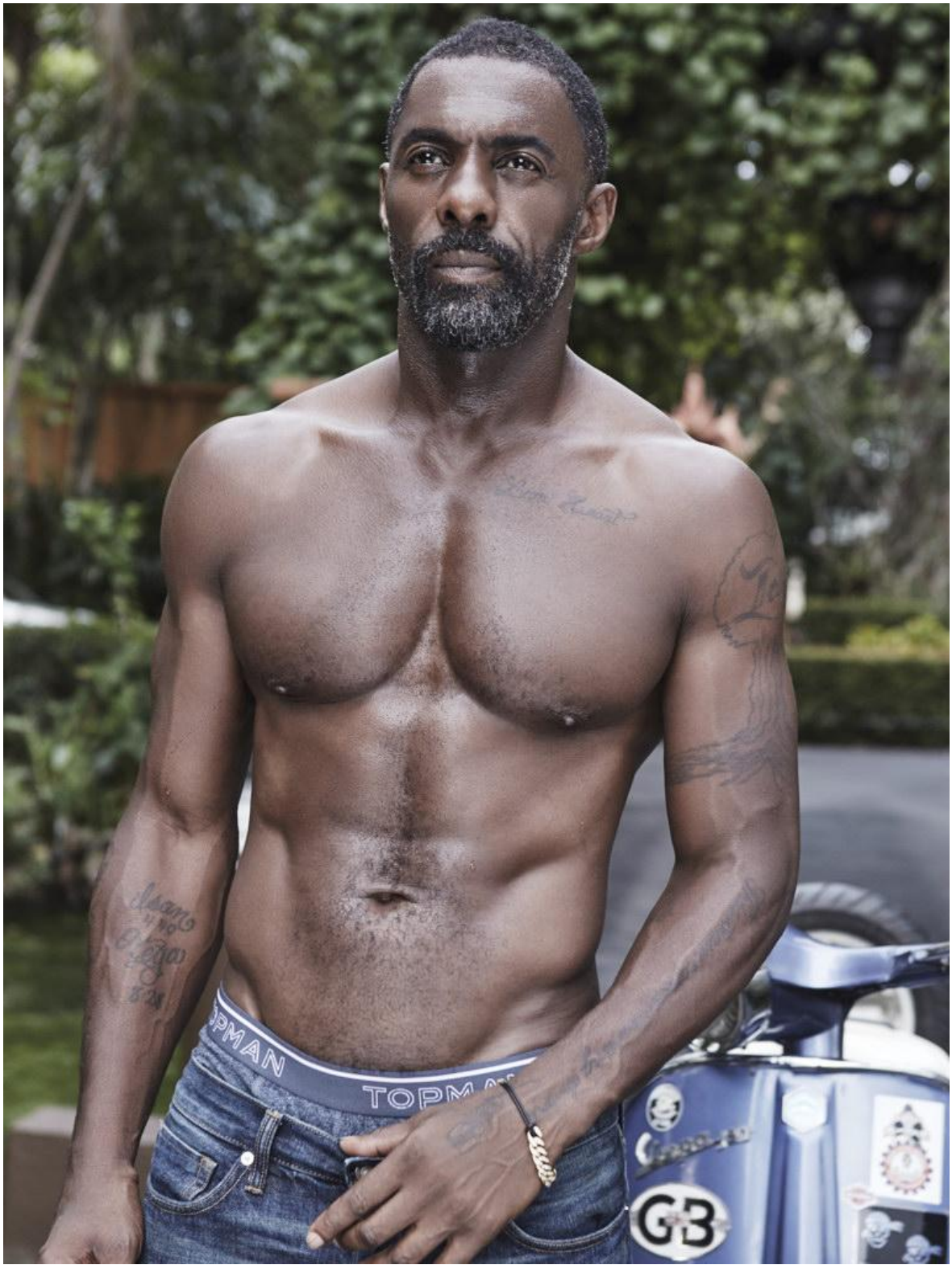


Keanu_Reeves_1

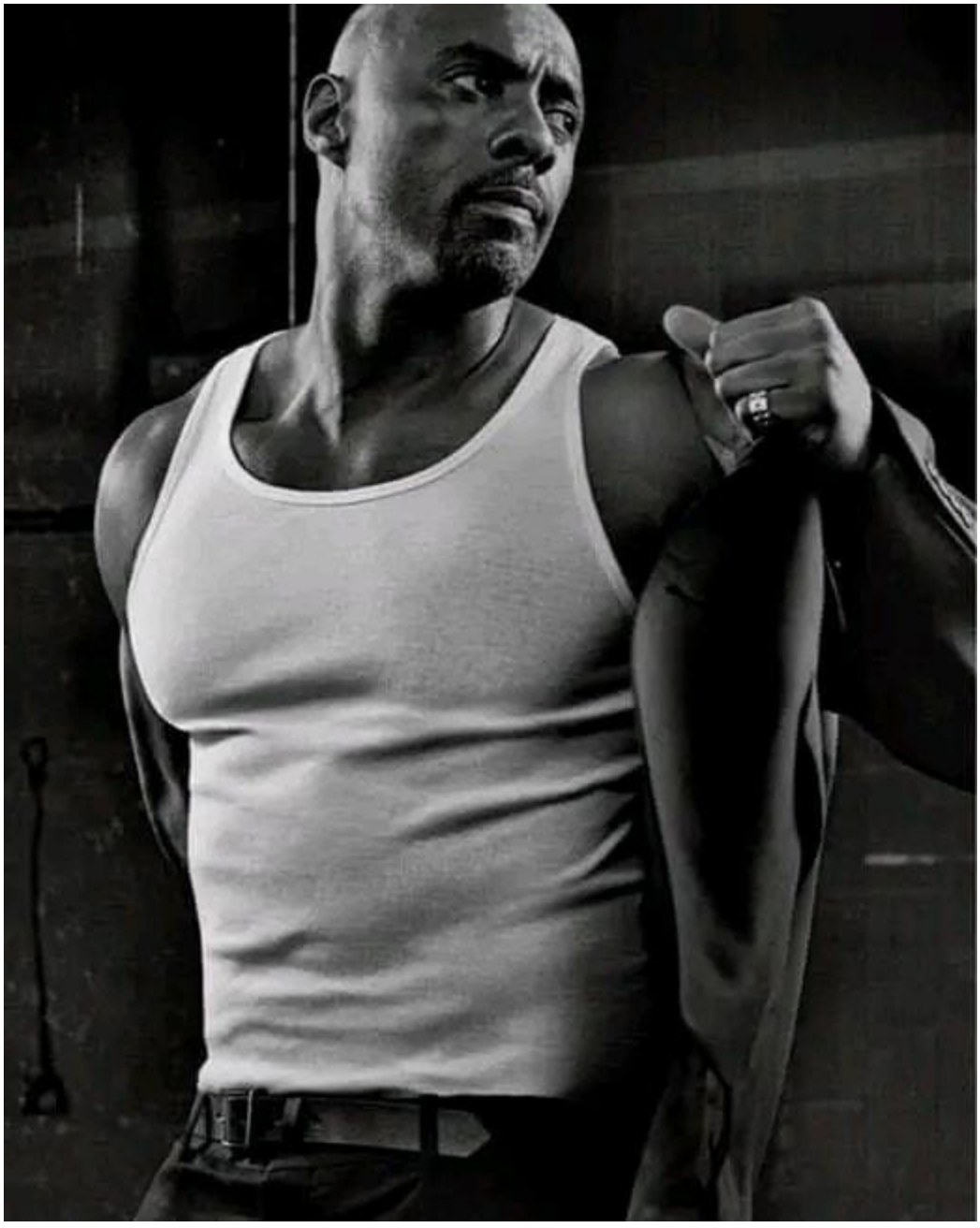
Idris_Elba_4

Idris_Elba_3

Idris_Elba_1

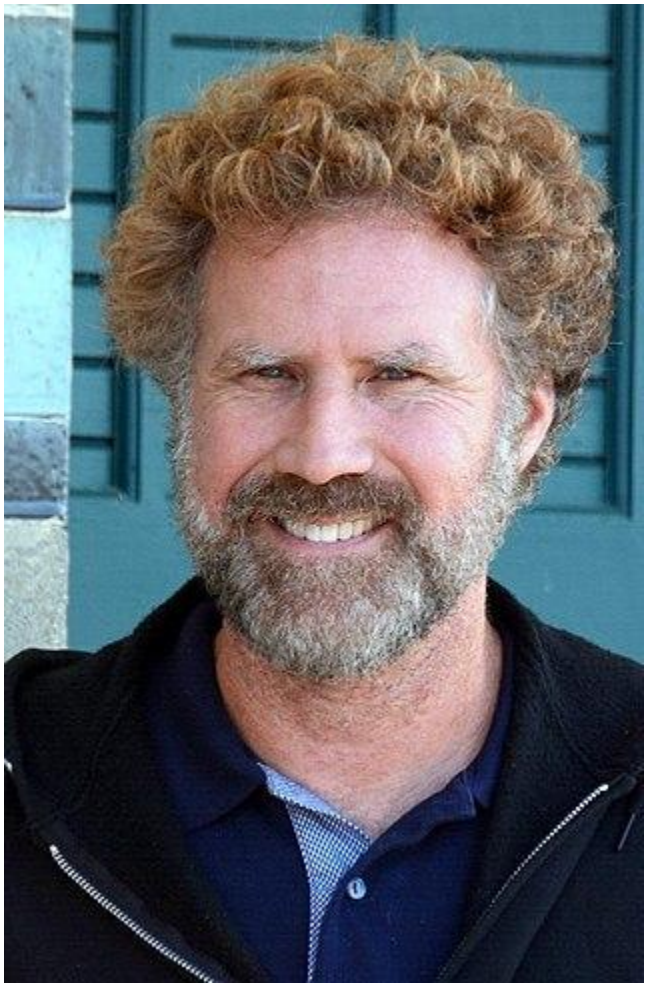


Idris_Elba_2



Idris_Elba

Will_Ferrel



Wil_Ferrel_2