Jaiden Atterbury

Peter Gao

STAT 303

04 December 2022

Final Project Part Three: Final Report

**Introduction:**

Facial recognition technology is a tool that has become more and more prominent over the years. It has slowly begun to play a role in the everyday life of an average person. From unlocking an iPhone to being used as evidence in a criminal justice case, facial recognition technology is everywhere. Facial recognition technology is the set of digital tools that perform tasks on human faces through the use of images and/or videos. These tasks include, but are not limited to: face detection, face attribute classification/estimation, face verification, and face identification. Likely the most common example of an FRT is unlocking one’s phone. In this scenario, each time you wake your screen, your phone’s camera will project and analyze the features of your face and match it to the stored data it’s familiar with to authenticate the user. Ideally, this technology works 100% of the time regardless of the subjects’ appearance. However FRT’s are not flawless yet. There are numerous concerns over privacy implications, racial biases, and \_\_\_\_\_\_\_\_\_. We’ll be going over why these concerns have arisen and recommendations for what we think can be done to improve FRT’s moving forward.

**Technical Details:**

In general, facial recognition works by identifying and measuring certain facial features in an input image, also known as a query image. Then, depending on which of the aforementioned uses was chosen, the machine outputs a decision on if a match or certain feature appeared in the query image. The query image can come in many different image data types. These image data types include: single images, video sequences, views from multiple cameras, and three-dimensional data. Due to the proprietary nature of the technologies themselves, most FRT’s don’t function exactly the same. However, the majority of FRT’s generally follow three broad steps when performing their duties, these steps are usually referred to as: enrollment, comparison, and matching decision.

To be used in an FRT, a face must be photographed or videographed so that it appears as one of the previously mentioned image data types. Once this query image is captured and a face is detected, the facial recognition system then analyzes this query image. It starts off by mapping and reading face geometry by identifying facial landmarks that are key to distinguishing a face from other objects. The system then converts this face data into a numerical format called a template or faceprint. The facial recognition technology typically looks at the following facial attributes when making a faceprint: distance between the eyes, distance from the forehead to the chin, distance between the nose and mouth, depth of the eye sockets, and shape of the cheekbones. Once the query image is transformed into a faceprint, there are two primary uses of this image data. The first of these uses is to build a gallery of people to be recognized. This process of recording visual information about an individual for the use in a gallery is called enrollment. The second major use of such photos is at the time of recognition, when the FRT is trying to identify or verify a person. The machine does this by comparing the query faceprint to the built gallery.

Once a faceprint has been extracted from a query image, the process of comparison then proceeds. The two main types of comparison that an FRT can perform are face verification, and face identification. In face verification, also known as one-to-one comparison, the goal is to confirm the identity of a certain query image by comparing the query faceprint to an existing faceprint of the expected individual. In this case the individual makes a claim about who they are and the task of the system is to verify this claim. The goal of face verification is to decide if two images show the same person (match) or two different people (mismatch). In face identification, also known as one-to-many comparison, the goal is to match an identity to given a face, without the expectation of who that person is. This process is done by comparing the query faceprint to

every individual faceprint in the set of faceprints in the gallery. When two faceprints are compared by a machine, a similarity score may be computed to represent the similarity of the two faceprints.

After the comparison has taken place the final step of the facial recognition process can take place, the matching decision. To decipher between match and mismatch, a certain score threshold must be set. Any scores above the threshold correspond to a match, and those below to a mismatch. Typically, one must make a compromise by setting a threshold which balances the number of false matches and false mismatches. During facial verification, when comparing a new query faceprint to an expected existing faceprint of the same individual, a similarity score is computed. Depending on the set threshold, the machine will either label the query image as a match or mismatch. During facial identification, when comparing a query faceprint to an entire gallery, one of three things can happen: no matches, one match, or multiple matches. In the event of multiple matches, an additional procedure will need to confirm the correct match, or decide that no correct matches are present. This job is usually left to a human to make the final decision.

**Ethical Concern #1: Racial Bias:**

While facial recognition technology does have many benefits, it does have its drawbacks. Unfortunately facial recognition technology has demonstrated a flaw that verifies faces of caucasian people with a higher precision than people of color. In his article *Report Finds Racial Bias in Facial Recognition Technology*, Jeff Stone writes, “According to the study, facial recognition systems are 5 to 10 percent less accurate when trying to identify blacks than when analyzing the facial images of white adults on the system.” This is especially concerning considering facial recognition systems are used in law enforcement. Moreover, this bias is further compounding a discriminatory issue that has been negatively affecting people of color for decades. Now this doesn’t mean that the developers or the technology itself is racist. Rather, disparities may arise unintentionally as a result of designing the algorithm itself, lack of diversity in training data, and prioritizing certain facial features over others. The facial features that the algorithm analyzes tend to be distinguished more easily by fair skinned faces rather than darker toned faces. This includes features such as the shape of a person’s eyes, width of their nose, and the size of the person’s mouth or chin.

**Recommendation #1: Racial Bias:**

However there are new methods being developed attempting to eliminate this racial bias. Researchers are beginning to expand their datasets and stretch the domain of facial characteristics and racial features their technology is utilizing in its analysis. A recent report from the European Union News said that this research has led to a 1% improvement in reducing racial bias and has increased the accuracy of facial recognition across all ethnicities. While the disparity of 5-10% still hasn’t been closed, it’s important that we begin to address the issue and eliminate the bias in the technology we use. Eventually we should hope facial recognition technology becomes less dependent on race by focusing more on identifying features of a person’s face instead of relying on certain racial characteristics of the algorithm as it does now.

**Ethical Concern #2: Privacy Concerns:**

One of the biggest existing ethical criticisms of FRT’s are the broad privacy concerns that they bring to the individuals subject to their use. Privacy infringements have become one of the general public’s main concerns with FRT’s, mainly due to a lack of transparency in how information is stored and managed. Furthermore, the most prevalent and scrutinized privacy implication of facial recognition technology is the use of the technology to identify individuals without their consent, this includes using applications such as real-time public surveillance or through databases that are not lawfully constructed. Without proper consent, FRT’s take away the reassurance of being able to move and act freely without the fear of constantly being watched and surveilled. The use of databases that were constructed without the consent of the individuals in them is prevalent throughout the field of facial recognition, two of the most famous examples of this phenomenon are the MegaFace database, and the Clearview AI database.

The MegaFace database is one of, if not the most famous examples of the use of facial recognition without the informed consent of the individuals present in the database. MegaFace was a research project created in 2015 by two computer science professors at the University of Washington; Ira Kemelamcher-Schlizerman, Steve Seitz, and their graduate students. This database contained nearly 700,000 images scraped from the old social media platform Flickr. However, none of the people who appear in the MegaFace database were informed that their images would be used. In 2015 and 2016, the University of Washington held an event known as the “MegaFace challenge” in which the university promoted the use of the dataset to test up-incoming FRT’s. Over these two years, it has been estimated that over 300 research groups worked with the database, with notable citations coming from Amazon, Mitsubishi Electric, and Phillips. It is important to note that despite the overall positive nature of the challenge, some companies such as SenseTime and NtechLab have been criticized for the way their algorithms have been implemented to perform unethical forms of surveillance.

The next, and one of the most recent examples of the use of facial recognition without the informed consent of the individuals present in the database, is the Clearview AI database. Clearview AI, which is self-described as the “world's largest facial network,” allows its customers to compare facial image data to over 10 billion images scraped from the internet. However, this database includes facial image data of a “substantial number” of UK citizens without these people's knowledge or consent. These images were scraped primarily from social media sites such as Facebook and Instagram. Furthermore, people who asked for their image data to be removed from the database often couldn’t proceed with their request due to Clearview asking them for additional personal information in order to meet their request.

**Recommendations #2: Privacy Concerns:**

Although individual privacy concerns such as the lack of informed consent are prevalent throughout the field of facial recognition, there are a few similar existing solutions that are being tried to combat this problem. These solutions primarily take the form of legislation, two examples of legislation used to combat the use of unethical collection of data are the Biometric Information Privacy Act and the General Data Protection Regulation (GDPR). Both of these acts/regulations seek to hold companies accountable for unethical data collection by imposing fines and sanctions on companies who violate the outlined laws.

By law, most Americans in databases such as the MegaFace database described in the previous section, don’t need to be asked for permission to be used in facial recognition databases. However, Illinois has the Biometric Information Privacy Act, a 2008 measure that imposes penalties for using Illinoisians biometric data such as faceprints without their consent. In the MegaFace database, there were thousands of photos from residents of Illinois. It is important to note that the Biometric Information Privacy Act doesn’t cover photos, instead they protect biometric data such as faceprints, fingerprints, iris scans, etc. However, due to the “MegaFace Challenge'' their biometrics were processed by hundreds of companies when used as test data for their FRT’s. Due to this clear violation, those individuals whose biometric data were used without their permission are entitled to $1,000 per use, and $5,000 per “reckless” use. The legislation has turned out to be effective as over 200 class-action lawsuits claiming companies have illegally used individuals’ biometrics have been filed in Illinois since 2015, including a $35 billion dollar lawsuit against Facebook. Recently, technology companies have been very cautious in states with biometric laws.

The next existing remedy to the lack of informed consent in facial recognition is the GDPR, the self-proclaimed “toughest” privacy and security law in the world. Although the GDPR was passed by the EU, it imposes obligations on organizations anywhere, given that they illegally collected data on individuals from the EU. In response to violators, the GDPR levies harsh fines against those who violate the privacy and security standards drafted in the bill. Under the GDPR companies can only process data from subjects if the subject gave the company “specific, unambiguous consent” to process the data. In the aforementioned Clearview AI example, Clearview AI failed to comply with the higher data standards set by the GDPR. This misuse of data of individuals from the UK has led to them receiving a 17 million pound fine. The GDPR has been very effective in forcing companies to think strategically regarding the use of consumer data. Furthermore, the risk of incurring hefty fines has made companies take privacy and security more seriously.

Although these current forms of legislation have been very effective in combating the lack of informed consent in FRT’s, due to the fact that as of the first quarter of 2022 only 7 states have biometric privacy laws based on that of Illinois, the legislation is not enough to fully combat this lack of consent in facial recognition. Furthermore, in states that don’t have biometric privacy laws Americans in facial recognition databases don’t need to be asked for permission to be included in said databases. Thus, in order to fully combat this lack of consent and clear violation of citizens privacy, we must create a task force that would draft an act very similar to that of the Biometric Privacy Act in Illinois, but make it federally effective. By doing this the act would impose certain obligations on companies/businesses in every state, including obtaining consent before any collection and use of biometric data, forcing these companies to explicitly state how the biometric data will be used and stored, and lastly making these companies employ reasonable security measures to ensure the safety of ethically obtained biometric information.