Seth Howell & Joshua Blank
Professor Derrick Tate, PhD
CS 308: Christian Ethics in a Digital Age
March 9, 2021

We Have Been Recognized: Facial Recognition and the Hong Kong Protests

Intro

In 2019, the Hong Kong government attempted to pass an extradition bill in response to a homicide in which a resident of Hong Kong murdered his pregnant girlfriend in Taipei. The bill would allow criminal offenders to be extradited between Hong Kong and other members of the People's Republic of China (including Taiwan). While in this specific case, the bill seemed justified, many worried that this would allow citizens of Hong Kong to be extradited to mainland China.[1] This fear caused a series of peaceful and violent protests that started in early 2019 and lasted until the beginning of 2020. Throughout the many months of the protests, many conflicts erupted between protestors and the police. This, however, was not the protestors' greatest fear. Instead, the protestors feared that the government would use surveillance technology such as facial recognition to gather information on them, information that would eventually be used against them. This fear led protestors to adopt some very interesting tricks and techniques in an attempt to be anonymous.

What Is Facial Recognition?

Facial recognition describes the process of using mathematics and computer programs to identify human faces within images. It is a technology that finds its origins, and arguably ends, in the hands of the police and military for the purpose of surveillance. In 1964 Woodrow Bledsoe produced some of the earliest Facial processing technology (FPT). He developed a computer program to identify suspected criminals by comparing a suspect's face in a probe photograph against a book of mugshots. Each person's face was encoded into a vector which contained the computed distances between facial features. Early FPT thus matched faces by comparing these measurement vectors and finding where the numbers were close to equal. This process however was computationally expensive and lacked robust datasets.

By 1996, U.S. government officials recognized the value of FPT, viewing the face as "a non-invasive biometric attribute that could be used to track and identify individuals without requiring their explicit physical participation."[2] Organizations like the Department of Defense and the National Institute of Standards and Technology (NIST) funded 6.5 million towards FERET, a dataset of 14,126 faces. Research thus increased exponentially and new computer methods such as support vector machines (SVM's), simple convolutional neural networks (CNNs) and hidden Markov models (HMMs) increased the accuracy of FPT. Yet, the technology still wasn't dynamic; small environmental changes and facial expressions could cripple recognition performance.

A third phase of FPT was reached in 2007 when web-scraping from platforms like Google and YouTube allowed for massive datasets with faces captured in an infinite number of settings.[3] Furthermore, benchmarks such as ChokePoint were developed to source face images from surveillance footage. One of the larger databases included 30.2 million images of 14.4 million individuals by 2013.

The final phase of FPT, which is continuing to be developed, is the use of deep learning AI. Alexnet in 2012 and DeepFace in 2014 introduced the use of neural networks to mainstream facial recognition research, allowing for up to 97% accuracy rates. With deep learning, computer programs are able to easily locate a face within a bounding box in an image. These programs can then match a specified image against the dataset repository and return the most similar results.[4] Science editor Ian Sample describes these two steps, face *detection* and *recognition*:

> [First the computer learns what a face is by training a] deep neural network on a vast number of photos that have faces in known positions. Each time the algorithm is presented with an image, it estimates where the face is. [After] multiple times, the algorithm improves and eventually masters the art of spotting a face… [Next, the recognition is commonly done by feeding a second neural network] a series of face pictures and [it] learns – over many rounds – how best to tell one from another. Some algorithms explicitly map the face, measuring the distances between the eyes, nose

> and mouth and so on. Others map the face using more abstract features. Either way, the network outputs a vector for each face – a string of numbers that uniquely identifies the person among all the others in the training set.

He explains that this software can be employed on video footage in real time (see exhibit 1). The computer examines each frame from the video and after detecting the faces in the frame it outputs a vector for each one. These vectors can then be checked against a specified person or a watchlist of people. All the matches exceeding a certain threshold (for example 60% in the UK), are then ranked and displayed (see exhibit 2 for a graphic of this vectorization process). Inversely, a person's image can be uploaded to trace back their movements from surveillance footage.[5]

FPT has become widespread. It is used as biometric identification to unlock devices, to tag people in photos on social media, to categorize your images by person in Google Photos, advertising, and much more. However, FPT remains primarily a tool of the government. It was historically developed for "the purpose of identifying suspects for pursuit and apprehension, whether in the context of law enforcement, war or immigration" and continues to be developed for these purposes today. Raji and Fried warn those working to improve FPT that they "must acknowledge its legacy as a military and carceral technology, and their contribution toward those objectives."[6] Examples of this usage are found most extensively in the US, Russia, China, Japan, Israel, and Europe.[7]

The Hong Kong Protests

A prime example of facial recognition and the effect it can have is the Hong Kong protests. In this situation, just the very possibility of being tracked using facial recognition and other technologies caused a great deal of fear among the protestors. Below is outlined some of the ways Hongkongers reacted to this threat.

Communications & Tracking

One of the surveillance technologies that the protestors most feared was the mainstream communications platforms. It is common knowledge that China monitors and censors WeChat, the Chinese equivalent of Whatsapp.[8] This knowledge drove protestors to opt for less conventional means of communication. Telegram, Apple Airdrop, and even apps like Pokemon Go were used by protestors to message dates for protests, locations of police, and general encouragement.[9]

Another technology that protestors feared was location tracking. Many believed that their phones and even ID cards could be scanned at protests by police and thus be used as evidence against them. In an attempt to prevent this, protestors powered down their phones and wrapped their IDs in tinfoil so that they could not be scanned.[10]

Facial Recognition

The technology that the protesters most feared was facial recognition and it was for this technology that protestors went to the most extreme measures. In preparation for protests, participants donned masks, hats, sunglasses, and any other form of covering in an attempt to protect their faces from the watching eyes of surveillance cameras. Beyond facial coverings, protestors directed much of their efforts towards eliminating as many cameras as possible. Spread across Hong Kong were "smart lamp posts" (see exhibit 3) that beyond simple lighting, provided extra camera surveillance. Protestors developed a strategy for disabling these cameras which involved huddling around the base of the post with umbrellas to provide protection for someone to cut through the base with saw, tear out wires, spray paint the lenses, or do anything else that could hinder the cameras' ability to operate (see exhibit 4). When this was not possible or the camera was too high to reach, protestors pointed lasers at the cameras in order to distract them.[11]

Whether or not the protestors were successful in their efforts is unclear. The fact also remains, there is no way of knowing for sure whether or not the government is using these technologies in the way that the protestors believed. The Hong Kong government has claimed that the "smart lamp posts" do not contain any facial recognition technology. However, this is hardly comforting considering that surveillance video can easily be stored and facial recognition could be run on the footage at any time. As discussed in an article by the Financial Times, Hong Kong citizens have long mistrusted their government because of lack of transparency and its broken democracy.[12] There does seem to be some evidence that gives credit to the suspicions of the protestors. For one, the government definitely has the technology to identify someone from a video or photo. In an article by Rosalind Adams, she explains:

> The photos taken for the IDs use live facial recognition to confirm a person's identity and are then stored in a database by the Immigration Department. The photos should be high enough resolution to include identifying features such as moles and scars, in order to provide a sophisticated level of facial recognition capability, according to a description of the contractor's requirements. The technology should also "support facial recognition from different sources, including camera and live video."

According to the article, the Immigration Department has so far claimed that they do not share this information with Hong Kong's police department. This, however, does not mean it is not happening. A second reason to question the government's claim that they are not using facial recognition is based on their banning of masks. After protestors began wearing masks in order to protect their identities, Hong Kong instituted an emergency ban that prohibited Hongkongers from wearing masks at the risk of a year in prison or up to a 25,000 Hong Kong dollar fine. The reasoning behind this ban was that masks made it easier for "lawbreakers" to get away with their crimes. The security secretary of Hong Kong said about this ban, "One thing is certain. If lawbreakers are not wearing masks, it is much easier for us to prove the charges and bring them to courts."[13] Unless Hong Kong was running some sort of facial recognition on protestors, it would seem as if this ban would be meaningless.

The protests ended in early 2020 mainly due to the sudden rise of Covid-19. While there was little resolution to the protests, many people's lives remain affected. Participants of the protests have been convicted and are continuing to be convicted. On March 31, 2021, seven pro-democracy leaders were convicted of unauthorized assembly. They await sentencing which will occur on April 16.[14]

China

The fearful disdain that protesters in Hong Kong have toward facial recognition is rooted in its abuses by the Chinese government. In *We Have Been Harmonized*, Kai Strittmatter explores how FPT is being used as a means of control, from areas of daily business and education to the areas of crime and security. High definition surveillance cameras record citizens on public transport and in the city, transmitting their facial expressions to ultra-clear images in real time. Paired with the government's detailed records of its citizens, the surveillance recognition is used in highly invasive ways and with great accuracy. For example, the police are using FPT in Jinan and Shenzhan to publicly shame jaywalkers by projecting their faces onto a video screen alongside their name, address, and ID number.[15]

In some schools, FPT is being used to monitor all of the students. The technology is so advanced that it is able to analyze the students' moods, whether they are on task or not, and their energy levels by examining their facial expressions and actions. This level of privacy invasion is expanding to the national level. In 2018, Chinese journalists reported that through Skynet—China's nationwide network of more than 200 million cameras—the government can instantly identify any one of China's 1.4 billion citizens.[16] More recently, China's FPT has been paired with the ability to read people's temperatures in the wake of the Coronavirus. Companies like SenseTime installed their cameras in subway stations, schools, and shopping malls. These cameras are accurate enough to recognize most individuals through their face masks and determine whether or not they have a fever. This technology was also used in Alibaba's incredibly popular health code app that became used in all sectors of society. The facial recognition app displayed either a green, yellow, or red bar based on a user's temperature, determining whether they should be in quarantine or travel freely.[17]

Given FPT's history of identifying false positives, perhaps China's most worrisome use of the technology is in the crime sector. Strittmatter points out that while the FBI's FPT in the US identified the wrong people in 15 percent of criminal searches, China has a conviction rate of 99.9 percent and the "state apparatus is always right," even where evidence is lacking.[18] VICE journalist Elle Reeve was told about this technology first hand. A Megbii employee described Skynet as follows:

> Everything that happens in the public can be recorded. We can know exactly what is happening at every second, in every corner of the city. [Pointing to a video stream from the subway where numbers appear above each person's face, he continues.] We can capture every face in real time. So if there is a criminal person out there, there is the "red box." [A warning is then] sent to the police station that there is a criminal person, so I need to locate them… [In the last year alone, we have apprehended] over 3,000 [fugitives] nationwide.[19]

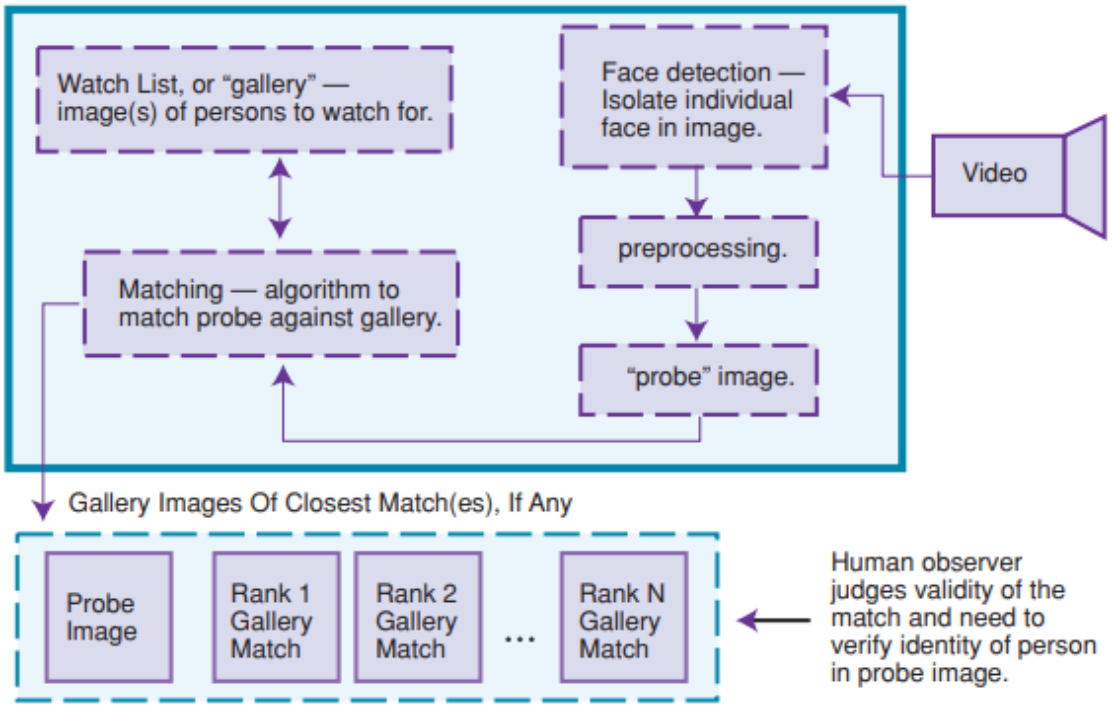
According to his account, it is evident that China is using video surveillance cameras to pinpoint criminals and take action against them.

Although some of China's claims about its FPT are overblown, the intimidation factor of being observed remains. Strittmatter captures this nicely: "The all-seeing eye doesn't have to be looking at you for the panopticon to function. All that matters is that you feel it might be—even if in reality, it isn't there yet." This tension is what we are seeing in the Hong Kong protests. Whether or not FPT is being used on footage from the smart lamps, the possibility itself is insiting fear into the protestors and leading them to take precautionary measures.

Conclusion

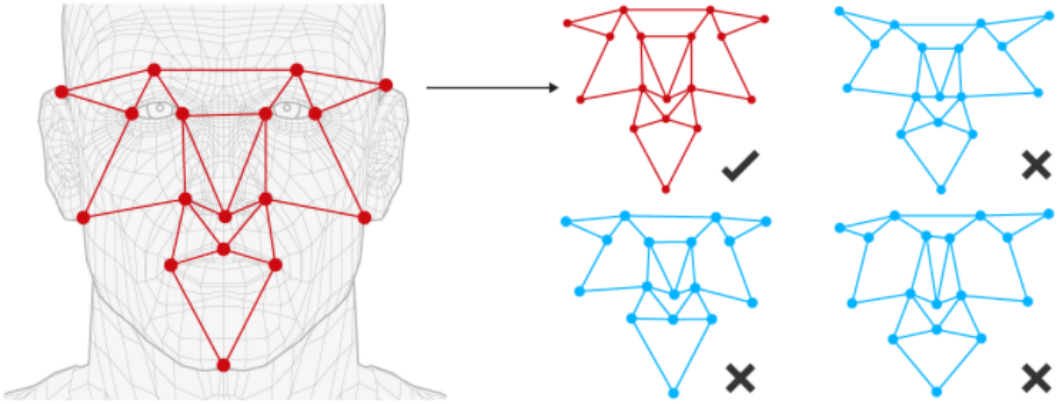
Facial recognition is ultimately a very controversial technology. One does not have to think very hard to realize the potential benefits that would come if it were perfected. However, throughout this article, it has been demonstrated that facial recognition also has some pitfalls and dangers. To summarize the main points of this case study, remember first that facial recognition has and will continue to be used as a tool of the state. It inherently attracts groups like law enforcement that are interested in using it to track and apprehend people. Because of this, many governments have begun gathering huge datasets of faces, generally without consent from their citizens. This allows these governments to track citizens on a massive scale. The problem is, any government can access facial recognition technology once it exists, whether they have good or ill intent. Even more, governments can be using facial recognition without the knowledge of their citizens. Hong Kong is the perfect example of this. There is no way of knowing how the Hong Kong government is using its facial recognition technology and this fact alone gives them a certain sense of power. Because Hongkongers did not know what their government was doing, they were forced to take preventative measures, sometimes quite extreme, during their illegal protests. Ultimately, the point is that facial recognition can be used for good (law enforcement apprehending real criminals) or for evil (corrupt governments using it to track, arrest, or even intimidate their people). While some of these evils may be mitigated with regulations, in the hands of an unchecked government, regulations mean very little. So the question that remains is, "Do the potential goods of facial recognition outweigh the potential evils?" If so, what should be done about the evils? And if not, what should be done with this technology? None of these have easy answers. But an answer must be given.

Exhibit 1 - Recognizing faces from videos



Source: Kevin W. Bowyer, "Face Recognition Technology: Security versus Privacy", University of Notre Dame.

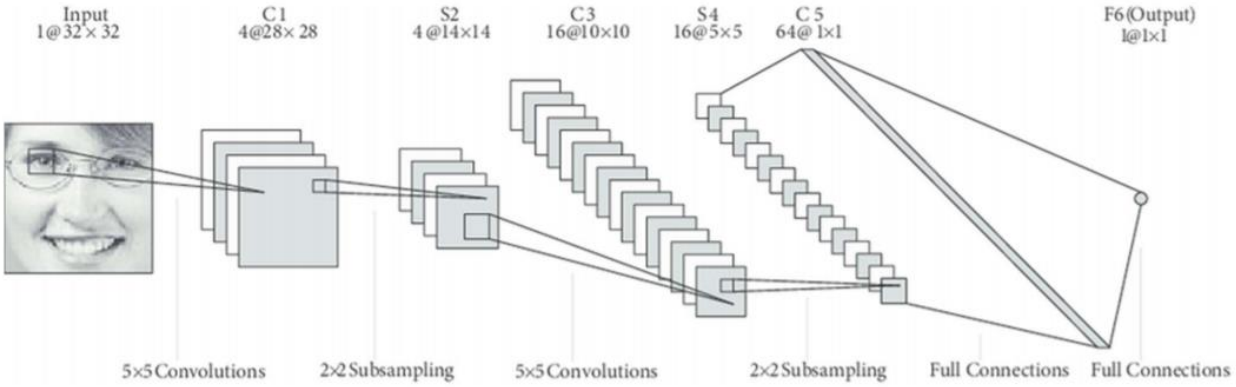
Exhibit 2 - Facial Recognition and Vectorization



1
Facial recognition software reads the geometry of a face captured from a photo or video to create a unique code or 'faceprint'

2
Faceprints are compared with those on a watchlist and a computer ranks likely matches which are later verified by a human operator

Source: The Guardian



Source: Yang Li, "Face Recognition System", Harrisburg University.

Exhibit 3 - Photo of Smart Lamp Post

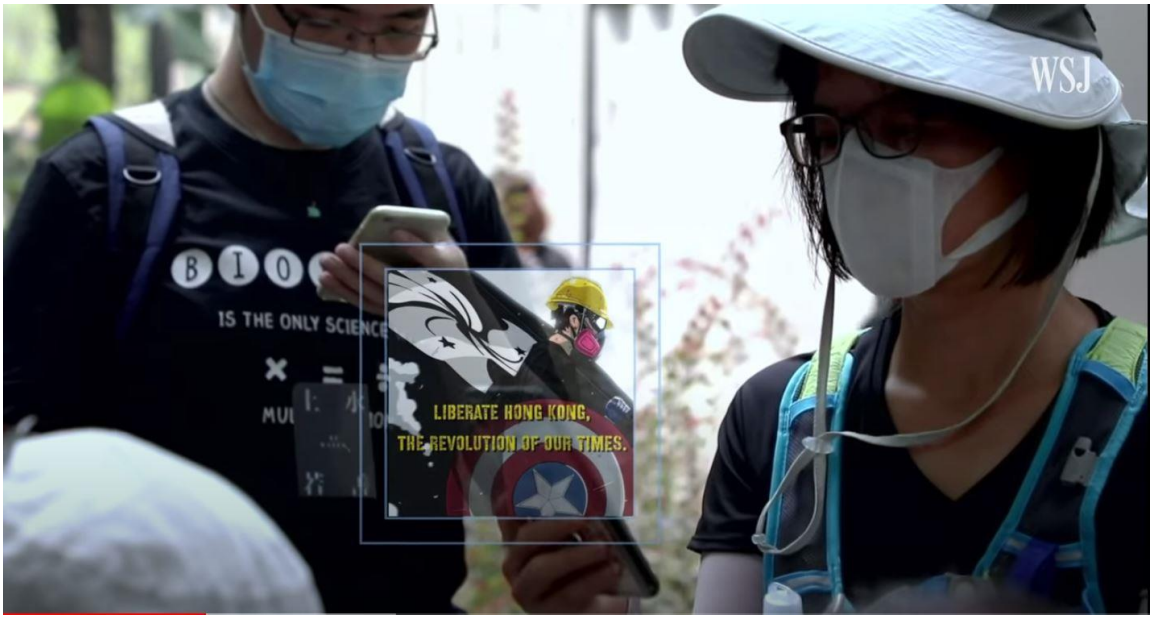
Source: The Construction Index

Exhibit 4 - Photo of Protestors Destroying Smart Lamp Post

Source: Tweed Daily News

Exhibit 5 - Video Discussing Technologies Used by Protestors

How Hong Kong Protesters Evade Surveillance With Tech | WSJ - YouTube



Source: Wall Street Journal

Exhibit 6 - Facial Recognition in China

How China Tracks Everyone

Source: VICE News

Bibliography

---

[1] Martin Purbrick, "A REPORT OF THE 2019 HONG KONG PROTESTS." Asian Affairs (2019), 50:4, 465-487, DOI: 10.1080/03068374.2019.1672397.
[2] Inioluwa Deborah Raji and Genevieve Fried, "About Face: A Survey of Facial Recognition Evaluation." ArXiv abs/2102.00813 (2021), 2.
[3] Ibid, 3.
[4] Ibid, 2.
[5] Ian Sample, "What is facial recognition - and how sinister is it?" The Guardian (2019). Accessed on March 6, 2021 at https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it.
[6] Raji and Fried, 8.
[7] Ian Sample.
[8] Shannon Liao, "How WeChat came to rule China." The Verge (2018). Accessed on March 1, 2021 at https://www.theverge.com/2018/2/1/16721230/wechat-china-app-mini-programs-messaging-electronic-id-system.
[9] Martin Purbrick.
[10] Wall Street Journal, "How Hong Kong Protestors Evade Surveillance With Tech | WSJ." YouTube (2019). Accessed on March 1, 2021 at https://www.youtube.com/watch?v=32KTKXZZ-BI.
[11] "How Hong Kong Protestors Evade Surveillance With Tech | WSJ."
[12] Yuan Yang, "Why Hong Kong protestors fear the city's 'smart lamp posts'". Financial Times (2020). Accessed on March 1, 2020 at https://www.ft.com/content/f0300b66-30dd-11ea-9703-eea0cae3f0de.
[13] Emily Feng, "Hong Kong Bans Face Masks At Public Assemblies." NPR (2019). Accessed on March 1, 2021 at https://www.npr.org/2019/10/04/767098579/hong-kong-bans-face-masks-at-public-assemblies.
[14] Austin Ramsey, "Hong Kong Court Convicts Democracy Leaders Over Protest March." The New York Times (2021). Accessed on March 1, 2021 at https://www.nytimes.com/2021/03/31/world/asia/hong-kong-democracy-protest.html.
[15] Kai Strittmatter. *We Have Been Harmonized*. Custom House (2020). Kindle Edition. p. 192.
[16] Ibid, 193.
[17] Ibid, 195.
[18] Ibid, 193.
[19] VICE News, "How China Tracks Everyone." YouTube, 2019. Accessed on March 8, 2020 at https://www.youtube.com/watch?v=CLo3e1Pak-Y.