Ethical Facial Recognition

By Peter Kloss

STORY

Facial recognition is an immensely powerful technology that creates a safer, happier, and more productive environment. Imagine walking through an airport with chaos all over the place - a child has lost their parents and a large search effort is underway, there are criminals and terrorists disguising themselves as the try to move across borders, people are trying to decide where to shop as they wait for airplanes, and passengers who are lost in the expanse of the airport. All four of these scenarios have one thing in common: facial recognition can help assist them in achieving their various goals. For instance, as the lost child wanders the terminal calling for the parents, cameras across the building identify every person in the room finding the child and show security guards where to go. As criminals try to move through the airport, the cameras using facial recognition pick up the person and identify local law enforcement who make an arrest. Shoppers get updates on their phone regarding sales or items they may like at stores as they walk by without even having to go into the store.

Only a few years ago the above story seemed farfetched. How could technology accurately identify unknown people in large areas effectively and efficiently? Today, many of these scenarios are already in effect. Governments across the world use facial recognition to stop terrorist and criminals from entering their country in places like Russia, Germany, China, and the United States. Another example is airports employing technology that help law enforcement find criminals and there are even rumors that pilot programs are being tested that identify everyone in real time. Maybe these programs could even solve the lost child problem. One thing is for sure, the picture painted above demonstrates the need for facial recognition; however, the same technology can be used by governments to spy on citizens illegally, used by identity thieves to steal identities, and used by ad agencies with targeted advertising - each of these points raise serious ethical questions, especially in regard to invasion of privacy.

Is it a privacy concern or a rights concern? With the waters being muddy, it is tough to tell when facial recognition crosses over from a privacy concern to a rights concern. On one hand, companies like Facebook and Google routinely push the boundaries of privacy with their automated facial recognition systems that tag you in a picture before you even get the chance to accept it. The U.S. government, on the other hand, pushes the boundaries of rights with advanced systems like Stingray and eavesdropping on citizens without the acceptance or even acknowledgement from the people.

WHAT IS THE TECHNOLOGY

Facial recognition is a technology that identifies a person and their attributes by examining a video frame or digital image. There are two general approaches to how the technology works. The first approach, geometric, identifies various geometric shapes like circles, triangles, squares, and other polygons in addition to distances between features in digital images and video frames. Then, the program runs a side by side comparison between the image trying to be identified and a database of identified images. The second approach, photometric or photometric stereo, compares the digital assets under various lighting conditions and then compares the result to a database full of assets to make an identification. Depending on the situation, the accuracy of geometric or photometric can vary due to low light conditions, use of masks, and speed at which the digital asset was taken.

Ten years ago it was challenging to find facial recognition programs that were operational and produced verified results. Today that is a different story; computer technology like mobile phones employ facial recognition for security and entertainment, areas with public transportation use the technology to help identify criminals and terrorists, and governments use facial recognition on a large scale to help monitor their citizens in places such as Russia, China, United States, and Germany. One thing is for sure, no matter the approach to facial recognition, the parties who use facial recognition, and the people who are observed every day, few people ask themselves the ethical question, did I agree to this? What about 3rd parties who get caught in the crosshairs?

HISTORY

In the 1960s, Woodrow Wilson Bledsoe, a University of California Berkeley educated mathematician, discovered a breakthrough with facial recognition essentially starting the movement. His effort was funded by an unknown government agency, who to this day remains classified, with the intent of winning the Cold War. His system had significant manual labor and involved RAND Corporation's tablet technology to hand classify various digital assets by computing distances between facial features and then retrieving the best fit identified asset from the database. During the 1970s and 1980s, little improvement was made on facial recognition still requiring biometrics done by hand; however, in the late 1980s and early 1990s, linear algebra was introduced into facial recognition systems enabling greater data analysis throughput.

The use of linear algebra coupled with rapidly evolving technology, such as memory stores and processing power, allowed scientists once again to make significant breakthroughs including the Eigenface system. This system used eigenvectors and covariance matrices to reduce the complexity of a human face and then compare the broken down faces to one another to determine the best fit. Once again seeing the potential in facial recognition, the U.S. government through Defense Advanced Research Projects Agency (DARPA) funded the FERET program (Facial Recognition Technology) in the mid-1990s. This program sought to build a database of high quality digital assets that could be used by researchers and scientists developing the next generation facial recognition systems. The turn of the millennium brought law enforcement and the Federal Bureau of Investigations (FBI) into the equation with their attempts to build various systems to help in identifying criminals. By the 2010s, the technology was in full swing with Facebook's face suggestion system in 2010 – automated identification of people in a user's picture, the system used by the U.S. government to identify Osama Bin Laden, and the new technologies: DeepFace by Facebook – facial recognition system said to be 97% accurate, Face ID by Apple – a new system that unlocks an iPhone via facial recognition, Vision API by Google – an image content analysis system, Trueface.ai, etc.

HOW ACCURATE IS THE TECHNOLOGY?

Accuracy is an ethical dilemma for facial recognition. A recent study by Joy Buolamwini at Massachusetts Institute of Technology's Media Lab showed that accuracy for facial recognition on lighter-skinned males was 99% whereas with darker-skinned females nearly 35% of the assets were misidentified - a clear indication of the prevalence of both racism and sexism. This prevalence is likely attributed to two factors, that artificial intelligence has more errors the darker the skin due to camera technology and that most data sets consist of mainly white males (remember that the more data you have the better facial recognition works, if there are more white males, then white males are identified better). This data shows that even artificial intelligence and facial recognition cannot escape the biases imposed by humans which is a byproduct of how the measurement system for accuracy works. If we continue to focus heavily on white males during creation of systems and then focus on the results of white males during testing, then the biases will remain in place favoring white males in this case. The National Institute of Standards and Technology (NIST) out of the U.S. Department of Commerce has an extensive testing program for facial recognition. This program came from the U.S. government's desire to have accurate technology to help in the war on terror, the drug war, and day-to-day law enforcement needs. A quick glance at the updated data from NIST shows how accurate the various companies are and an interesting side note is most of the "most" accurate systems come from China and Israel.

Going forward, technology that enables facial recognition has been the main factor that prevented recognition from being more accurate. As a result, in the coming decade facial recognition will likely halve the quantity of mistakes as computing power becomes inexpensive and widespread. As mentioned before, China and Russia have implemented country-wide initiatives to monitor their citizens in real time, can you imagine in ten years when facial recognition is 99.9% accurate allowing governments to monitor specific people or the whole country? Should we as citizens of Earth allow our privacy to be removed completely by the government or should we enact laws? What choices should we have and where must we sacrifice personal privacy in order to be part of a civil and safe society?

CRAZY STORIES

A Russian company, Ntech Lab, created a mobile application called FindFace that allows people who use the Russian social media site, VKontakte, to take a picture of a random person and find that person on the website. The accuracy of this technique is roughly 70% which it seems is good enough for the typical consumer. This product raises the question, do you own your own face? Is there a way to stop people from snapping random pictures of you to then use them to find and stalk you? Regardless, the technology is quite powerful. FindFace has expanded from facial recognition to emotion recognition, age recognition, and sex recognition and is even certified by NIST, a U.S. government entity, to be used by U.S. agencies such as law enforcement.

Security is one of a country's biggest problems and facial recognition can solve part of the security problem. Seeing this niche, Russia's capital city, Moscow, now employs over 170,000 CCTV cameras to monitor the city and quickly saw results with the apprehension of dozens of criminals. Upon activation of the facial recognition network, public outcry was prevalent accusing the government of spying on all citizens in real time, yet unfortunately citizens were unable to stop the system from continuing. The one catch is the amount of computing power required to do this spying, at the moment public information proves that this would be impossible, however, unknown classified government projects may prove otherwise. It would be safe to reason that in the not so distant future, technology like this will be able to monitor people in real time allowing the government to jail political dissidents, foreign citizens, and petty criminals. Should we stand by and allow governments to implement real time facial recognition systems to monitor everyone?

China sees the advantages of facial recognition and is deploying systems all over the country. One such instance was recently at an outdoor concert with over 60,000 attendees. A finance criminal entered the venue to watch the show carefully avoiding any venue near his house in the hopes of stumping the police by going far away. Police officers received an alert from the facial recognition program responded and made a timely arrest within the venue. It is hard enough to match a portrait to a sample of 1,000 digital assets, but to find one individual in a large crowd and then compare that individual to a large database takes enormous resources. Even if the government only goes after the criminals, they still need to include your face in the database to eliminate you as a possibility until a point at which the person is identified, did you okay that?

Facial recognition systems can also be used for public awareness and safety. The Chinese city of Shenzhen, a city with over four million residents, has an enormous jaywalking problem that can create day-long traffic jams. In response to this issue, the city administrators found their solution with facial recognition. When someone jaywalks across the street, the digital image is compared with the citizenship database and then is posted in public across the street. Additionally, the person receives a text message fine and the associated data. This example is a great one to demonstrate what someone can do ethically with this technology.

CURRENT REGULATORS

There is good news on the ethics front. Some organizations do understand the implications and are taking steps to safeguard against potential ethical violations, however, they are not doing enough. In the U.S., NIST runs a program called Face Recognition Vendor Test (FVRT) which continuously looks at the various technologies and ranks them. Although NIST does not tend to ask ethical questions, they do provide a baseline to understand the complexities of the technology, an important step in educating people on what the technology is to enable more people to shape the future. Additionally in the U.S., both the House Oversight Committee and the United States Senate Committee on Homeland Security and Governmental Affairs monitors the facial recognition trend, albeit rather poorly, since both groups have missed numerous scandals involving artificial intelligence and facial recognition.

On a more cheery note, international organizations and organizations overseas are asking more questions about ethics - specifically privacy. For instance, the Electronic Frontier Foundation (EFF) produces white papers on the privacy concerns and government interference concerns that one could encounter when using the technology and tries to explain how governments use the technology to spy illegally on their own citizens. EFF is the leading nonprofit group in the world that defends digital privacy, free speech, and innovation and the group has put facial recognition technology on watch. The European Union General Data Protection Regulation (GDPR) is the first large scale push for privacy in technology setting guidelines for companies on what they can and cannot do. Still, there are many questions not being asked even in such a large and comprehensive document.

QUESTIONS AND ETHICS

1. Product
   - 1.1. How will facial recognition change the future for humans?
   - 1.2. What is the tradeoff between building facial recognition technology and our privacy/rights?
   - 1.3. What are we missing?
   - 1.4. Does it matter who designs facial recognition systems?
2. Process
   - 2.1. Who is responsible for designing standards and checks for facial recognition?
   - 2.2. How do we approach the issue of privacy versus rights?
   - 2.3. What parties are not involved and need to be to ensure success of facial recognition in the future?
   - 2.4. What happens if one party can control the technology's path forward?
3. Purpose
   - 3.1. What are the benefits of pursuing more accurate facial recognition systems?
   - 3.2. How do we know when facial recognition benefits us and how do we know when it hurts us?
   - 3.3. How do we develop a monitoring system built on trust that perseveres against corporations and governments?
   - 3.4. Who decides what is a just use?
4. Commercialization
   - 4.1. What is the cost to rights/privacy of developing facial recognition without oversight?
   - 4.2. Is your company pursuing both privacy and rights pathways at no cost to your customers?