Heavy Use of Facial Recognition Technology on China's Citizens, Government, and Industry

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Bryan Kim

Spring 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Sean M. Ferguson, Department of Engineering and Society

Heavy Use of Facial Recognition Technology on China's Citizens, Government, and Industry

Introduction

From recreational uses to unlock smartphones or make payments to security applications for surveillance and identification, the rise of Facial Recognition Technology (FRT) is not slowing down. Sixty-four out of 176 countries are actively using FRT systems for surveillance purposes, with China and the US being major suppliers (Feldstein 2019). While both countries provide a large portion of global distribution and use a good amount of the technology themselves, China's deep integration of FRT in its private and public sectors has heavily impacted China's culture and way of life. Using the Social Construction of Technology (SCOT), this paper will be looking at the rise of FRT in China's private sector and explore the power dynamics within the ecosystem consisting of citizens, government, and industry that paved the way for FRT to take over China's culture with their actions. This case study is important as it can provide insight to other countries on the effects of heavy usage of mainstream technologies such as FRT that handle highly sensitive information and the privacy concerns that follow.

Background: SCOT

The Social Construction of Technology (SCOT) framework looks at how relevant social groups of a specific artifact, in our case the artifact would be facial recognition, shape how such artifacts develop as they play off of other social groups in the mix. For a social group to be relevant, the group should be interacting with the artifact one way or another such as producing, investing, consuming, and regulating such artifacts. An

important characteristic these social groups have is interpretive flexibility, meaning that each group can have their own positive or negative interpretation of the artifact. SCOT takes this into account during the developmental process of the artifact. Developmental processes are traditionally viewed in a multi-directional model, explaining why some variants of solutions survive while others die (Pinch 1984). In the context of FRT in China, the developmental process will be more of a linear model, as the technology will be discussed on how it is being applied in China rather than on how it was conceived.

This moves us to the first stage of SCOT, which is to reconstruct the alternative takes and interpretations from different social groups on the artifact to analyze why problems arise in some social groups while working for others. From here, SCOT will go through one of two types of closure. The first is the rhetorical closure, where all groups seem to have reached a solution adequate for all parties. The other solution would be to redefine the problem as new iterations of an artifact can cause further issues with existing or new groups. With enough closure, there will remain a dominant strand where alternative innovations are no longer viewed as viable in the long term (Pinch, 1984, pg 419-428). The main focus of this paper will be on how relevant social groups and stakeholders affect the usage of FRT in China. By discussing the different motives and power dynamics between the members of the ecosystem above and going into how change and agreement will occur among the three actors.

Background: Facial Recognition Technology

FRT's main role is to authenticate the identity using biometric data extracted from an individual's face and has been developed to perform very efficiently. This task is

done by utilizing automated face detection and analysis software including artificial intelligence that takes into account various features of the face, including the eyes, nose, and mouth. These personal identifiers are then extracted into manageable data and compared to a database to finally match and authenticate whatever needs to be processed (Zhang 2021). The highly sensitive data is being extracted from the users, or in this scenario the people of China, by the industry and Chinese government for their use of profit and surveillance respectively. To summarize, the ecosystem comprises the citizens, who actively use FRT in their daily lives, China's government, which utilized FRT for surveillance and security, and the industry, which provides various implementations of FRT to the public.

Though this paper will be talking about China's role as a legislator, it is important to point out the government's use of the technology as well. They view FRT as an "effective tool to improve public service provision and supervise corrupt government officials", with over 400 million CCTVs planned to be installed by 2020 (Kostka 2021). Even with a large presence of FRT in China, there is still a high acceptance from the public. A study with 4 countries including China and the United States was conducted with online surveys to gauge the acceptance of facial recognition usage by the government. From the 6100 Chinese citizens surveyed, the acceptance for FRT use by private enterprises is 17%, private-public partnerships (PPP) is 58%, and central government is 60% (Kostka 2021). With China's government being authoritative there is a motive for some participants in the study to answer out of fear. However, with the guaranteed security and safety the government has provided, it is very likely that the citizens are willing to sacrifice their privacy. Unlike the profit-driven industry, China's

government claims to provide security and surveillance for the citizen's best interest with their use of FRT, with large support from the public.

Background: Scholarly Conversation

Conversation about FRT and other "Smart" systems have been in discussion for a while. A recent study in 2013 took place in Germany looking at how "Smart" CCTV systems that utilize algorithmic surveillance such as FRT were socially constructed into Germany's infrastructure. This paper will see similarities of gripes with FRT in China and "Smart" CCTV's in Germany as the study was able to determine that the core argument against "Smart" CCTV was that it "might pose threats to the value of personal liberty" with privacy infringements (Möllers, 2013). Möllers and Hälterlein, authors of the study, determined that the "success and failure of technology depend not only on their social meanings, but also on structural factors" including power dynamics between social groups and the country's political culture (Möllers, 2013). This is shown as the study states that the use of "Smart" CCTV matched with Germany's present political culture, helping the push for providing more security at the risk of losing some privacy liberties. Also, any arguments in opposition to "Smart" CCTV was brought to the attention of its developers resulting in further research and development to reach Germany's standards, thus helping the technology's case. A good portion of the public had concerns about their privacy, yet these other factors had outweighed the largest argument against the technology.

Though there was discourse throughout the process of integrating "Smart" CCTV's, the technology was eventually implemented in Germany thanks to a version of

checks and balances with the opposition groups, supporters of “Smart” CCTV, and the government. Their actions, whether to intentionally help CCTV or not, helped mold the technology to better fit with Germany's culture and regulations, resulting in the technology’s implementation.

Rise of Facial Recognition

With the lack of regulation for FRT from the government and the advancements that occurred with FRT in 2014, According to Tristan Brown, a researcher at MIT, and other researchers in their article on facial recognition technologies in China, they state that China saw various tech companies and startups rising up and taking advantage of this sudden gold mine of an industry (Brown 2021). The industry soon after pushed out innovative and experimental FRT tools to citizens to the point where actions ranging from making payments to accessing parks and facilities are handled with FRT (Zhang 2021). As the FRT continues to increase its presence in the market, the ease and satisfaction the new technology provided to the users outweighed much of the peoples’ concerns about giving away their sensitive data. A major reason why FRT from industry had taken over China’s citizens was due to two key factors; improved security and more convenience (Brown 2021). By providing an option for simplification to mundane actions such as online payments with a single face scan, people will be more likely to choose the path with the least resistance.

The initial public acceptance and lack of government regulation only grew the industry’s presence in the facial recognition market. With more potential for profit, the industry began to incorporate the technology in ways that strayed from the two key

factors and began to infringe on privacy. Such risks include identity theft sold for cheap, facial data being publicly accessible online, or even sold to third-party companies overseas to be used for their own benefit. The people's right to their data should not be overlooked, especially due to the sensitive nature of the data.

The Industry and the People

The power dynamic between the industry and citizens of China initially can be classified as seduction as citizens were enticed by the positive benefits of convenience and security, but it has now shifted more towards coercion as industry strays away from those two main factors, as mentioned in Brown's article discussed in the previous section. This is apparent with the first lawsuit case involving FRT and privacy. In 2019, a safari park in the city of Hangzhou recently replaced its fingerprint-based admission with a facial recognition system. It was when Guo Bing, a professor of law and owner of a year pass at the zoo, noticed that the private zoo had signed him up for the facial recognition system without consent with his pictures already in their database. Deeply concerned about his privacy, Guo asked for a refund of his yearly pass. He, however, was refused a refund, thus sparking the lawsuit (Shen 2021).

The industry's unnecessary usage of FRT is very apparent in this case. With a secure fingerprint system already in place, bringing in a far more information-sensitive system just for admission shows the redundancy in their actions. RecFaces, a facial recognition company based in Russia, states that fingerprint biometrics is the most accurate biometric recognition system with facial recognition following it. Also, while listing the cons of FRT, they mention the usage of highly sensitive data and privacy

matters, with the cons of using fingerprint sensors including hygiene and sensor disadvantages (RecFaces 2020). Companies such as RecFaces are not oblivious of the privacy infringements their products could have and with alternative tech such as fingerprint sensors available, it brings into question why such a massive push for facial recognition.

In an interview with Guo, he mentioned that he had a growing concern about the "rapid rollout of facial recognition cameras in venues across China over recent years, which had proceeded with little accompanying effort to regulate the industry (Ye 2021). Even with Guo's lawsuit, nothing of substance really changed from that viewpoint. The Court ended this case in favor of Guo, but not in the way that was expected. The decision with the full deletion of Guo's data and refund for the pass, however, failed to address any regulation of the industry's usage of FRT.

Top responses on Weibo to news report on the court's decision:

1. A very good precedent. We can say no to the costs of sacrificing privacy for the convenience high tech brings. **Liked 8,458 times**

2. Residential buildings require facial recognition for entering, it looks fancy, but who knows to whom the residential managing companies sold our data? **Liked 6,762 times**

3. Personal privacy and security are a big problem. Wherever we go, we have to provide our ID card information and phone numbers, and some places even require face scanning and fingerprint collection. How do those companies use and protect the data? We don't know. **Liked 2,447 times**

Figure 1 (Brown, 2021)

This lawsuit was also followed by stirs in social media along with other similar scenarios. A popular Chinese social media website, Weibo, showed massive support following Guo Bing's case verdict. Figure 1 shows the top comments in response to the verdict, with the top comments showing distrust with the private industry's usage of their data along with the several thousand that liked these comments. A place where people unveil what is on their minds, this shows us that there is much to talk about within the public on this topic of facial recognition and their privacy rights.

In 2020, Lao Dongyan, another law professor located in Beijing and a deep advocate for data privacy, fought her property management company for installing mandatory facial recognition to replace the already existing access card system. By leading her fellow residents with her knowledge of the law, she was able to continue

Top responses on Weibo to news reports on Lao's protest against the use of facial recognition in her residential community

1. This is a true expert! **Liked 282 times**

2. There are also those online fortune-tellers who can most easily collect faces and then compile them into big data. Only idiots would willing take a picture of their face and give it to others. **Liked 95 times**

3. This level of person is pretty real; she's able to push forward a lot of progress. **Liked 81 times**

Figure 2 (Brown, 2021)

using their access cards (Shen 2020). This is another attempt at the public pushing against the industry's decision to implement redundant uses of facial recognition similar to Guo's situation with the zoo. Figure 2 shows the top responses on Weibo as well about Professor Lao Dongyan's protest against uses of facial recognition technology in her residential community. Again, the public on social media are providing their support for these individuals pushing for privacy changes. According to Brown's article, Lao's actions not only made social media, but popular media outlets, providing more awareness to the public eye.

Though this seems like a victory at first glance, the company in Dongyan's residential area still installed facial recognition. This also won't hinder the rest of the residential companies to install facial recognition around the country. It is important to note that in both cases, highly educated individuals are leading the public to make micro-changes in the system. Cases such as these seem so limited due to the common citizens' lack of information in defending their rights legally. Guo continues in his interview by stating that this is why "public interest litigation is important. [They] can't pursue class-action lawsuits like in the United States, as [their] system doesn't allow it. So, [they] can only use the power of public institutions to restrict abuse of the technology" (Ye 2021). The safari zoo will still use facial recognition for entry to patrons and other less fortunate residential neighborhoods will still be forced to switch to facial recognition to access their homes. These small victories aren't meant to change the country alone, but to bring someone even more power into play. They gave the people of China a voice and sparked discussion on the topic of defending their rights to privacy.

In the end, however, the public's actions can't do much against the industry's intentions with FRT, causing conflict between these two actors.

The People and the Government

Facial recognition was under regulation by the Cybersecurity Law of the People's Republic of China and the Personal Information Security Specification (Lee 2021). With the Cybersecurity Law being a very broad framework to work with, facial recognition and other biometrics were not the central focus and were unable to stop the industry's infringements. The Personal Information Security Specification was an answer to the issue, but acted as more of a guideline on data handling and lacked any enforcement from the government. With such weak frameworks and lack of enforcement, the government had no leash on the industry allowing for the situation to escalate in a matter of years.

With the public's growing dissatisfaction with the industry's abuse of privacy, the power necessary to start to change all comes down to the Chinese government. Several high-profile cases including Guo and Dongyan along with growing security threats from third-party companies incited the Government to take action against FRT abuse; drafts for more robust privacy laws were set in play. There is this persuasive power the people of China have on the Chinese government as the government should be working for the best interest of the people and the country. Essentially, the citizens helped push the government to visualize safer and privacy focused ideals on how FRT should be used when compared to the existing intrusive standards initially set by the industry.

As of November 2021, new legislation addressing data usage and privacy had passed since Guo's lawsuit; the Personal Information Protection Law (PIPL) (FORUM 2021). To quickly summarize, the PIPL's main goal is to "protect the rights and interests of personal information, regulate personal information processing activities, and promote the rational use of personal information" with any violation resulting in a 7.7 million fine or 5% of the previous year's revenue (Bryant 2021). According to Yue Zhongming, the spokesperson for the Legislative Affairs Commission of China's legislature, PIPL will limit facial recognition to be only used in specified cases and when sufficiently necessary with a risk assessment conducted (Zheng 2020). On paper, this would be one of the first laws active that would finally penalize any party that would violate user data, beginning the crackdown on privacy abuse including FRT. The PIPL, though broad with its specifications, acts as a stepping stone in the regulation of the unfair use of facial recognition as the Government has finally brought a more accepting version of FRT usage with these new regulations.

The Government and the Industry

Following China's PIPL taking effect, the industry had no choice but to concede to the new regulations. This coercion from the government from the new laws finally turned the tides in favor of the people's privacy rights, however, the transition process isn't as smooth as envisioned. According to Paul McKenzie, a Morrison & Foerster partner based in Beijing and Shanghai, compliance to the PIPL could take months and enforcement would unlikely be aggressive for a while (Bryant 2021). Due to the fact that facial recognition had taken its roots deep within the infrastructure of many products and

services, along with the PIPL enacted in such a short time, many companies needed to scramble to meet the standards of the new law.

PIPL also puts restrictions on international companies as well. Such companies were able to transfer the people of China's data overseas without much resistance. Peggy Chow, a lawyer at Herbert Smith Freehills specializing in data protection and cybersecurity, states that the PIPL will require much stricter requirements including volume-based restrictions on personal data as well as a privacy impact assessment to take place before any data transfers (Swabey 2021). China is getting every aspect covered when it comes to the people's data as international companies have seen China as a large portion of their market as well. The PIPL law, however, gives guidance on compliance to international companies and paves an opportunity for them to "demonstrate their commitment to data protection" (Swabey 2021). In a way, China is going from one of the worst privacy-rated countries into one of the leading advocates of privacy protection around the globe.

Though it will take time, complying to the PIPL is necessary to make sure the product's standards will catch up to what was expected from the people. The main cause for this compliance is due to the industry's income being threatened, thus giving more incentive to implement such privacy guidelines from the bottom up. The government's prior lack of control with privacy and FRT and lack of preparation and foresight from the industry shows that regulations need to be in place as soon as possible from the introduction of such new technology.

Discussion of Stabilization

As facial recognition initially became popularized by the industry amongst the people of China, there seemed to be an initial understanding of how FRT fits within society. That idea would be to utilize facial recognition technology to provide convenience and security to the users. FRT, as an artifact, needs to have a consensus among the three actors on its main purpose in order to thrive as an ecosystem. The government themselves saw the benefits of facial recognition and utilized them in their own frameworks of security. This, however, soon falls apart due to the faults of both the industry and the government. The lack of risk and regulation from the government on facial recognition allowed for the industry to step out of line when dealing with its user's privacy and data security. Their conquest for profit outweighed many private companies straying away from the main artifact and the other two actors which would cause the ecosystem to dissolve the technological frames between them and the industry. With the main source of FRT losing sight of privacy and data security, it calls upon the citizens and government to help correct the industry's path.

The citizens of China are seen to have similar views on how the industry should use facial recognition in their products with the dissatisfaction from the users and the guidelines, though not enforced, the government encourages the industry to follow. This common interest along with the government working for the best interest of the people helps form the technological frame between these two actors. This allows the government to take appropriate action and apply their power with legislation upon the industry as they are hindering the citizens. Looking at this from the SCOT framework, this can be seen as where the alternative view the Industry had on the usage of FRT will

soon be wiped out and replaced fully with how the Government and people view proper FRT usage. The stage of closure is near with the PIPL taking place. With the start of the crackdown on data abuse including facial recognition, the industry begins to pull back its dubious operations and begin to adopt the original idea of the artifact once again.

Due to the sudden changes with the PIPL in November of 2021 and the lack of already built infrastructure in the industries, it will take some time before the actions of the industry can reflect upon the new changes Mckenzie, a Morrison & Foerster partner based in China, states that companies at the time were awaiting answers to their questions to clarify about compliance to the new law (Bryant, 2021). The willingness to cooperate with the government shows that the frames between the industry and the other two actors are more than likely going to build once again. This can be seen as a beginning stage of rhetorical closure from the SCOT framework as resolution can be seen with the compliance from the faulting actor, the industry, as they are forced to align their views to match the other two actors. Though there seems to be more work to be done, the ecosystem in China once again will eventually reach a consensus on how the industry's FRT should approach privacy, reaching stability amongst the actors.

Conclusion

FRT had come out of nowhere and grew so rapidly making a huge impact on the quality of life for the people of China. FRT became a goldmine opportunity for the industry in combination with the lack of action from the government allowing the industry to reap heavy profit. The citizens, a major stakeholder as users and casualties of the industry's products, had no real power to have an effect on the industry's decisions.

However, their actions did persuade the government to take action against the industry by finally setting up regulations. Such regulations finally put the government in power over the industry. With the new rules finally in effect, the government finally has a foot in the door to deal with any future industries that would infringe upon the citizen's privacy by branching from the existing frameworks they had recently set into play.

Looking back at the recent developments in regulations, it is certain that the concurring ideals of FRT usage from both government and the people had pushed the previously dominating FRT standards set by the industry to the past, paving a future for a more privacy centered utilization of FRT in China.

References:

Bryant, J. (2021, November 1). *China's PIPL takes effect, compliance 'A Challenge'*. China's PIPL takes effect, compliance 'a challenge'. Retrieved March 1, 2022, from https://iapp.org/news/a/chinas-pipl-takes-effect-compliance-a-challenge/

Brown, T. G., Statman, A., & Sui, C. (2021). Public Debate on Facial Recognition Technologies in China. In MIT Case Studies in Social and Ethical Responsibilities of Computing. PubPub. https://doi.org/10.21428/2c646de5.37712c5c

Feldstein, S. (2019, September 17). *The global expansion of AI Surveillance*. Carnegie Endowment for International Peace. Retrieved February 19, 2022, from https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

FORUM Staff. (2021, September 24). *China keeping citizens' data to itself with privacy law: Indo-Pacific Defense Forum*. Indo-Pacific Defense Forum |. Retrieved March 1, 2022, from https://ipdefenseforum.com/2021/09/china-keeping-citizens-data-to-itself-with-privacy-law/

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. Public Understanding of Science, 30(6), 671–690. https://doi.org/10.1177/09636625211001555

Lee, S. (2021, September 30). Coming into focus: China's facial recognition regulations. Coming into Focus: China's Facial Recognition Regulations | Center for Strategic and International Studies. Retrieved October 4, 2021, from https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations

Möllers, N., & Hälterlein, J. (2013). Privacy issues in public discourse: The case of “Smart” CCTV in Germany. *Innovation: The European Journal of Social Science Research*, *26*(1-2), 57–70. https://doi.org/10.1080/13511610.2013.723396

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the Sociology of Technology might benefit each other. *Social Studies of Science*, *14*(3), 399–441. https://doi.org/10.1177/030631284014003004

RecFaces. (2020, November 17). *Facial recognition vs. fingerprint recognition - what biometric is better*. RecFaces. Retrieved March 9, 2022, from https://recfaces.com/articles/facial-vs-fingerprints-biometrics

Shen, X. (2020, October 8). *China embraces facial recognition even as data leaks are rampant*. South China Morning Post. Retrieved February 28, 2022, from https://www.scmp.com/abacus/tech/article/3104512/facial-recognition-data-leaks-rampant-across-china-covid-19-pushes

Shen, X. (2021, April 13). *China's first facial recognition case raises more questions than it answers*. South China Morning Post. Retrieved February 28, 2022, from https://www.scmp.com/tech/policy/article/3129226/chinas-first-facial-recognition-lawsuit-comes-end-new-ruling-and-new

Swabey, P. (2021, August 26). *Here's what PIPL, "China's GDPR", means for global firms*. Tech Monitor. Retrieved March 9, 2022, from https://techmonitor.ai/policy/heres-what-pipl-china-gdpr-means-for-international-businesses

Ye, Y. (2021, April 26). *A professor, a zoo, and the future of facial recognition in China*. Sixth Tone. Retrieved March 2, 2022, from https://www.sixthtone.com/news/1007300/a-professor%2C-a-zoo%2C-and-the-future-of-facial-recognition-in-china

Zhang, L.-L., Xu, J., Jeong, D., Ekouka, T., & Kim, H.-K. (2021). The effects of facial recognition payment systems on intention to use in China. *Journal of Advanced Researches and Reports*, *1*(1), 33–40. https://doi.org/10.21742/jarr.2021.1.1.05

Zheng, S. (2020, December 21). *China's new Data Privacy Law 'will state how facial recognition can be used'*. South China Morning Post. Retrieved March 3, 2022, from https://www.scmp.com/news/china/politics/article/3114829/chinas-new-data-privacy-law-will-state-how-facial-recognition