Facial Recognition Technology & Surveillance

Trisia Baltazar & Ryan Smith

2018

**Executive Summary**

Facial recognition is an emerging and rapidly growing technology. It has enormous potential in both governmental and commercial use. Citizens need to be aware of the consequences that can come with this type of technology. There is not much an individual can do to combat this technology. Its use is growing worldwide, and we take a look at the role it’s playing in the United States and China and discuss the ethical implications. The next steps that are taken with this technology could completely revolutionize how privacy and security are viewed. Once this technology is implemented there is likely no going back.

**Facial Recognition Technology**

Biometrics has become a prominent technology when it comes to authentication. Facial recognition is a category of biometrics that has become popular worldwide. Its uses range from securing work and home property to entertainment use in social media platforms such as Snapchat’s filter software and Facebook’s tagging system on pictures. Facial recognition has expanded and will continue to develop to a very promising technology in the future.

A human face is unique and facial recognition takes advantage of this. There are about eighty unique points on a human face called nodal points. These facial features include distance between the eyes, width of the nose, depth of the eye socket, and many other unique identifiers. All these points create a faceprint, a numerical code that represents a face in a database. (Bosnor and Johnson)

Facial recognition technology works in a series of steps. The first step is detection. When an image is captured, the software must identify the visible faces. Once a face is detected, the face is aligned to allow the system to measure the nodal points. A faceprint is generated that is then compared with other faceprints in the database and guarantees that only one match is found. (Bosnor and Johnson)

Recent advances in facial recognition has made 3D scanning possible. Initial facial recognition software relied on 2D image comparison which relied on pictures. If the lighting or angle was different from the picture taken, the chances of a match being found would be low. In fact, during the alignment stage the head must be turned at least 35 degrees towards the camera for 2D image comparison to be even considered accurate. 3D scanning has made this process easier because a human head can be turned to up to 90 degrees and it will be able to find a match. It does not just rely on one pictures lighting and angle. It relies on the nodal points because they rarely change over time. It is much more flexible and has made facial recognition technology accurate in different types of situations.

This technology has improved quickly over the years through deep learning. Deep learning works like neural networks. If the facial recognition software captured an image, extracted the face, measured and compared it to other faceprints in the database and it came up with two matches, it would learn from that mistake, thus making it more accurate with every error it encounters. Deep learning is used in many artificial intelligence systems because of its similar function to human neural networks and it allows machines to learn and create a pattern of their progress. An example of this would be Facebook’s facial recognition software, DeepFace. DeepFace is the system Facebook uses to tag friends onto photos. Soon, this software will be able to identify facial expressions and emotions and analyze facial attributes that determine age, gender, skin color, and many more traits. With the help of deep learning it will be able to accurately verify that a face belongs to one image in the database. With more than 2 billion Facebook users this system has a lot of potential. (DeepFace)

**Avoiding Facial Recognition**

When a technology like this comes along countermeasures can be expected. There are a few interesting ways to attempt to avoid having ones face recognized by facial recognition technology. One of these methods is a pair of glasses developed by a team at Carnegie Mellon University, these glasses can confuse facial recognition software by making the system think the glasses are part of the wearers face (Revell). Anyone with a 3d printer could make a pair of glasses like this which makes it a practical option for people looking to avoid facial recognition technology. Another technology that works like this is a hat that is lined with infrared LED lights that shine onto the face of the wearer. (Pettit) These infrared lights are invisible to the human eye but not to cameras. The camera will see the light as part of the wearers face and not be able to accurately determine their identity. This hat is more inconspicuous than the glasses and with further developments could likely be made to be completely undetectable from human eyes.

The simplest counter to facial recognition technology is of course obscuring one’s face. Wearing a hat, glasses, and scarf will cover a lot of one’s face making it more difficult for facial recognition to determine one’s identity. Wearing a mask of course is a way to guarantee one can’t be identified by one’s face. This doesn’t mean one can’t be identified at all, as gait is a measurable biometric that can be used to identify a person. In the future it will likely be very difficult to completely conceal one’s identity.

Of course, there is large interest in stopping people from avoiding facial recognition. One machine learning algorithm can accurately identify people wearing obscuring clothing. It’s an algorithm that identifies 14 key points on a face. Researchers manually selected the 14 key points for 2000 photographs of people wearing obscuring clothing and guessed where their key points would be if they were obstructed. This allows the algorithm to make its own guesses and it’s successful. It can correctly identify people wearing a scarf 77% of the time, people wearing a hat and scarf 69% of the time, and people wearing a hat, scarf, and glasses 55% of the time. (Reynolds) This example is showing that the potential for powerful facial recognition technology on limited information exists.

The ultimate method to stop people from avoiding facial recognition technology is policy. A policy requiring the removal of all obscuring clothing, glasses, or jewelry where facial recognition is being used. This sort of policy may cause great outrage in a country like the United States but could be implemented in a country like China. It may start with requiring the removal of all facial clothing when entering certain buildings, then certain areas, then certain cities. Glasses might have to be the exception to this policy as it’s something that people need. Hats are already not very common in Chinese culture. A law banning hats and scarves in an area doesn’t sound too farfetched. People in the United States are already required to remove clothing articles when going through security checkpoints like an airport. Policy is certainly necessary to guarantee the accuracy and usefulness of facial recognition technology.

**Facial Recognition use in China**

China is the most populated country on Earth. With about eighteen percent of the world’s population, China has the capabilities to have the largest and most accurate facial recognition database. Their initial goal was to catch jaywalkers in busy streets. The police can catch these jaywalkers by scanning their faces on CCTV cameras and matching their face with a face in the database. To enforce punishment for jaywalking, they have implemented a public shaming event in which case if one were to be caught by the CCTV the face captured would be displayed on large LED screens. These screens can be found on sidewalks and bus stops. There are companies that have started working with social media platforms and cell phone carriers to implement texting fines to those who were caught jaywalking. This would mean one’s cell phone number and social media accounts would be linked to one’s face in the database. Their goal is clear; to implement safety and control, but is this the furthest China is willing to take it?

As the technology proved more useful and advanced, they have expanded its capabilities to simple tasks such as using facial recognition for unlocking apartment doors, verifying identities at ATMs, bank, airports, some popular apps such as China’s uber system, as well as suspect tracking and crime monitoring. Through the implementation of facial recognition people are likely feeling safer.

Suspect tracking and crime monitoring is where facial recognition is used the most. After all, it was initially used to punish jaywalkers. Facial recognition allows individuals to be caught completely off guard. A thirty-one-year-old Chinese man wanted for economic crimes was caught in a concert. He was first seen by CCTV in the ticket entrance. The police were able to follow him and identify him within a crowd of 600,000 concert goers. Another twenty-five suspects in Qingdao International Beer Festival was also caught unexpectedly through facial recognition (Malm). The police have started using facial recognition sunglasses. They look like regular sunglasses, but they are connected to an internal database of suspects making it easier to scan crowds for wanted persons (BBC). This shows the dedication the police have to find, monitor, and track suspects, as well as how accurate their tools are. China is not afraid to use any type of technology that they deem will make the country safer. This is a concerning position and likely means that there will be future technologies that are even more invasive implemented in China.

Safety is not the only goal for China. The social credit system is being introduced and facial recognition is a big part of its growth. “...In China, the government is developing a much broader ‘social credit’ system partly based on people’s routine behaviors with the ultimate goal of determining the ‘trustworthiness’ of the country’s 1.4 billion citizens” (Rollet). This system aims to assign every citizen a credit score and based on that score they will either be prohibited to do activities or rewarded with financial benefits. A couple things that will lower social credit would be as small as jaywalking or buying too many video games. A couple of absurd reasons that will lower social credit is playing more than ten hours of video games a day or if you are caught cheating in a video game. Activities that one might enjoy are now limited through this system. This is because of its long term and severe social punishments and limitation of freedom. Some of the punishments one might receive if their social credit were to go down would be banning one’s right to purchase plane or train tickets, banning domestic flights, slowing internet speeds, banning families from the best schools, limiting job options, as well as being publicly named as a bad citizen. Rewards for having a great score are financial gain such as discounted energy bills, better interest rates, as well as having more matches in dating sites and jumping healthcare waiting lists (Rollet). A person’s score will depend on how they will live, and the unpredictability and omnipresence of social recognition technology leaves little room for human error in what China deems a proper citizen.

By 2020 China aims to have social credit fully implemented nationwide, add an additional four hundred million CCTVs to the 170 million they currently own, and aim to make the video surveillance network “omnipresent, fully networked, always working and fully controllable” (Denyer). The Chinese government is willing to go as far as to be able to link and monitor citizens in their homes by accessing smart devices. Companies are developing the “Sharp Eyes” platform that allows them to link up with street CCTVs and smart home devices (RFA Staff). This means privacy of one’s own home is now being taken away for the convenience of the government and the social credit system will follow the citizens to their homes.

China is not the only country to use facial recognition technology, but China’s ambition makes them stand out the most. Their large population, number of CCTVs, and dedicated police force makes it easy for their facial recognition database to grow, as well as make the deep learning aspect of facial recognition grow at a significant rate compared to other countries. The world may be shocked to see how different China will be in 2020 and years to come.

**Facial recognition in the United States**

Many may be surprised to learn the degree that facial recognition technology is being used in the United States. There is a program being launched called the Vehicle Face System that will aim to capture a high-quality image of every person entering and leaving the United States at a particular border checkpoint. This system will compare this image to existing data from sources like passports and visas and attempt to find a match. This is a test program of sorts and the government is trying to see what their current technology is capable of. “Once these kinds of powerful surveillance systems are built and deployed, the privacy harms … can’t be undone,” said Mitra Ebadolahi a staff attorney with the American Civil Liberties Union (Levin).

The FBI uses facial recognition a substantial amount. It has two facial recognition programs the Next Generation Identification (NGI) system and the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit. The NGI is a biometrics database that is gathered from those with a criminal record. Its facial recognition data comes from mugshots. The FBI will accept a photo from a law enforcement agency and search that against their NGI database. The FACE Services Unit is reserved for cases that the FBI is investigating (Del Greco). The FBI’s facial recognition searches return a list of between two and 50 candidates and this list is sent to the agency that requested the search. From there humans analyze the results and search for a match, but research shows that humans are not very good at identifying people especially if they don’t already know them or they are a different ethnicity (Lynch). This is definite cause for concern because the risk of misidentification is high in these cases and the effectiveness and accuracy of this technology needs to be called into question. If these methods aren’t reliable they should not be used especially in criminal cases where people's lives are at stake. This is compounded by the fact that one of FBI’s senior photographic technologist conducted researching finding that, “face recognition misidentified African Americans and ethnic minorities, young people, and women at higher rates than whites, older people, and men, respectively” (Lynch). These minority groups already face discrimination in the United States justice system and the potential for injustice is only raised by using facial recognition technology.

The United States is certainly entering a dangerous territory with technology that is this invasive on privacy. It can be expected that this is just the beginning and that the government will aim to expand projects like these. It’s use at the border can easily be justified as wanting to identify criminals entering or leaving the country. United States citizens needs to be weary as this technology will likely be appearing in other sectors. There are some major issues with the way the FBI specifically is using facial recognition technology. The biggest problem is their lack of transparency especially when it comes to privacy. There are no clear rules for the collection and storage of facial recognition data by the FBI. This is concerning because their collection could be expanded at any time. A driver’s license photo is meant to confirm an identity and information in person. Consent was never given to allow these photos to be used by the FBI for any purpose. The way facial recognition data is collected and used needs to be addressed. People have the right to know when their data is collected, how it’s being stored, and what it’s being used for. Ideally there would be a process a person could go through to request their data be removed from these databases.

There are certainly benefits of using facial recognition technology. It can be used to help identify fugitives and missing persons. It can help law enforcement agencies identify persons of interest from images. It can be used to reduce crime by performing automated surveillance at high-risk locations. The benefits of facial recognition right now in the United States are virtually all security related. It’s being used to prevent crime and prosecute criminals. As of now it doesn’t seem like the United States is moving the same direction as China when it comes to its use of facial recognition. However, the future is still unclear, and the FBI has made it clear that it wants to adopt facial recognition and any future technologies to help their agency provide the best security they can. US citizens need to be weary of the implications this technology brings.

**Ethical Analysis**

Facial recognition is used in many ways and is still a new type of technology, making its ethicality questionable. The Chinese government clearly states what they wish to achieve with this technology and its wish to become omnipresent and always watching is very similar to George Orwell’s 1984. Orwell’s 1984 explores a dystopian future where “Big Brother is watching you.” People are constantly being monitored and anything that seemed to threaten the stability of the government or upper class was punishable through doublethink (brainwashing) or disappearing (death). This results in a loss of self and freedom for everyone, and full control of all lives was given to a handful of people through fear and constant surveillance.

It is very possible to think that China may end up in an Orwellian dystopia. China’s goals by 2020 plant seeds towards this future. Their goal of adding four hundred million more cameras to the millions they currently have means more surveillance in more places. The ability to link up to any smart devices in a citizen’s home greatly suppresses freedom of thought and speech as one’s home is a place where they can truly feel and be who they are. China’s main reason for these is for safety and requires full compliance from its citizens for this type of system to work effectively. Even in its early stages, many have found this type of system undesirable and have been caught and punished. “It’s basically a crime in China to advocate for human rights protection… The government treats human rights activists, lawyers and ethnic Uighurs and Tibetans as criminals, and these people are being caught, jailed and possibly tortured as a result of this technology” (Denyer). These human rights activists, lawyers and ethnic groups are being treated very similar to the people under Big Brother. What enforces this Orwellian future even more is the social credit system. This system lays foundation to Big Brother’s punishments to those who oppose. In China’s case, these are punishment to those who do not meet their standard of an ideal citizen. It is still unclear what China’s future may hold and whether a dystopia will be in China’s sights, but its current path frighteningly reveals a very similar future to Orwell’s 1984.

In a teleological sense, facial recognition is unethical. Teleological depends on the ends. The actions in between mean little if the end is good, then it is ethically acceptable. Since facial recognition is such a young new technology and even if goals have been stated, the end is still a mystery. China aims to apply numerous cameras and facial recognition technology for the safety of its people. As time moves forward, it starts to go towards an Orwellian dystopia. If it were to go towards a path of safety, then it would be ethically correct, but if it goes towards harming people more, then it is ethically unacceptable. Even if the case were to be look in a utilitarianism view, Jeremy Bentham, one of the most influential utilitarian philosophers would also agree. In utilitarianism, the greater happiness means the greater moral merit of the act. Looking at the three main stakeholders that are directly affected, the government, the people, and AI companies, only the government and the companies will fully gain rewards for such a system. These handful of people would gain economic power and control. While the majority of the population, the people, would be controlled and live through fear. The indirect stakeholders are the future generations. One of the punishments of social credit involve banning people and their children from the best schools, as well as banning people from the best jobs. Families will be limited from the best education and income because of close and strict monitoring of their actions. Therefore, the number of stakeholders being affected by the possible Orwellian dystopian end is more in quantity and intensity than the handful of those in the government and companies.

Facial recognition is also deontologically unethical because it harms people’s basic human rights of freedom of speech, thought, choice, and privacy. Deontology is principle and rights-based meaning that individuals have rights that should not be sacrificed simply to produce a net increase in the collective good. Even on the surface of the issues of the implementation of a facial recognition system, human rights are being pushed aside for the safety of all people, but how safe can people really be if they have to hide how they live from the government that wishes to keep them safe. Immanuel Kant, a famous deontological philosopher stated that people should not be treated as ends or means to ends. The government is doing just that. Their system currently is very similar to how an anomaly-based intrusion detection system works. The government wishes to have a safe country and by doing so wants to eliminate bad citizens by punishing them through the social credit system. In this case, the government is using its own citizens as means to achieve this goal. Anomaly based IDS works by collecting statistical data by observing traffic that is known to be normal and overtime this period is called the training period If any activity is above this baseline, an alert is sent to the administrator (Whitman et al). The training period would be based off what the government deems to be a good example of a citizen. Anyone who does not follow that example, would be tracked by the facial recognition cameras and the police department and the Chinese government would be alerted of this behavior. In this case, the Chinese are treating their people as viruses and to be kept in their system, they must have fully compliance to the example of a good citizen as well not show any signs of threat to the stability of the system.

Overall, facial recognition may seem acceptable currently in the short-term, but it is also important to analyze its social and ethical effects on society in the future. China is one example many people do not wish to follow due to its similarities with Orwellian dystopia. The United States has more cameras than China, but ambitions and dedication set them apart. “China seeks to achieve several interlocking goals: to dominate the global artificial-intelligence industry, to apply big data to tighten its grip on every aspect of society, and to maintain surveillance of its population more effectively than ever before” (Denyer). Facial recognition is a technology that has many opportunities to be useful and promote safety without sacrificing human rights and happiness of individuals and their future kin. It is important to think of how this affects an individual and not just its effects on the collective good. This technology is coming, and its ethical consequences are being ignored in China. The United States government clearly wishes to utilize this technology as well. Currently, the United States isn’t aiming for the same level of control as China, but citizens must remain vigilant to ensure that their privacy isn’t forfeited under the guise of security. Facial recognition could find an acceptable role in society. It’s usefulness for authentication commercially and identification governmentally can’t be denied. On its current trajectory the use of facial recognition technology by the governments of the United States and China is unethical and needs to be addressed.

**Citations**

Bonsor, Kevin, and Ryan Johnson. “How Facial Recognition Systems Work.” HowStuffWorks, HowStuffWorks, 4 Sept. 2001, electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition1.htm.

“Chinese Police Spot Suspects with Surveillance Sunglasses.” *BBC News*, BBC, 7 Feb. 2018, www.bbc.com/news/world-asia-china-42973456.

“DeepFace.” *DEEPFACE*, deepface.ir/.

Del Greco, Kimberly. “Law Enforcement's Use of Facial Recognition Technology.” *FBI*, FBI, 22 Mar. 2017, www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology.

Denyer, Simon. “China Bets on Facial Recognition in Big Drive for Total Surveillance.” *The Washington Post*, WP Company, www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?utm\_term=.7777286b7987.

Denyer, Simon. “China's Plan to Organize Its Society Relies on 'Big Data' to Rate Everyone.” *The Washington Post*, WP Company, 22 Oct. 2016, www.washingtonpost.com/world/asia\_pacific/chinas-plan-to-organize-its-whole-society-around-big-data-a-rating-for-everyone/2016/10/20/1cd0dd9c-9516-11e6-ae9d-0030ac1899cd\_story.html?utm\_term=.5b25060ecdb1.

Levin, Sam. “US Government to Use Facial Recognition Technology at Mexico Border Crossing.” *The Guardian*, Guardian News and Media, 5 June 2018, www.theguardian.com/technology/2018/jun/05/facial-recognition-us-mexico-border-crossing.

Lynch, Jennifer. “Face Off: Law Enforcement Use of Face Recognition Technology.” *Electronic Frontier Foundation*, 23 Feb. 2018, www.eff.org/wp/law-enforcement-use-face-recognition.

Malm, Sara. “Chinese Police Use Facial Recognition Technology to Pick out a Suspect in 60,000-Strong Concert Crowd and Arrest Him.” *Daily Mail Online*, Associated Newspapers, 12 Apr. 2018, www.dailymail.co.uk/news/article-5607559/Chinese-police-arrest-man-using-facial-recognition-60-000-concert.html.

Pettit, Harry. “'Face Stealing' Cap Uses Infrared to Fool Facial Recognition Systems.” *Daily Mail Online*, Associated Newspapers, 21 Mar. 2018, www.dailymail.co.uk/sciencetech/article-5526885/Face-stealing-cap-uses-infrared-fool-facial-recognition-systems.html.

Revell, Timothy. “Glasses Make Face Recognition Tech Think You're Milla Jovovich.” *New Scientist*, New Scientist, 1 Nov. 2016, www.newscientist.com/article/2111041-glasses-make-face-recognition-tech-think-youre-milla-jovovich/.

Reynolds, Matt. “Even a Mask Won't Hide You from the Latest Face Recognition Tech.” *New Scientist*, New Scientist, www.newscientist.com/article/2146703-even-a-mask-wont-hide-you-from-the-latest-face-recognition-tech/.

Rollet, Charles. “The Odd Reality of Life under China's All-Seeing Credit Score System.” *WIRED*, WIRED UK, 5 June 2018, www.wired.co.uk/article/china-social-credit.

Staff, RFA. “China Aims For Near-Total Surveillance, Including in People's Homes.” *Radio Free Asia*, Radio Free Asia, 2 Apr. 2018, www.rfa.org/english/news/china/surveillance-03302018111415.html.

Whitman, Michael E., and Herbert J. Mattord. *Principles of Information Security*. Cengage Learning, 2018.