Face-swiping: threat or opportunity?

A discourse analysis on the Chinese government's message to the people concerning facial recognition technology

DANIËL OP DEN BUYSCH – S1226770 – ASIAN STUDIES: POLITICS, SOCIETY & ECONOMY
D.OP.DEN.BUIJSCH@LEIDENUNIV.NL – 1ST JULY 2019

SUPERVISOR: DR. S. S. KHARCHENKOVA

Preface

Before you lies the thesis ‘Face-swiping: threat or opportunity?’ It has been written as a final requirement for my MA degree Asian Studies: Politics, Society and Economy. Before starting this journey, the wish to write on a subject concerning China and technological innovation was already clear to me. After discussing with my supervisor, Dr. Svetlana Kharchenkova, the topic of facial recognition technology sparked my interest, and it did not cease to do so after finishing.

I would very much like to express my gratitude for Dr. Kharchenkova, who has helped me in this process by being very understanding of my wishes and providing me with professional, critical and very helpful feedback. She has motivated and coached me to think and write academically. The writing of this thesis was a process that took more time of me than I had hoped for in the beginning, and Dr. Kharchenkova has never lost her patience, nor her will to guide me in finishing my largest project so far. Furthermore, I would like to thank my fiancé Youri Hagemann for his unceasing support and his drive to motivate me in making this last step in my university career at every moment. I have felt trusted in and supported until the very end. A big thank you also goes out to my mother Eefje Op den Buysch for discussing my work with me and providing me with fresh angles of research every time.

I hope you enjoy reading this thesis.

Daniël Op den Buysch

Contents

Chapter 1 - Introduction

In the ‘New Generation Artificial Intelligence Development Plan’, put in effect in 2017, the Chinese government lays out how artificial intelligence can help China forward. One of the subjects in this plan is the use of facial recognition technology to help safeguard the national security. The use of facial recognition technology in China is already quite advanced and Chinese people are becoming more and more familiar with the benefits of this piece of technology. However, the Chinese government so clearly chooses to further develop facial recognition technology in order to help improve the national security, it has also received criticism by some journalists for doing so (see e.g. Strittmatter, 2019; Doffman, 2018; Mitchell & Diamond, 2018; BBC, 2017; Gillespie, 2018; Lin & Chin, 2017). These journalists fear that the Chinese government is overstepping boundaries of the rights to privacy in order to gain a sense of national security. Mozur (2019) even brings to light the use of facial recognition technology to monitor and to crack down the Uyghur ethnic minority in Western China. ‘It is the first known example of a government intentionally using artificial intelligence for racial profiling, experts said.’ (Mozur, 2019). Taking into account the benefits but also these rough downfalls of facial recognition technology, the impetus of writing this thesis was to see what the Chinese government itself declares when talking about facial recognition technology; after having received this much criticism about the use of facial recognition technology, how do they respond? The main research question for this thesis will therefore be: what is the message that the Chinese government conveys to its people concerning facial recognition technology?

In answering this research question, this essay touches upon two concepts that are closely related, but that also conflict at times: privacy and security. The academic debate on the relationship between the two is already very extensive, so this essay will not try to add any knowledge to this information; it will only provide with an overview of this debate, as this is necessary in grasping the underlying problem of the research question (see chapter 2.1). Next, the topics of artificial intelligence and more specifically facial recognition will be discussed. These are also topics about which much academic debate already exists (see chapter 2.2). Although being a very contemporary subject at the time of writing this thesis, facial recognition technology has been discussed by scholars at length. As will also be clear from chapter 2.2.3, facial recognition technology is a topic that leads to much controversy, especially in the media. Even though this controversy exists, the Chinese government continues to apply this technology. The goal of this thesis and the addition it is to the existing debate, is to find out how the Chinese government conveys the message it is using this controversial piece of technology to its people. By analyzing the tone of voice and the other subjects of state media articles about facial recognition technology (see chapters 3 and 4), this thesis will try to add to the existing debate. Although also receiving international criticism (e.g. Ma, 2018; Marr, 2019; Vlaskamp, Persson & Obbema, 2015), and having close ties to surveillance as well, this thesis will not cover the debate on the Chinese social credit system (see for example Fan, Das, Kostyuk & Hussain (2018) for more information) for the sake of scope. There will also not be too much detailed technological explanation on facial recognition technology, as basic knowledge of what it can do suffices for the understanding of this thesis.

Chapter 2 - Theoretical Framework

This chapter will outline the existing academic debate on the different topics of this thesis. It is divided into two main parts: the first part gives a general and a China-specific overview on the topics of privacy and security; the second part will discuss the rise of problems between technological innovation on the one hand – more specifically artificial intelligence, and, as a part of this, facial recognition technology - and privacy issues on the other.

2.1) Privacy versus Security

With the development of technological innovations, some scholars are worried about what impact that will have on their privacy (e.g. Santanen, 2019; Kaplan, 2019; Gogus & Saygın, 2019). Santanen (2019) even states that 'new technologies represent the single greatest category of threat to the preservation of individual privacy'. As these technologies are more and more embedded in our lives and people start to need them to function properly, people also providing these technologies with more information about themselves. It seems that, in modern day society, everybody seems to agree that privacy is such an integral part of human beings that no one should never try to invade it. This is where a popular debate rises: what if people's individual security is compromised, is privacy protection then still paramount? To answer this question, this paragraph will first investigate the definitions of both concepts and look further into why there is a dichotomy between them. Then, this knowledge will be placed in a cultural context: does this popular agreement of the importance of privacy really apply universally? At last, the debate on privacy versus security will be discussed in the light of technological innovations and especially artificial intelligence.

2.1.1) Privacy

First, what is privacy exactly? The dictionary says that privacy is 'the freedom from unauthorized intrusion'.[1] In other words, the free possibility to keep information that you do not want others to know, to yourself. Parent (1983) defines privacy as 'the condition of not having undocumented personal knowledge about one possessed by others. A person's privacy is diminished exactly to the degree that other possess this kind of knowledge about him.' This means that as long as people do not have undocumented personal knowledge about you, you remain having privacy. The degree in which people do have this undocumented personal knowledge about you equals the degree to which

[1] Privacy (n.d.) In Merriam-Webster's collegiate dictionary. Retrieved from https://www.merriam-webster.com/dictionary/privacy

your privacy is diminished. By 'personal knowledge', Parent (1983) means the 'facts about a person which most individuals in a given society at a given time do not want widely known about themselves'. Both definitions of privacy include the unwanted possession of information that one would rather not share widely with others. I believe everyone would agree with the fact that all people have a right to privacy, which is why the Universal Declaration of Human Rights also includes this right to privacy (United Nations, 1948). Article 12 states: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.' This law protects human beings from their invasion of privacy by higher powers, such as governments for example. Thomson (1975) goes as far as to state that 'the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is'. What this rather critical viewpoint puts forward anyway is that the right to privacy and privacy is a multi-facetted debate. In this debate, there is however an underlying question that needs to be explored, which is simply looked over as every individual has an instinctive sense of the answer: why do people value privacy that much?

According to Bloustein (1964), the need for privacy has everything to do with human dignity. He explains that the person, who has no privacy left at all, of whom everybody knows everything, will start to merge with the masses, as his thoughts and feelings gradually become those of everyone. This person is not an individual anymore, and thus stripped of all his dignity. The merging of this person with the masses through the loss of privacy is not a sudden process; the more privacy one has, the more one is an individual in his thoughts and feelings, and vice versa. In the same line of thought, privacy also promotes freedom: if not everything is known about a person, thus them having some kind of privacy, this person will have some individuality which makes them free to be themselves. Fried (1970) states that 'privacy provides the rational context for a number of our most significant ends, such as love, trust and friendship, respect and self-respect. Privacy is a necessary element of those ends, [but] not the whole, [so] we have not felt inclined to attribute to privacy ultimate significance.' To put it shortly, people value privacy so much as it gives them a sense of freedom and individuality, and provides with a context for bases on which to fund relationships with others.

2.1.2) Security

Second, how does this notion of privacy then relate to security? Again, looking at the dictionary for a definition on security, it says: 'the quality or state of being secure', to which follows the definition of secure as: 'free from danger, free from risk of loss, affording safety'. The nature of this danger could be physical, in which case security would be the protection of people against physical harm such as violence, murder and rape. The nature of the risk of loss lies more in the fact that security entails the protection of your possessions from being stolen, damaged or otherwise compromised. According to Hobbes (1996), protection from each other is the sole reason for the emergence of states. Security is still today one of the most important tasks of a national government: they are in charge of the army, navy, air force, police but also cyber security for example. Not every country has armed forces (Costa Rica even abolished armed forces by constitution in times of peace) but the protection of its civilians even then is a major task of the government. People, like privacy, also require a sense of security for their quality of life. Also, like privacy, security enhances people's individual freedom: living with fear or anxiety of something bad happening to you or your goods being stolen from you, makes your mind preoccupied with these cases, instead of enjoying your life free of worries.

2.1.3) Conflict between privacy and security

Even though the two concepts of privacy and security both promote a sense of individual freedom, they at times also clash. The government or other institutions can sometimes require information from people, with or without their consent, in order to prevent a threat to security from happening. A basic example of this is airport security. People traveling by airplane are aware of their luggage being checked and scanned, and they cannot but consent to this, as traveling by airplane is otherwise not possible. Travelers are willing to give up their privacy of the contents of their bags to enhance security in the air. However, people do not always consent this easily to giving up privacy for the gains of security. The rise of technology, that processes this data (also known as information technology) has certainly sharpened this dichotomy. This chapter will later provide more information on this matter. Cyber security has definitely found its place next to national security as an important task of the government. Many governments are therefore granted by law to monitor and collect personal data from its citizens, in order to prevent any threats to the security from occurring, even when this means infringing upon one's right to privacy. As security is such a capital task for governments, they want to able to safeguard it at any cost. An example of where a government wanted to take its ability to infringe upon individuals' right to privacy, and where in the public eye the importance between privacy and security clashed, was the Dutch 'Wet inlichtingen en veiligheidsdiensten' [Law on Intelligence and Security Services] (abbr: Wiv). As Modderkolk (2016) describes, the Dutch parliament had made plans for this new law, that made it possible for the Dutch intelligence services to tap internet traffic from its citizens without having a direct lead to do so: not only those who were already being monitored by the Dutch intelligence services, but practically anybody's internet traffic could be monitored, in order for the government to be able to locate people who pose a threat to national security at a much faster rate. Modderkolk (2016) says that the Dutch parliament believed this law was necessary as 'cyberthreats and threats of terrorist attacks were not recognized soon enough'. Soon, a voice against this law came from Dutch citizens, as they feared their privacy was to be severely compromised by the law. Amnesty International, for one, writes[2] that the Wiv goes against human rights, as it would pose an unnecessary threat to privacy and freedom of speech. 'Data of those, who do not pose a threat to the national security, should not be collected and analyzed systematically and on a large scale', the website states. In light of this potential breach of privacy, a consultative referendum, established by Dutch citizens, was held questioning whether people were in favor or against this law. The majority of the Dutch people voted against the law, giving the Dutch government the message that it should not go forward with the law in that form. The public debate on the Wiv is an example on when security and privacy openly clash. The Dutch people chose in favor of their privacy in the referendum; the government still continued to establish the law, albeit in a different form, which was in the end less invading to the privacy of those who do not pose a threat to security. The protective task and the possibility of privacy invasion of citizens by the government in this case was very publicly disputed, which shows that privacy is a matter of fundamental rights to many.

2.1.4) Privacy in China

Following the Sapir-Whorf hypothesis that the language one speaks also shapes the way the speaker sees the world, the notion of 'privacy' shall be experienced the same in a single language community. As these language communities differ from each other, so differ the notions of privacy also. According to McDougall & Hanson (2002) state that it is 'quite commonly claimed […] that the Chinese language lacks an equivalent vocabulary for privacy and that therefore Chinese people do not have a sense of privacy'. He (1996) also states this, adding to the idea that the Chinese do not have a term for privacy that 'Westerners only base the definition of privacy on Western values.' According to He (1996), Westerners also believe that due to a historical disbalance between right and responsibility in China, personal responsibility for households and society gained more importance than rights, which meant that the Chinese had no rights, and therefore no privacy. Thirdly, He (1996) says that in 'Chinese culture, duty comes first, and rights come second. […] The second placement of rights over duty implies the denial of privacy.' Although the argument, that Chinese culture does not possess a notion of privacy, is extreme, as McDougall & Hanson (2002) also underline, privacy in China is a fairly new academic research topic. This part of the chapter will relate the previous knowledge about privacy to what the Chinese believe of this notion.

When looking in a dictionary, privacy is translated to Mandarin Chinese as *yinsi* [隐私][3]. The first character *yin* on its own means 'hide from view, conceal', whereas *si* means 'private, selfish'. According to Zarrow (2002), the modern Chinese notion of privacy can be traced back to late 19th century discussion on the relationship of *si* [私] 'private' in relation to the realm of *gong* [共] 'public, public space'. 'Promoting *si* at the expense of

[2] https://www.amnesty.nl/mensenrechten-in-nederland/veiligheid-en-mensenrechten/sleepwet
[3] https://www.youdao.com/w/eng/privacy/#keyfrom=dict2.index

gong had been condemned as selfish […]. The cultivation of personal morality beyond the élite and in the private sphere was for the first time promoted as the basis of public authority.' (Zarrow, 2002). Nearing the end of the imperial era in China in the late 19th, early 20th century, the relationship of the private life and the public life began to shift, making way for a sense of personal secrecy to be kept. The rise of communism, as a 'strong reinforcement of *gong*', caused for the *si* to become almost a 'survival technique', as opposed to the constant group thinking communism inclined. From the Cultural Revolution and the reforms of Deng Xiaoping onwards, the balance between *gong* and *si* shifted again, making 'privacy […] an ethics of trust in a disordered, anonymous and insecure economy […].' (Zarrow, 2002). The importance of privacy in China has therefore changed much in the past century.

He (1996) continues in the line of thinking that *si* and *gong* are related in the meaning of both words. As opposed to the definitions of privacy given earlier, He (1996) discerns two types of privacy: personal privacy and communal privacy. An important aspect of general privacy is the protection from outside 'intruders' into matters that people wish to keep to themselves. The difference that He (1996) makes from the beforementioned notice of privacy however is that this intrusion can not only happen to individuals, but also to whole groups of people. This is then what He would call the intrusion of communal privacy. Private affairs can also play within groups, and to maintain the privacy of this matters, the members of a group must work together to keep it that way. The distinction between in-groupers and out-groupers is the basics for ensuring this group privacy; to see who belong to 'your group' and who do not. According to He (1996), the importance of the sense of belonging to a group stems from the ancient Chinese core of society: the family. 'The place of the individual is submerged by the interests of the family'. (He, 1996). He himself says that he is critical towards the Western view that the Chinese do not have a notion of privacy: 'that our notions of privacy are not the same, does not mean we [the Chinese] do not have one. The Chinese not only have a notion of privacy, but also value it very much.' (He, 1996). And He is not the only one critical against this Western research into (Chinese) privacy. Lü (2012) describes that Western privacy issues are traditionally confined to the private, i.e. individual, domain. Nevertheless, with the emergence of the technological era, this notion of privacy does not apply solely to the private domain anymore: privacy in the public area has become a matter of more importance. Lü (2012) then critically continues to conclude that Western research on this new public domain privacy has been research by trying to forcefully fit the existing theories on private domain privacy into this new realm, creating all kinds of deficiencies. According to Lü (2012), because of the Chinese traditional awareness of this notion of public domain privacy, this should contribute to a better understanding of privacy as a whole. Nevertheless, as Western research has both theoretical and practical value, Chinese scholars should use this to form their own theories on privacy (Lü, 2012).

So, what is this public domain privacy exactly? According to Lü (2012), the development of information technology is closely related to the emergence of this public domain privacy. The collection and analysis of data, including personal information that not everybody wants to share, gives rise to privacy problems. As this data collection and analysis happens in the public domain (it is not in the hands of the individual anymore), Lü's thought is that the unwanted sharing of personal information is a great risk to the privacy of the society. Mi (2013) takes e-commerce as a lead to show risks in privacy: e-commerce involves among others bank payments, commercial advertising services, insurances, etc. These data are very personal, and if the data protection is not done properly enough, there is a substantial risk of private data leakage. Mi (2013) suggests that there are still improvements to be made in China on the field of private data protection. He proposes there should be better legislature about data protection, the establishment of a protection certification system, and that the e-commerce companies should improve their privacy policies.

This first part of the chapter has looked into some definitions, some similarities but also some differences between the concepts 'privacy' and 'security'. Both valued highly by many, individual privacy and protection from harm are important rights that people have. However, at times, they can also clash with one another. In the example of the Dutch Wiv, the clash was a result of the government wanting to give itself the power to infringe its citizens' privacy rights without them being an immediate threat to national security. The Dutch government in this case chose to enhance security at the cost of privacy of its citizens. As for China, there is a popular idea that, as the Chinese language does not contain a one-on-one translation of the English 'privacy', the Chinese do not have a notion of privacy at all. Chinese scholars like He (1996) and Lü (2012) are critical of this view, stating that the Chinese sense of privacy is just different, not non-existing. As traditionally, the Chinese attach more value to the community, they both discern private domain privacy and public domain privacy. The latter receives more and more attention in China due to the rise of information technology. The effect that this technology has on the balance between privacy and security, but also on the definition of the two, is significant. The information that people, before the emergence of internet, used to have for themselves, they know often share with their mobile phones, computers, etc. This new type of information sharing requires protection, as some of this information could be very private. The next chapter will discuss in more depth the relation between privacy and technological innovations, of which the emergence of artificial intelligence is the major point of interest.

2.2) Technological developments and privacy

When looking at the relation between technological advancement and privacy, as briefly mentioned in the previous part of this chapter, there is one development that has sparked unrest and critique for its danger to privacy: the rise of artificial intelligence. This part of the chapter will first outline what artificial intelligence exactly is, and secondly, what causes this kind of technology to be critiqued for its risk to privacy. Then, this knowledge will be assessed in a Chinese context: how does China deal with this artificial intelligence development? Lastly, this chapter will look at the application of facial recognition by the Chinese government, before moving on to the analysis on how the government conveys the message of this application to the public.

2.2.1) Artificial Intelligence

Artificial intelligence (abbr: AI) has quite remarkably never been defined with a single, universally adapted definition. Stone (2016) states strikingly that 'an accurate and sophisticated picture of AI – one that competes with its popular portrayal – is hampered by the difficulty of pinning down a precise definition of artificial intelligence.' It is therefore difficult to start this piece by explaining what artificial intelligence exactly is. There is however a broad shared idea that the science and business of artificial intelligence began with Alan Turing. Beavers (2013) states that 'Alan Turing [...] is often credited with being the father of computer science and the father of artificial intelligence', for Turing was the first to build an 'automated computing engine' in the 1950's, what later became the first computer. Turing was already breaking his head over the leading question in his computing theory study: 'Can machines think?' (Sharkey, 2012). This question contains assumption that 'thinking' is not something a machine or any inanimate object can naturally do. This stands in contradiction to the assumption that 'thinking' is something a human can do. Therefore, providing a machine with the ability to think, like humans do, would be in any case 'artificial', in that it is a man-made object intentionally given the ability to 'think'. But, when can a machine think? The answer to that could be the Turing Test. The idea of the Test is as follows: an interrogator asks questions to a person and a machine, although not being able to see them. If the interrogator, by studying the replies to the questions asked, cannot determine who is the person and who is the machine, the machine would be considered to be thinking (Sharkey, 2012). So, if a machine is considered to be able to think in a matter that is indiscernible from human way of thinking, one could also say this machine is as intelligent as a human. Artificial intelligence is, in other words, the pursuit, science and business of making machines able to perform human tasks – like thinking. However, thinking is not the only human task artificial intelligence should be able to perform when wanting to recreate human intelligence. Mehr (2017) says that AI should also possess 'the ability to understand and monitor visual/spatial and auditory information, reason and make predictions, interact with humans and machines, and continuously learn and improve'. The latter has become one of the major fields of artificial intelligence that received investment from outside the business. According to Shields (2018), machine learning applications received almost 60% of total investment from outside of the artificial intelligence industry in 2016, because of its potential to make the artificial intelligence industry grow exponentially. Although the learning and improvement ability of AI is very important, the two terms are not synonymous, Mehr (2017) continues. Machine learning, i.e. making a machine able to learn and become smarter by providing it with data, is what makes AI powerful and what really gives a machine the ability to think, but it is not all that artificial intelligence encompasses.

Within the field of AI, many subdivisions have been created; too many to list them all here. Some examples of artificial intelligence are self-driving cars, chess-computers, chat-bots such as SIRI, and facial recognition technology. These are examples of types of artificial intelligence that individuals nowadays could encounter on a nearly daily basis. But not only ordinary civilians make good use of the advantages that AI could give them, but also a wide range of institutions, such as governments, hospitals, commercial corporations but also smaller enterprises. As this thesis will mostly focus on the (Chinese) government's application of artificial intelligence, I will highlight the governmental aspect more than the other institutions mentioned before. One reason for governments to use machines and software that contain human-like thinking capabilities is to make its services more approachable to the citizens and to be able to manage it better, faster and at a larger scale. Through the analysis of large amounts of data by artificial intelligence, for which there is simply not enough manpower to do, AI can, help to reduce administrative paperwork and long waiting periods for example. However, the government uses AI for the largest part not in administrative work or in business that civilians have with governments, such as e.g. renewing licenses or filing for a parking permit. It does use it for the most part for national security, defense and intelligence. Shields (2018) states that 'AI may significantly improve military and intelligence capabilities, and analysts see its potential impact on military superiority as being on par with the development of airplanes and nuclear weaponry'.

2.2.2) Critique on artificial intelligence

According to Cockburn, Henderson & Stern (2018), the development of artificial intelligence will have profound implications for both the economy and society at large. It will impact the way products and services are produced, but also on employment rates and competition amongst producers. (Cockburn, Henderson & Stern, 2018). Verma (2018) adds to the implications on employment rates that, however it could free humans from repetitive and tedious acts, this replacement of human labor by artificial intelligence leads to unemployment. According to Verma (2018), this is a change to which humans will eventually adapt, albeit difficult at first. A third impactful change, but also reasonable fear, according to Solanas & Martínez-Ballesté (2009) that (the development of) artificial intelligence brings to society, is the risk of a breach of privacy. The discussion on the processing data versus individual privacy has been held for a long time now. As seen in 2.1.1, the right to privacy has even been included in the Universal Declaration of Human

Rights (United Nations, 1948). All the data that artificial intelligence machines need to function properly are stored, and some even try and learn or improve their services by using that data. These data would be harmless to one's privacy if they were stored anonymously. Schmid (2009) states that 'absolute' anonymity can only be ensured by publishing no data or outputs at all, although the utility of this data is maximized when there is no anonymization done at all. The dichotomy between these two factors is of such proportions that the one will always be severely harmed when the other is pursued, and vice versa. Solanas & Martínez-Ballesté (2009) add to this by saying that privacy is not really something commercial, as it is likely to heighten the production costs of a product or service, because of the extra safety measures that have to be taken.

One of the usages of artificial intelligence that has received the most widespread critique in light of this breach of privacy is surveillance. Collecting data from surveillance cameras is both very common and also never quite with everyone's consent, in the sense that people do not choose to be under surveillance when walking on the streets, for example. Now at first, video images from CCTV cameras are not really checked when there is no direct lead to do so – when a store has been robbed, the shop owner will most likely look at the video images to see what happened, but would not really care to look at it when all goes perfectly normal. What artificial intelligence changes about this, says Vincent (2018), is that it can analyze these video images without any humans necessary. The combination of artificial intelligence with surveillance suddenly means that all video image is being seen and analyzed. The data that is generated in this process is stored without direct consent from the person appearing on the video images, thus not being anonymized. It is with this knowledge that the application of artificial intelligence and therefore the collection of large heaps of non-anonymous data that this development receives so much critique.

2.2.3) Artificial intelligence and surveillance in China

When it comes to combining these surveillance cameras with artificial intelligence, there is one leading country in the world right now: China. According to the BBC (2017), China has been building 'the world's biggest camera surveillance network.' At the time of publishing, the BBC (2017) states that there were 170 million CCTV camera already actively in place and 'an estimated 400 million new ones will be installed in the next three years.' That means that, with a population of about 1,3 billion in 2019, there is currently close to one camera for every three citizens of China. In these recent three years, the Chinese government did not only install many CCTV cameras, but also equipped them with artificial intelligence. The majority of this artificial intelligent cameras use 'facial recognition technology' (abbr: FRT) to help identify the passing civilians. (Jacobs, 2018)

What is facial recognition technology exactly? Facial recognition technology uses the biometrics, i.e. the unique external features of an individual, of the face to determine one's identity, but also one's gender, age, current mood or even one's sexuality. These cameras transfer measurements of depth, width etc. of your face to data, that then get transferred to a giant database that collects all this information, from where an analysis can be made on who the scanned person is within a matter of seconds. The databases where all this data is being stored are essential for facial recognition to function properly. As this database grows, so will the ability of this software to identify human beings. Through machine learning, as mentioned before, this technology will grow stronger and stronger. Gillespie (2018) states that Dr. Dong Xu, chair in computer engineering at University of Sydney, says that 'the technology is even more reliable at identifying criminals – and presumably other people – than using fingerprints.'

The usage for this kind of technology is very broad. The scanning of one's face could for example replace using a key to enter a house, to get a car to start or as a security check and passport in one at an airport. There are many thinkable usages of facial recognition technology; although, as mentioned before, facial recognition technology is still mostly used for guarding safety and security. According to Gillespie (2019), the global FRT market is worth approximately US$3bn and is expected to grow to US$6bn by 2021, having China as world leader. The Chinese receives a great deal of help in FRT innovation from several Chinese tech giants like Alibaba, Tencent and Baidu. Lin & Chin (2017) state that in the process of building the 'biggest camera surveillance network', the cooperation of those tech giants plays a central role, as they are 'openly acting as the government's eyes and ears in cyberspace'. Whether or not these tech giants are voluntarily contributing to the surveillance of the Chinese people, or if the Chinese government is forcing them to in some degree, still remains questionable, according to Lin & Chin (2017). 'Tech giants have little choice but cooperate in a country where the Communist Party controls both the legal system and the right to function as a business', they state.

The control the Chinese government has over its people, whether through surveillance or social control, has long been a topic of discussion for scholars. Chen (2004) states that the community in China plays a larger and also more formal role in social control than in the West. As seen in 2.1.4, the Chinese society traditionally puts more emphasis on the community as a whole, and less so on the individual member of this community. The focus on the community instead of the individual causes for social pressure to be a useful way to govern the country. This, according to Chen (2004), on its turn sometimes causes the Chinese government to rule more informally (through the indirect use of social pressure) than formally. However, Chen (2004) notes that the Chinese are starting to realize the limitations of this control by the masses and is trying to form a social model that is more formally governed. One of these new developments in China's social control model is its cyber governance. Xi Jinping declared at the 2015 World Internet Conference that 'cyberspace, like the real world, is a place where we should advocate freedom, but also maintain order' (BBC, 2015). In the same conference, Xi also pleaded for 'cyber sovereignty': the right for each country to control their own cyber spheres. This internet governance can be divided into two forms, according to Broeders (2015): governance *of* the internet at first (i.e. network governance), and governance *using* the internet as second (i.e. especially information security). For Xi, the governance of the internet should be a right of each country, and other countries should not interfere with the way one choses to govern their own cyber sphere. This cyber sovereignty has as its advantage that governments can more easily shut off their own internet spheres from malicious influences from outside. The Arab Spring could be named as an example where internet, or more specifically here social media, can be put to use from the outside to cause a revolution on the inside. On the other hand, the Chinese government has also used this cyber sovereignty to provide domestic business the opportunity to grow more, without having to go against the competition from e.g. the United States. According to Shen (2016), the United States are expanding its own cyber sovereignty at the expense of others, trying to also gain cyber sovereignty in other countries; China on the other hand sees cyber sovereignty as a matter of domestic national security, and something to not be interfered with by other countries (Shen, 2016). This cyber sovereignty is a way of governing that is a very practical example of what He (1996) describes as communal privacy and the difference between in-groupers and out-groupers: out-groupers should not be able to gather in-groupers' private information. In following this line of thought, the cyber sovereignty policy of the Chinese government takes its people as the in-groupers who should be protected against the risk of intrusion of the right to privacy by the out-groupers, i.e. the non-Chinese.

The fact that national security is important for China, is as evident as it is for any country in the world. The areas in which the Chinese government wants to exert power however can at times be different than that from other countries. One major example is the surveillance state, and the ways in which the Chinese grants itself power to govern its own people. Following recent developments, facial recognition technology is a major development in this field. The China State Council published a plan on the development of next-generation artificial intelligence in 2017, describing in detail what the Chinese government is planning to do with artificial intelligence and how to achieve the Chinese goal of becoming a 'global technology superpower' (世界科技强国). A major point of interest for the Chinese government in achieving this goal is using artificial intelligence to ameliorate national security. The strategic plan of the China State Council (2017) states that 'we [the Chinese government] will include artificial intelligence in the National System Structure Strategy and we will make plans proactively. We will hold on firmly to the new stage in artificial intelligence development of the strategic initiatives of international competition. We will create new advantages over the competition and exploit the new area of development, which will be effective to safeguard the national security'. This quote shows that the role that national security plays in formulating this new strategy about artificial intelligence, is very distinct. It clearly states that having an advantage over international competition will be a way of protecting the national security. This again leads back to the cyber sovereignty discussed before. The Chinese government is promoting domestic technological development and trying to turn away from innovations created abroad. One of the means to enhance national security described in China State Council (2017) is also facial recognition technology. 'To facilitate the profound use of artificial intelligence in the domain of public safety, we will promote the establishment of a more intelligent monitoring, warning and controlling system for public safety. Concerning the comprehensive governance of society, new forms of criminal investigation, anti-terrorism regulations and other pressing matters, we will develop and integrate smart safety products that will also be used by the police, such as multiple kinds of sensor and detection technologies, recognition technologies that can analyze video images and biometric identification technologies, to establish a smart monitoring platform.' (China State Council, 2017). In this quote, the Chinese government is stating more clearly what it is planning on developing concerning facial recognition technology, although it does not call this technology directly by its name; 'biometric identification technologies' however comes down to the same kind of technology.

In summary, the second part of this chapter has discussed the meaning and development of artificial intelligence. The ability of machines to 'think' for themselves, makes their possible applications very broad. However, this development has also sparked unrest and critique, as worries arise about the risk of a breach of the right to privacy by this new technology. Surveillance, and especially the increased use of facial recognition technology, is a major topic of concern in this debate, as one simply cannot chose to be seen by surveillance cameras. Nonetheless, the Chinese government sees potential in the deployment of facial recognition technology, as it has the ability to substantially improve national security. As mentioned before, the use of artificial intelligence in the field of surveillance– in this case specifically facial recognition technology – has been criticized internationally. Despite this criticism, the Chinese government continues with this kind of surveillance. The media analysis, as described in the next chapters, will go deeper into how the Chinese government conveys the message of its use of facial recognition technology to its citizens.

Chapter 3 - Methodology

For this thesis, the main modus of research will be a so-called 'discourse analysis'. A discourse analysis is a research method used to profoundly analyze texts (or sometimes spoken material). The goal of using this research method for this thesis is to profoundly understand the message that the Chinese government puts forward on the topic of facial recognition technology through texts – in this case, news articles from state media outlet Xinhua News. The detailed explanation of my steps will follow later.

In itself, the term 'discourse' and its meaning have long been debated. Michael Foucault is seen by many, such as Willig & Stainton-Rogers (2008) as the founder of the idea that researching discourse is useful in academic research. Foucault believed that the 'world we live in is structured by knowledge' (Schneider, 2013-a). For Foucault, this meant that the way we see the world and think about everything in that world, is all structured by the knowledge people have about it and what people say about it. In this line of thought, discourse is the representation of this structure of knowledge on a topic, created by human communication and interaction. The representation of this structure of knowledge happens through communication: written texts, spoken texts and non-verbal communication are all examples of this communication. So, by analyzing for example written texts, as is done in this thesis, one can gain better understanding of the structure of knowledge behind it.

For this thesis, the main topic is facial recognition technology in China and the way the Chinese government discusses this topic. To draw conclusions on the discourse of this topic, the twenty most recent articles about facial recognition technology from the website of state-media publisher Xinhua News Agency, have been analyzed. The website of Xinhua News Agency was used as the source for the articles, as Xinhua News Agency is 'the national news publisher', according to their own website (Xinhua, 2019). Next to this, Xinhua News Agency was founded in 1931 by the Chinese Communist Party, then called 'Red Chinese News Agency'. Given this information, the close ties with the Chinese government are evident, thus providing reliable state-media news articles.

The articles in the corpus were found following the next steps. First, I have entered the search word '人脸识别' (*renlian shibie* "facial recognition [technology]") in the search engine of Xinhuanet.com. The articles that appeared were not all written by Xinhuanet journalists. The search engine works as a database for news articles, whether they were written by Xinhuanet journalists or not. I chose to order the articles from newest to oldest and selected the twenty most recent articles. The range of the publishing dates of the articles is from March 25th, 2019 to June 27th, 2019.

Moreover, I filtered the articles by the criterion that they had to contain the term 人脸识别 in the title. Some of the hits only contained film clips – I did not incorporate those. Also, for some articles, it was required to log-in into the system; for the sake of accessibility of the articles, I did also not incorporate these articles. Some of the articles appeared several times when searching for them; the reason for this was that they were published on several different websites, which made them appear several times in the database. I have only integrated them once in the corpus. The choice to analyze the twenty most recent articles was made to avoid any researcher bias, and to provide a broad overview of the different areas of interest the term 'facial recognition' is used in. For a full overview of the articles selected, see appendices 1-20. The corpus makes up a total of 18489 characters. The lines of the appendices have been numbered, to provide an easy way of reference. See 'Sources' for an overview of the articles used.

The next step in the discourse analysis is the coding of the material. According to Schneider (2013, b), coding 'means that you are assigning attributes to specific units of analysis, such as paragraphs, sentences, or individual words. I have chosen eleven attributes both before beginning my analysis as well as during the process. These attributes were selected based on discourse strands that are interesting to the topic and to finding an answer to the research question. The preliminary choice of these discourse strands was based on the theoretical framework, from which questions about privacy and safety already rose quite clearly. These attributes are 'safety', 'government', 'innovation', 'privacy/right to privacy' and 'warning/danger', 'trouble', 'positive attitude towards FRT' and 'negative attitude towards FRT'. Some of the articles (see chapters 2.2.2 and 2.2.3) were critical towards facial recognition technology and/or the Chinese system, which resulted in the choice of discourse strands as 'warning/danger' and 'trouble'. As mentioned, some of these attributes were only selected after the beginning of the analysis, because of their apparent relevance to the topic and the fact that these themes turned up so many times, that they could not be left out of the analysis. These attributes are 'quote (direct/indirect)', 'company/corporation/business' and 'reassurance/relief'. The attributes are also fully listed in the legend of the appendices. The attribution of these strands to the articles was done on the basis of relevance with the strand to the piece of text. This relevance at times is that the word of an attribute is literally in the text. However, in most cases, the words, clauses or sentences that were marked contained the topic of this particular attribute. For example, the attribute 'trouble' was given when the word 问题 *[wenti]* 'problem' was in the text, but also if the lines describe some sort of difficulty.

What follows are the actual conclusions that can be drawn from the described analysis. The conclusions from this analysis, in combination with the theoretical framework will pave the way towards answering the research question of this thesis.

Chapter 4 - Analysis

After providing the chosen texts with appropriate attributes, on the basis of the discourse strands they correlate with, this chapter will discuss the findings of the analysis. The examples that will be given to back up the conclusions all come from the chosen articles.

4.1) Safety

The fact that public safety is a major theme when discussing facial recognition technology, already became clear in the theoretical framework. Following Vincent(2018), the largest advantage that artificial intelligence has by using it in combination with surveillance cameras is that every second of video image can be analyzed, 24/7, instead of human eyes that will get tired very easily after watching video material for such a long time. Fulfilling such a task would simply ask to much of humans. This advantage however also comes with its major disadvantages, according to many: all the footage is being recorded and saved in databases, where these artificial intelligence machines are using them to learn and improve, posing serious threat to individual privacy. As mentioned before, one simply cannot choose to not be on video images of cameras out on the street for example.

The discussion of safety is also very much prevalent in my corpus. Of the twenty articles analyzed, I attributed the strand 'safety' in seventeen, attributing it a total of 95 times. The word 'safety' (安全 *anquan*) is mentioned a total of 29 times. In this process of attribution, I have marked words, phrases but also whole sentences. Lines 156 to 158 say that "[w]ith the rapid development of facial recognition technology comes the unceasing improvement of algorithmic accuracy, and also the increasing enhancement of safety. 'Face-swiping' is already gradually put into practice in domains like finance, public safety, border defense, aerospace, education, medicine, amongst others, whilst guaranteeing to safeguard everyone's privacy and letting everyone enjoy an even more convenient life." This is an example where safety is put forward as a domain that will greatly benefit from facial recognition technology. The journalist however does not specify how the safety will be enhanced; just that it will. Also, the writer of the article immediately adds to this that privacy will at all times be safeguarded. It seems as if the writer is aware of the problems that exist around facial recognition technology and want to reassure the reader right away that this problem actually is solved from the start. The point the writer actually wants to draw the reader's attention to is the fact that facial recognition technology is developing so rapidly and in so many domains, public safety being one of them.

As seen in China State Council (2017), explained in chapter 2.2.3, the Chinese government is keen on improving public safety. The overlapping topic of seven articles (appendices 3, 5, 10, 12, 14, 19 and 20) is how facial recognition technology can help the government in enhancing public security. One example from appendix 12 is that FRT helps in finding drunk drivers, stating in lines 444 to 447 very clearly that there have already been 7989 cases of drunk driving caught by the police, using facial recognition technology. Articles 14 and 19 both discuss the same use of facial recognition technology, i.e. airport security. As lines 706 to 710 state, facial recognition technology can not only help to secure air travel, but also to smoothen the traveling process for the benefit of the travelers. One could say that these seven articles provide practical examples of the Chinese government using FRT as planned: to enhance public security. By providing these examples, Xinhuanews as state-media expresses a certain progress in this development, and it shows how facial recognition technology can be useful in various fields. When looking at the tone with which these seven articles discuss the topic of safety, I would certainly argue that it is rather neutral. These articles provide with factual information like statistics more than emotional response to the developments. Also, none of these articles engage in the discussion between safety and privacy, as put forward in the theoretical framework. These seven articles provide with sec information on the development of facial recognition technology in various fields.

The beforementioned seven articles all discuss public safety. There is however also a case in the corpus in which the safety of facial recognition technology itself is being questioned. Lines 196 and 197 pose the next question: 'Some people are having doubts, because at first, if you want to pay by 'swiping your face', you need to fill in a password on your phone, but after you have done that once, you no longer need to fill in your password anymore. Is that safe?' This is an example of the writer actually acknowledging the fact that there are some popular doubts about the safety of facial recognition technology, and even posing one of these question in the article. After this sentence immediately follows a reassuring part of how the largest tech giants are dealing with this issue. What is striking about this example is the fact that the writer copies the questions possibly raised by the reader: a serious concern about safety. However, this question, seen from the quotation marks, is not being raised by the author himself. Thus, this example provides more with reassurance on the safety of facial recognition technology than on the doubts on this development.

Another striking element, when looking at the topic of safety throughout the corpus, is that the degree of safety, i.e. how many people are concerned in this safe keeping, differs very much. These degrees range from safety on school campuses (appendix 8) and the ability to find missing people faster by using FRT (appendices 2 and 16), to a special public toilet that dispenses less toilet paper (appendices 6 and 17). As far apart as these degrees of safety might be, there is one commonality in many of the articles in the corpus: fourteen out of twenty articles discuss local initiatives of using facial recognition technology for safe keeping, in contrary to discussing this development on a national scale. All of the articles highlight a special measurement a city or even neighborhood has taken to improve public security by using artificial intelligence. Of the twenty articles analyzed, eleven discuss also the contribution that private companies have made to the development of facial recognition. To take appendix 20 as an example: from lines 722 to 729, the article discusses that Damai.com has become the head sponsor of the Dalian Marathon. Damai.com has implemented facial recognition technology to ease the registration process and to be able to find frauds. This is an example of where a corporation has added to the safety and also the smoothness of the procedure of, in this case, the Dalian Marathon. The local initiatives in many cases appear to be made possible through the help of albeit large scale private companies. It is therefore not only the government who itself invests in the spreading of artificial intelligence and facial recognition technology, but companies also do it themselves. This topic will be discussed more in depth further on in this chapter.

4.2) Privacy

As seen in the theoretical framework, privacy is also a theme that is strongly linked to facial recognition technology. In the discussion on facial recognition technology and safety, the other side is privacy: what is the border between providing national security using FRT, and invading individuals' privacy and therefore breaching their human right (United Nations, 1948)? Critics are afraid that the storage of data received through video image analysis by artificial intelligence will mean a breach in people's privacy. As privacy is such an important topic, I also chose to attribute the discourse strand 'privacy' to text in the corpus. There are however only three articles (appendices 4, 15 and 16) that discuss privacy. I have attributed this discourse strand only ten times. As privacy is such a major concern in this topic, the small amount of privacy discussion in these articles is remarkable.

The article in appendix 4, for example, does mention privacy and also gives a critical note towards the issues with privacy in combination with facial recognition technology. The lines 243 to 250 express critique towards facial recognition technology, saying: "Does facial recognition contain the risk of leaking private information? Business representatives keep saying that the users' personal information from 'face-swiping' will not be recorded or stored. Operations expert from the company Cainiao Ming Yu says that through face-swiping, users do not need to preserve their personal information. Relevant information is protected at the highest standards in the Cloud. Not even site personnel can access this information, thus safeguarding everyone's privacy and security. However, similarly, there are scholars who posit that a person can change passwords, but he or she cannot change faces. This means that if he or she is the victim of a cyberattack, the facial recognition system can even cause more serious threats to the safety problem. Suelette Dreyfus, researcher in statistics, privacy and safety at the University of Melbourne states: 'Once the facial recognition system has been the victim of a cyberattack, users cannot possibly remove themselves from this system, which can lead to unprecedented safety issues’”. This lengthy quote clearly expresses critique to the development, after talking rather positively about facial recognition technology in lines 183 to 188 for example. However, the corporation officials reassure the reader that nothing can happen to people’s personal information, dr. Dreyfus explains what a threat cyberattacks can form to this kind of system. As mentioned before, the problems that are posed in the articles are immediately countered by providing with a solution to this problem. The excerpt from lines 243 to 250, however, is the only instance where the writer does not continue with a direct solution to the problem, as this is the last fragment of the whole article.

4.3) Cooperation between government and enterprises

As mentioned before, the articles in the corpus seem to address local initiatives much more than they address facial recognition on a national scale. In China State Council (2017), the Chinese government describes the way in which it wants to cooperate with enterprises to carry out the construction of artificial intelligence disciplines. The government, for example, wants to ‘guide the existing key national laboratories, key enterprise laboratories, national engineering laboratories and other bases that focus on AI, towards the forefront of AI research’. Now, the New Generation Artificial Intelligence Development Plan is a plan that encompasses the whole of artificial intelligence in China, but as seen from the corpus, facial recognition technology is also one of these fields for which the government wants to cooperate with enterprises and universities.

The discourse strand ‘company/corporation/business’ has been attributed 143 times, to lines of texts both discussing small scale and large-scale corporations. The strand ‘research’ has been attributed 39 times, discussing both research and research centers. Examples of large-scale corporations are Tencent (appendix 2, 4 and 16), Alibaba (appendix 16), Baidu (appendix 2 and 16), Cainiao (appendix 4), Damai.com (appendix 20) and Microsoft (appendix 15). Examples of research centers are the Chongqing Research Institute of Chinese Academy of Sciences (appendix 19), Shenzhen Institutes of Advanced Technology of Chinese Academy of Studies (appendix 4) and the University of Science and Technology of China (appendix 4). The two attributes of ‘company/corporation/business’ and ‘research’ are often encountered with the attribute ‘innovation’. As is also apparent from China State Council (2017), is that the Chinese government wants to cooperate them not only for the sake of production and manufacturing, but also for research and development in the field of artificial intelligence. ‘We shall encourage and guide domestic innovative talents and strengthen cooperation with the world’s top research institutions of artificial intelligence.’ (China State Council, 2017). The wish for more research and development for artificial intelligence also is clear from the articles in the corpus. In appendix 1, for example, the author says in line 57 that ‘the city of Beijing is guiding and promoting the innovative development of medical and technological enterprises in Beijing’. Another example from appendix 4 for focus on research and development is lines 194 and 195: 'the retail innovation of China's leading enterprises has entered a no man's land, and is going a way that no one else has gone before'. As seen in lines 103 to 106 (appendix 4) tech giant Tencent is even praised for its work for society, and the constant drive to innovate for the people. Lines 103 to 106 say: "As an internet technology company, Tencent over the years has devoted itself from beginning to end to its own capabilities and technological superiority, practicing the concept of science and technology for the good cause, and promoting social progress. In the domain of artificial intelligence, Tencent has always insisted on starting from the users' value and continuously resolving social difficulties through innovation of the scenarios in which to apply AI." The cooperation with these companies, as can be seen from these articles, appears to be very important for the government in the quest of applying facial recognition technology in Chinese society.

Just as mentioned before in the part on privacy, also the research and development as well as the cooperation with enterprises and research centers is focused on China. Except for appendix 15, an article about Microsoft, the rest all discuss China domestic enterprises and research centers. There is only one mentioning of competition with other countries or the international cooperation. This example can be found in the lines 232 to 234: 'China's face recognition technology is leading the world. In the latest global face recognition algorithm test results, released by the National Institute of Standards and Technology, three Chinese teams – Yitu Technology, Sensetime Technology and the Shenzhen Institute of Advanced Technology of the Chinese Academy of Sciences – took a spot in the top five'. The author very clearly sets out very clear the superiority in the field over other countries in the world. However, as this is the only instance of international competition and comparison, I would still argue a rather protectionist view over the Chinese facial recognition technology market. As seen in chapter 2.2.3, Xi pleaded for cyber sovereignty, and the right for each country to govern cyberspace in the way they wanted. This protectionist view can also be found in the corpus when talking about the cooperation between the Chinese government and enterprises and research centers in pursuit of innovation. Chinese companies like Tencent, as seen above, are even praised for their work for society and innovative talent. However, in the article in appendix 15 about Microsoft, the tone of appraisal is barely found. As explained in lines 514 to 517, the topic of this article is the news that 'Microsoft had decided to delete its largest public database of facial recognition information, MS Celeb'. Microsoft is reported to have done so for ethical reasons. Line 521 adds to this saying that Microsoft was 'worried that [the information in the database] might violate human privacy rights.' Line 535 also states that Microsoft has been 'vocal in its opposition to the technology as a form of government control'. However, in the same article in lines 529 to 531, the author makes the remark that 'facial recognition technology is certainly a marketable technology. First of all, it brings a lot of convenience. It is a major trend in the global consumer electronics market for customers to unlock their mobile phones and make electronic payments by "swiping their faces". The contrast between the factual statement of why Microsoft deletes its database on the one hand, yet the positive attitude towards facial recognition technology as a whole, is remarkable.

4.4) Tone of voice

In wanting to find the message that the Chinese government conveys to the people about facial recognition technology, it is important to discuss the tone of voice of the articles in the corpus. This attribution of discourse strands is different from the others mentioned above, as it does to a lesser degree deal with factual information, and of course more with emotions and feelings. This attribution is therefore also more prone to being subjective. I have attributed both the strand 'positive attitude towards FRT' and 'negative attitude towards FRT' according to what I believed were lines either positive or negative about facial recognition and the use of it. The choice of this attribution sometimes lies in the nature of certain words (e.g. the words 'convenient' and 'comfortable' in line 712: to make the process of traveling abroad much more convenient and comfortable) or more abstractly in between lines (e.g. line 619: facial recognition toilet paper dispensers have really opened people's eyes).

One of the first conclusions one can draw when looking at the tone of voice of the articles is the overall positive attitude towards facial recognition technology. The attribution of 'positive attitude' has been given to 81 phrases, yet the attribute 'negative attitude' has been given to only 6 phrases. The reasons for having a positive attitude towards facial recognition technology vary more than the reasons for being negative. One of the main instances when the positive attitude in the corpus in usually found, is when the author talks about the convenience of FRT in everyday life. In line 212 for example, when talking about payment using facial recognition, the author says: 'like facial recognition payment, 'face-swiping' is a way to prove that 'I am me', bringing convenience and efficiency'. Another example of convenience can be found in line 697, where the author discusses the speed in which people can pass airport security by using facial recognition technology: 'the average speed with which people pass customs before they go through security is already under six seconds'. A different case of positive attitude can be found when the authors talk about the functionality of the system. To take lines 217 and 218, in which the author discusses the matching between one's face in the airport security with their check-in luggage, as an example: 'in previous trials, Cainiao's 'Smart Cabinet' has generated over a million face-swiping records. So far, there has been no case of mistaken identity leading to the wrong collection of bags'. Another example of the praising of the functionality of facial recognition technology is the lines 345 to 348: 'when a 3D-sensor camera is used for facial recognition, the built-in dot matrix projector can project more than 30.000 infrared points, invisible to the naked eye, to the user's face, providing richer data in terms of color, texture and depth, higher security and accuracy and faster recognition'.

When looking at the negative attitude towards facial recognition technology, there is evidently less diversity to be seen. The amount of attributions is the main reasons for this. The first example of negative attitude towards FRT is found in the lines 246 to 250, and has been discussed before in the paragraph on privacy, so I will not go into more detail. The lines 510, 521 and 534 provide other examples of negative attitude towards facial recognition. These lines occur also in the article in appendix 15, on Microsoft. As said before, the article discusses the deletion of a facial recognition database by Microsoft because of fear of privacy breach. Line 534 says: ‘it should also be noted that facial recognition technology has the potential to break through these areas [such as the hunt down of fugitives, conduct rapid security checks (see line 532)], and violate civil rights’. This line very clearly states the negative issue with facial recognition technology as also described in chapter 2.2.2. Besides these examples, none of the issues as raised in chapter 2.2.2 are described in the entire corpus.

4.5) Conclusions

This chapter has looked at four different topics that have stood out after the performance of the discourse analysis. The overall focus of the articles in the corpus appears to be safety: there is a clear intent to provide the reader with knowledge on how facial recognition technology can be put to use to improve public security on various degrees. Furthermore, the articles in the corpus are predominantly enthusiastic and positive about the development of facial recognition technology. The convenience it brings to the citizens, as well as the widespread usages of FRT are being described in a positive matter. Also, there is a focus on the cooperation between the Chinese government and Chinese enterprises and research centers that cannot be overlooked. Several articles discuss local innovative initiatives by enterprises and research centers in the development of facial recognition technology. The issues with facial recognition technology, as raised in chapter 2.2.2. of the theoretical framework, are much less prevalent in the corpus. The discussion about privacy is hardly mentioned, nor are the authors speaking negatively about the development of FRT.

Chapter 5 - Conclusion

China has set the goal to becoming a 'global technology superpower'. In order to achieve that goal, the Chinese government describes in its 'New Generation Artificial Intelligence Development Plan' how the research and development of artificial intelligence will be crucial and important to help the whole country forward. But there is also a great downside to the development. Because these 'smart' machines are gathering, storing and analyzing data, critics fear that individuals' privacy could be compromised. One of the most critiqued applications of artificial intelligence is facial recognition technology. By scanning a person's face and measuring his or her biometric features, the system can identify a person within milliseconds. China is in the process of building the largest CCTV surveillance network in the world, installing roughly one camera per three citizens.

China has been critiqued by scholars for their use of facial recognition technology, as it would harm people's privacy. However, no academic research had yet been done on how the Chinese government itself tells the people about how and why it uses facial recognition technology. To answer the question "What is the message that the Chinese government conveys to its people concerning facial recognition technology?", I have conducted a discourse analysis. Through the analysis of texts, and the inclusion of the context in which the texts were written, one can draw conclusions on how these texts relate to the existing debate on a topic, which for this piece is the use of facial recognition technology in China. The texts in the corpus are news articles from state-media outlet Xinhua News, all containing the word '人脸识别' (facial recognition) in its title.

I found that there are two main topics surrounding the Chinese government's message on the use of facial recognition technology: safety and cooperation with enterprises and research centers. The articles in the corpus provide with plenty examples of how facial recognition can benefit public safety, such as the identification of drunk drivers and the improvement in airport security. The government has made it clear in its New Generation Artificial Intelligence Development Plan that it seeks to cooperate with enterprises and research centers in order to improve the artificial intelligence as a whole, and facial recognition technology specifically. This cooperation also was prevalent in the corpus. Two of the major striking conclusions from this was that the authors predominantly discuss local-scale initiatives, that were initiated by Chinese-domestic enterprises. The mentioning of competition with international companies is only mentioned once in the whole corpus. The importance of domestic development of facial recognition technology is a crucial factor in the message the Chinese government wants to convey.

The critique towards facial recognition technology as mentioned above is quite remarkably not to be seen as an important subject in the corpus. Any issues that facial recognition technology could cause in terms of breach of privacy are mostly not even discussed, and if they are, they are negated quickly. There is but one example where the author raises a critical viewpoint of facial recognition technology without adding a negation of the argument. The continuous positivity about facial recognition technology stands in contrast to the critiques that the Chinese government has received, as discussed in the introduction. To finally answer the research question: 'what is the message that the Chinese government conveys to its people concerning facial recognition technology?' The Chinese government wants to convey a positive message about the development and use of facial recognition technology and wants to advocate for the domestic cooperation between the government and enterprises and research centers to further develop facial recognition technology.

Chapter 6 - Discussion

As seen in chapter 2.1.4, according to He (1996), the Chinese value privacy very much. The small-scale discussion on the topic of privacy therefore surprised me. It is however very difficult to pinpoint the reason of the size of the privacy discussion, as the real intentions of the Chinese government are hard, if not impossible to research. The articles in the corpus are only a handful of all the articles on Xinhuanews containing the search word '人脸识别' (facial recognition technology) in its title. The analysis of even more articles could shed more light and provide with more examples on how facial recognition technology is being put to use. For the sake of scope, this thesis deliberately did not discuss the social credit system and the implications the development of facial recognition technology has on this phenomenon. As this system has been internationally critiqued, further research could incorporate this system to see what facial recognition technology adds to the functions of this system.

Chapter 7 - Sources

7.1) Bibliography

BBC (2017, December 10). *In Your Face: China's all-seeing state.* Retrieved from: https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state

BBC (2015, December 16). *世界互联网大会： 习近平吁尊重"网络主权".* Retrieved from: https://www.bbc.com/zhongwen/simp/world/2015/12/151216_world_internet_conference

Beavers, A. (2012). Alan Turing: Mathematical Mechanist. In Cooper, S. B., & Leeuwen, J. van. (Eds.) Alan Turing: His Work and Impact. (pp. 481-485). Waltham, MA: Elsevier Science.

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: an answer to Dean Prosser. *New York University Law Review*, 39(6), 962-1007.

Broeders, D. (2015, April). *The Public Core of the Internet: An International Agenda for Internet Governance.* The Hague: WRR-Policy Brief No. 2, The Netherlands Scientific Council for Government Policy (WRR).

Candela, J. Q. (2017, December 19). *Managing Your Identity on Facebook With Face Recognition Technology.* The Facebook Newsroom. Retrieved from: https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/

Chen, X. (2004). Social and Legal Control in China: A Comparative Perspective. *International Journal of Offender Therapy and Comparative Criminology, 48*(5), pp. 523-536.

China State Council (2017, July 8). *新一代人工智能发展规划的通知 [Report on the New Generation Artificial Intelligence Development Plan].* China State Council.

Cockburn, I., Henderson, R. & Stern, S. (2018, March). *The Impact of Artificial Intelligence on Innovation.* NBER Working Paper Series. National Bureau of Economic Research: Cambridge, Massachusetts.

Doffman, Z. (2018, October 28). *Why We Should Fear China's Emerging High-Tech Surveillance State.* Forbes. Retrieved from: https://www.forbes.com/sites/zakdoffman/2018/10/28/why-we-should-fear-chinas-emerging-high-tech-surveillance-state/#1f08a7ed4c36

Fan, L., Das, V., Kostyuk, N., & Hussain, M. (2018). Constructing a Data‐Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy and Internet, 10*(4), pp. 415-453.

Fried, C. (1970). *An Anatomy of Values: Problems of Personal and Social Choice*. Harvard University Press: Cambridge, Massachusetts.

Gillespie, E. (2019, February 24). *Are you being scanned? How facial recognition technology follows you, even as you shop.* Retrieved from: https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop

Gogus, A. & Saygın, Y. (2019, May). Privacy perception and information technology utilization of high school students. *Heliyon, 5*(5).

He, D. (1996, November). 简论中国人的隐私 [Simple statement on privacy of Chinese people]. *深圳大学学报（人文社会科学版）[Journal of Shenzhen University (Humanities and Social Sciences), 13*(4), pp. 82-89.

Hobbes, T. (1996). *Leviathan.* Edited by J. C. A. Gaskin. Oxford University Press: Oxford.

Jacobs, H. (2018, July 15). *China's 'Big Brother' surveillance technology isn't nearly as all-seeing as the government wants you to think.* Business Insider. Retrieved from: https://www.businessinsider.nl/china-facial-recognition-limitations-2018-7/?international=true&r=US

Kaplan, A. (2019, January). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons, 62*(1), pp. 15-25.

Lin, L. & Chin, J. (2017, December 1). *China's Tech Giants Have a Side Job: Helping Beijing Spy --- Alibaba and its peers assist authorities in policing crime, silencing dissent.* The Wall Street Journal. Retrieved from: https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284

Lü, Y. (2012, January). 当代西方对公共领域隐私问题的研究及其启示 [Contemporary Western research on privacy issues in the public domain and the lessons to learn from it]. *上海师范大学学报（哲学社会科学班）[Journal of Shanghai Normal University (Philosophy & Social Sciences Edition), 41*(1), pp. 5-17.

Ma, A. (2018, October 30). *China social credit system, punishments and rewards explained.* Business Insider. Retrieved from: https://www.businessinsider.nl/china-social-credit-system-punishments-and-rewards-explained-2018-4/?international=true&r=US

Marr, B. (2019, January 21). *Chinese Social Credit Score: Utopian Big Data Bliss or Black Mirror on Steroids?* Forbes. Retrieved from: https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#1ec5afdf48b8

McDougall, B. S. & Hansson, A. (2002). *Chinese Concepts of Privacy*. Leiden: Brill.

Mehr, H. (2017, August). Artificial Intelligence for Citizen Services and Government. Retrieved from: https://ash.harvard.edu/files/ash/files/artificial_intelligence_for_citizen_services.pdf

Mi, T. (2013, July). 中国电子商务领域隐私数据保护研究 [Research on the protection of data privacy in the domain of Chinese e-commerce]. *北京邮电大学学术交流 [Beijing University of Posts and Telecommunications Academic Exchange], 232*(7), pp. 38-41.

Mitchell, A. & Diamond, L. (2018, February 2). *China's Surveillance State Should Scare Everyone.* The Atlantic. Retrieved from: https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/

Modderkolk, H. (2016, April 29). *Kabinet houdt vast aan massaal aftappen internetverkeer.* De Volkskrant. Retrieved from: https://www.volkskrant.nl/wetenschap/kabinet-houdt-vast-aan-massaal-aftappen-internetverkeer~b3d85383/

Mozur, P. (2019, April 14). *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority.* The New York Times. Retrieved from: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Parent, W. (1983). Privacy, Morality and the Law. *Philosophy and Public Affairs, (12)*4, pp. 269-288.

Santanen, E. (2019, January). The value of protecting privacy. *Business Horizons, 62*(1), pp. 5-14.

Schmid, M. (2009). Data Mining in Large Databases — Strategies for Managing the Trade-Off Between Societal Benefit and Individual Privacy. In Solanas, A. & Martínez-Ballesté, A. (Eds.). *Advances in Artificial Intelligence for Privacy Protection and Security*. Singapore: World Scientific Publishing Co Pte Ltd.

Schneider, F. (2013-a, May 6). Getting the Hang of Discourse Theory. Retrieved from: http://www.politicseastasia.com/studying/getting-the-hang-of-discourse-theory/

Schneider, F. (2013-b, May 13) How to do a Discourse Analysis. Retrieved from: http://www.politicseastasia.com/studying/how-to-do-a-discourse-analysis/

Sharkey, N. (2012, June 21). Alan Turing: The experiment that shaped artificial intelligence. Retrieved from: https://www.bbc.com/news/technology-18475646

Shen, Y. (2016). China and global internet governance: Toward an alternative analytical framework. *Chinese Journal of Communication, 9*(3), pp. 304-324.

Shields, J. (2018). Smart machines and smarter policy: foreign investment regulation, national security, and technology transfer in the age of artificial intelligence. *John Marshall Law Review, 51*(2), pp. 279-307.

Solanas, A. & Martínez-Ballesté, A. (2009, August 3). *Advances in Artificial Intelligence for Privacy Protection and Security*. Singapore: World Scientific Publishing Co Pte Ltd.

Stone, P. (2016, September). *Artificial Intelligence and Life in 2030 – One Hundred Year Study on Artificial Intelligence.* Retrieved from: https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai_100_report_0831fnl.pdf

Strittmatter, K. (2019, May 26). *Big Brother is watching: inside China, the ultimate surveillance state.* The Times. Retrieved from: https://www.thetimes.co.uk/article/big-brother-is-watching-inside-china-the-ultimate-surveillance-state-l6cfd7f8r

Thomson, J. (1975). The Right to Privacy. *Philosophy & Public Affairs, 4*(4), pp. 295-314.

United Nations (1948, December 10). *Universal Declaration of Human Rights.* Retrieved from: https://www.un.org/en/universal-declaration-human-rights/

Verma, P. (2018, September). The natural impact of artificial intelligence. *International Journal of Critical Infrastructure Protection, 22*, pp. 150-151.

Vincent, J. (2018, January 23). *Artificial Intelligence Is Going to Supercharge Surveillance.* Retrieved from: https://www.theverge.com/2018/1/23/16907238/artificial-intelligence-surveillance-cameras-security

Vlaskamp, M., Persson, M. & Obbema, F. (2015, April 25). *China kent elke burger score toe – ook voor internetgedrag.* De Volkskrant. Retrieved from: https://www.volkskrant.nl/nieuws-achtergrond/china-kent-elke-burger-score-toe-ook-voor-internetgedrag~bd93ed29/

Willig, C. & Stainton-Rogers, W. (2008). *The SAGE Handbook of Qualitative Research in Psychology*. London: SAGE Publications.

Xinhua (2019). 新华社简介. Retrieved from:
http://203.192.6.89/xhs/static/e11272/11272.htm

7.2) Corpus

1. Du, Y. (2019, May 6). *北京重拳打击骗取医保待遇 探索引入人脸识别技术就医 [Beijing to crack down on medical insurance fraud; exploring how to use facial recognition technology in seeing a doctor].* Retrieved from: http://www.xinhuanet.com/city/2019-05/06/c_1210127125.htm
2. [Writer unknown] (2019, May 4). *腾讯优图突破“跨年龄人脸识别”，助力警方寻回被拐十年儿童 [Tencent break through ‘facial recognition across the years’ , helps police find lost child after ten years].* Retrieved from: http://www.xinhuanet.com/tech/2019-05/04/c_1124447988.htm
3. Wang, J. (2019, April 28). *南昌：’AI’ 人脸识别锁定‘毒驾、失驾’ 群体 [Nanchang: ‘ AI ’ facial recognition technology identifies “drunk drivers”.* Retrieved from: http://www.jx.xinhuanet.com/2019-04/28/c_1124425994.htm
4. Chen, J. (2019, April 16) *人脸识别技术正广泛用于线下支付取快递等 [Facial recognition technology is being used to speed up offline payment.* Retrieved from: http://www.xinhuanet.com/2019-04/16/c_1124373216.htm
5. Liang, Z. (2019, April 16). *海南省旅馆旅租场所实现人脸识别全覆盖 [Hainan province hotels and rental places to achieve full coverage of facial recognition].*

Retrieved from: http://www.hq.xinhuanet.com/news/2019-04/16/c_1124371442.htm

6. Wang, J. (2019, April 13). *如厕还能体验人脸识别。景德镇‘厕所革命’有特色 [Facial recognition is even used in going to the bathroom. Jingdezhen's 'toilet revolution' is special.* Retrieved from: http://www.jx.xinhuanet.com/2019-04/13/c_1124361405.htm
7. He, H. (2019, April 2). *合肥推行公租房人脸识别系统 [Hefei uses a facial recognition technology system for renting houses].* Retrieved from: http://www.ah.xinhuanet.com/2019-04/02/c_1124316264.htm
8. Chang, N. (2019, April 1). *'智慧校园人脸识别'系统助力中央文化和旅游管理干部学院校园管理 ['Smart campus facial recognition' system helps campus management of Central Cadre College of Culture and Tourism Management].* Retrieved from: http://m.xinhuanet.com/culture/2019-04/01/c_1124309716.htm
9. Cao, X. (2019, March 30). *3D传感摄像头人脸识别率99.9% [3D Sensitive camera has a facial recognition rate of 99.9%].* Retrieved from: http://m.xinhuanet.com/culture/2019-04/01/c_1124309716.htm
10. Yang, B. (2019, March 25). *人脸识别'签到'即可'巡河' ['Patrolling the river' by 'checking-in' using facial recognition].* Retrieved from: http://www.xinhuanet.com/tech/2019-03/25/c_1124276192.htm
11. Hui, G. (2019, June 20). *'人脸识别'助93人成功寻亲 [Facial recognition has helped 93 people successfully find their relatives].* Retrieved from: http://wx.xinhuanet.com/2019-06/20/c_1124647710.htm
12. Jia, Y. (2019, June 27). *半年查了8000个济南查酒驾用上大数据、人脸识别 [In half a year, 8000 drunk drivers have been caught in Jinan using big data and facial recognition].* Retrieved from: http://www.sd.xinhuanet.com/sd/jn/2019-06/27/c_1124679770.htm
13. Huang, J. (2019, June 18). *天津市中研附院推出'人脸识别'预约挂号系统 [Tianjin City China Research Centre is using 'facial recognition' for an appointment making, hospital registering system].* Retrieved from: http://m.xinhuanet.com/tj/2019-06/18/c_1124639297.htm
14. Dong, Y. (2019, June 14). *新机场安检引入人脸识别技术 [New airport safety check uses facial recognition technology].* Retrieved from: http://m.xinhuanet.com/bj/2019-06/14/c_1124622241.htm
15. Liu, Y. (2019, June 12). *微软删除人脸识别数据库，源于'伦理'识别 [Microsoft deletes facial recognition database, reason is 'ethics'].* Retrieved from: http://m.xinhuanet.com/tech/2019-06/12/c_1124609721.htm
16. Ye, Q. (2019, June 10). *人脸识别让寻亲不再是大海捞针 [Facial recognition stops finding relatives from being the search for a needle in a haystack].* Retrieved from: http://m.xinhuanet.com/gd/2019-06/10/c_1124601825.htm

17. Shi, X. (2019, May 27). *人脸识别供纸机不只是解了公厕的围 [Facial recognition public paper dispenser is not only in the room of the toilet anymore].* Retrieved from: http://wx.xinhuanet.com/2019-05/27/c_1124546042.htm
18. Nie, C. (2019, May 25). *郑州市所有出租车将安装人脸识别系统 [All taxis in Zhengzhou City will install facial recognition system].* Retrieved from: http://m.xinhuanet.com/ha/2019-05/25/c_1124539877.htm
19. Jing, Z. (2019, May 21). *中科院重庆研究院牵头研发的‘机场安检智能识别系统’实现全流程人脸识别 [The ‘airport security smart identification system’ led by Chongqing Research Institute of Chinese Academy of Sciences realizes the whole process with facial recognition technology].* Retrieved from: http://www.cq.xinhuanet.com/2019-05/21/c_1124522782.htm
20. Liu, S. (2019, May 12). *人脸识别黑科技为大连国际马拉松赛保驾护航 [Black technology facial recognition is Dalian Marathon’s escort].* Retrieved from: http://www.ln.xinhuanet.com/2019-05/12/c_1124484102.ht

Chapter 8 - Appendices

Legend

安全 (safety)

政府 (government)

创新 (innovation)

隐私权 (privacy/right to privacy)

警报/危险 (warning/danger)

人脸识别科技 (facial recognition technology)

研究 (research)

问题 (trouble)

引用 (quote (direct/indirect))

公司 (company/corporation/business)

释怀 (reassurance/relief)

Appendix 1

北京重拳打击骗取医保待遇 探索引入人脸识别技术就医

2019-05-06 15:53:57

一张医保卡多人使用、套取药品倒买倒卖……北京欺诈骗取医疗保障基金的手段不断提升，呈现出方式多样、隐蔽性强、团伙作案，甚至通过高科技手段骗保等趋势。北京将探索建立“黑名单”制度联合惩戒，并探索将人脸识别技术等应用于门诊、住院等环节，解决骗保问题。

这是北京市医疗保障局局长于鲁明在 6 日召开的北京市医疗保障工作会议上透露的。

于鲁明表示，北京医保基金监管面临的问题复杂、严峻，一方面是由于较长时间以来，北京市各级各类医疗机构执行的是以药和耗材补医等运行机制，使得过度医疗、过度使用药品耗材具有普遍性。另一方面，一些医疗机构在逐利机制驱使下，引导患者过度就医造成医疗费用快速成倍增长，像一些社区一级医疗机构年医疗费用，最高的竟达到近亿元。

北京的医疗机构吸引了大量外埠患者。于鲁明指出，一些不法公司为外埠患大病的病人虚构劳动关系，骗取北京市医保待遇。还有的医疗机构利用单病种人头按天收费政策，在本来仅审批 100 张床位的医院，不择手段挤下近 300 位病人，严重损害参保人的权益和基金安全。

“对这些现象和问题，必须保持高度警惕，敢于担当、敢于出手、敢于亮剑。”于鲁明强调，北京将在基金安全监管上下功夫，提高医保管理智能化、信息化和精细化水平。

他表示，北京将持续打击欺诈骗保，通过“发现一批、查处一批、公布一批、防范一批、教育一批、移送一批”，全面加大对欺诈骗保行为的震慑力度。对所有定点医药机构实现督查全覆盖，针对薄弱环节，确定 1 至 2 项专项治理重点，限期整改到位，并引导参保人员切实认识到医保基金是自己的救命钱，共同维护医保基金安全可持续运行。

他称，北京还将推进医保诚信评价体系建设，健全信息披露制度，对定点医药机构进行综合评价和排名，建立按比例末位退出机制。探索建立“黑名单”制度，发挥联合惩戒威慑力。加强与卫生健康、公安等部门的联动配合，建立基金监管协调常态化工作机制，构建“一案多查”、“一案多处”制度，推动基金监管无缝衔接、闭环管理。

于鲁明强调，北京将依托科技力量，建设智慧医保。探索将人脸识别技术、就诊信息互联互通、住院登记时间采集比对、医疗机构药品和耗材购销存信息同步采集、医保缴费信息与纳税信息协查比对等机制，应用于门诊、住院和后台监控等环节，解决一卡多用、挂床住院、替换药品、虚报费用、虚假用工等骗保问题。

与此同时，北京将加强数据标准化建设，推进中药饮片标准化、门诊诊断标准化和药品说明书电子化，优化药品监测平台，精准分析药品支出异动，追踪存在过度医疗行为的定点医疗机构和医师，及时干预提醒；强化医疗机构医保费用增长趋势分析监测，准确把握医疗机构价值取向特点，对增速排名前 50 位的医疗机构，尤其是民营医疗机构，进行精准监管；充分挖掘运用医保大数据，探寻医疗市场服务需求供给洼地，引导促进北京医疗和科技企业创新发展。(记者 杜燕)

Appendix 2

腾讯优图突破“跨年龄人脸识别”，助力警方寻回被拐十年儿童

2019-05-04 10:32:51 来源： 新华网

被拐十年的“小耗子”（化名），终于找到了。

十年间，父母和警方从未放弃过寻找。“小耗子”被拐时才 3 岁，十年中孩子成长过程中容貌变化巨大，寻找孩子的难度与日俱增！与千千万万被拐儿童的父母一样，“小耗子”的父亲桂宏正除了靠着“一张嘴两条腿”走遍全国各地不断寻找之外，几乎没有任何办法能够找回自己的孩子；这起案件也成为了所有参与办案的民警的心结，任何相关消息都牵动着孩子亲生父母的心弦。

在警方的不懈努力和腾讯公司“跨年龄人脸识别”技术帮助下，“小耗子”终于被找到了。2019 年 5 月 3 日晚，中央电视台《等着我》栏目报道了这一历时十年的寻亲案件，以及在其背后提供 AI 技术支持的腾讯团队和故事，展现了这家互联网公司在 AI+公益事业上的不断创新与投入。

千万级数据检索精度超 99.99%，解警方“大海捞针式”寻人之困

据公开报道，我国每年新增失踪人口数量众多。人口众多加之流动节奏加快，一旦错失了寻回走失人员的黄金时间，就只能从市县一级适龄人口中进行搜索，这意味着至少数十万级别的检索规模。如果进一步扩大搜索范围至省一级，检索规模将急剧扩大到千万以上，比对的难度堪称“大海捞针”。

为了协助警方提升寻人的效率和准确度，腾讯优图实验室依靠在计算机视觉领域多年的积累，不断迭代人脸检索技术，增强人脸识别能力，协助警方在海量的人脸数据中快速对比、锁定、匹配出可能的失踪人口。

随着人脸识别算法的不断迭代优化，腾讯海量数据检索能力的精准度已超过 99.99%，毫秒级时间内便可完成千万级人脸检索，大大提高了走失人口匹配的精准度和速度，为警方寻人减轻压力，节省大量人力物力，帮助更多家庭团聚。

至今，腾讯优图已协助福建、四川等多地警方打拐寻人。其中，帮助福建省公安厅“牵挂你”防走失平台，累计找回 1091 余人；截至 2018 年 10 月，接入腾讯优图“天眼寻人”功能的 QQ 全城助力，累计找回 600 多人。通过公益寻人的多年积累，腾讯充分发挥技术的社会价值，让 AI 给社会带来更多可能。

过往的寻人案例，大多是在人口走失后短时间内的找回。而此次腾讯协助四川警方攻坚的打拐历史积案，除人口基数和地域外另一个需要突破的难点便是时间。在央视《等着我》栏目中报道的孩子们被拐均超过 10 年，而这段时间正是人一生中人脸变化最为剧烈的阶段，仅有几张婴幼儿阶段的模糊照片成为此次寻亲的唯一线索。

然而，跨年龄段识别本身就是学术界的一大难题，而且这个项目中走失的儿童都在 10 年以上，这对算法模型和数据量来说都是极大的挑战。

依托腾讯海量数据，腾讯优图首创跨年龄人脸识别技术，重点解决寻人场景中婴幼儿被拐的情况。为了充分的从数据中学习人脸自然的跨年龄变化规律，腾讯优图提出了基于 DDL（分布式蒸馏学习法则）学习策略的正则化迁移学习策略。基于该策略，算法模型可充分进行跨年龄人脸识别学习，从而让困难的跨年龄识别更加可靠和精准。

从 2018 年初开始，腾讯优图通过守护者计划平台与四川警方紧密协作，经过近一年时间的资源投入和优化调整，进行了上千次模型训练，经历 5 次版本更新，最终沉淀版本为一个具有上千层复杂结构的深度神经网络模型，跨年龄识别精度提升至近 96%。

仅凭被拐儿童幼年时期的照片与海量数据库进行比对，腾讯优图帮警方圈定与走失儿童最像的 5 名。最后的 DNA 验证结果证明，多位被命中的儿童都位于腾讯优图人脸比对结果的首位，央视《等着我》节目中报道的“小耗子”就包含其中。AI 技术的创新应用，让警方过往大海捞针式的人力摸排成为过去式。

践行科技向善理念 腾讯AI 有温度

作为一家互联网科技公司，多年来，腾讯始终致力于发挥自身能力与技术优势，践行科技向善理念，推动社会进步。在人工智能领域，腾讯一直坚持从用户价值出发，通过AI应用场景创新，不断解决社会难题。

此次为警方提供技术支持的腾讯优图团队，系腾讯公司顶级AI实验室，聚焦计算机视觉研究与落地，拥有超过700项全球专利，并在人脸识别数据库LFW、MegaFace、MOT challenge等多个国际赛事中不断刷新纪录，领先于国际水平的人脸识别技术为现实场景中的应用提供了保障。

为提升AI技术的普惠价值，2017年6月，腾讯优图联合腾讯云和腾讯志愿者等正式发布“优图天眼寻人解决方案”，进一步将科技更广泛地应用于社会，通过解决实际问题来践行科技向善的价值主张，帮助更多人找到回家的路，圆更多的家庭的团聚梦。

腾讯AI成为一个时间折叠者，连接十余年、千百公里的时间与空间。未来，腾讯将通过守护者计划平台，持续助力警方打拐寻人，让AI更有价值，更有温度。

Appendix 3

南昌：“AI”人脸识别锁定“毒驾、失驾”群体

2019-04-28 08:46:11 来源： 南昌晚报

原标题：南昌：“AI”人脸识别锁定“失驾”群体

注销、吊销、暂扣了驾照不能开车上路是众所周知的事情，更不用说无证驾驶，但总有一些人抱着侥幸心理。如今，随着人工智能技术的应用，失驾人员只要开车上路，交管部门就会发现其违法行为。

据了解，失驾是指驾驶员在失去驾驶资格后仍驾驶机动车上路行驶的交通违法行为，“失驾”的原因有多种，譬如“醉驾”吊销、“吸毒”注销、“超分”未学习、逾期未审验等。

为了防范毒驾、失驾人员违法驾驶机动车等隐蔽性强、社会危害性大的交通违法行为，南昌交警在全市范围内开展“鹰击”行动，并全面部署“人脸识别”卡口。南昌作为公安部集成指挥平台人脸识别系统全国首批试点城市，应用“AI”人脸识别技术的数据比对、分析、研判功能，在路面就能锁定失驾人员的违法行为。

记者了解到，自本月“鹰击”行动开展以来，南昌交警查获超百起失驾人员违法驾驶行为，其中 50 多名失驾人员在接到通知后主动投案自首。(记者 汪晶晶)

Appendix 4

人脸识别技术正广泛用于线下支付取快递等

2019-04-16 10:53:07 来源： 经济日报

北京市味多美朝阳门华普店的店员展示支付宝刷脸支付产品“蜻蜓”。消费者首次购物只要在“蜻蜓”上完成手机认证就可以通过摄像头快速完成刷脸支付。

新华社记者 张晨霖摄

人脸识别技术正广泛应用于线下支付、乘地铁、取快递等场景

“刷脸时代”真的来了

随着人脸识别技术快速发展，算法精度不断提升，安全性能也日益提高，“刷脸”已经逐步在金融、公安、边防、航天、教育、医疗等多个领域“落地开花”，确保公众隐私的同时，使公众享受更便捷的生活

中国科学技术大学附属第一医院近日上线了刷脸支付功能，患者为就诊卡充值时，只要通过人脸识别，再输入手机号就可以完成支付。据介绍，未来建档、挂号、查询报告等都可以通过“刷脸”完成，实现全流程“刷脸就医”。

“刷脸时代”真的来了！从身份审核到线下支付，从乘坐地铁到取快递、领养老金，“刷脸”正在变得一路畅通。数据显示，预计未来几年，人脸识别市场规模将保持年均20%左右的高速增长，到2022年，全球人脸识别市场规模将达75.95亿美元。

“暗战”刷脸支付

本月初，蚂蚁金服宣布支付宝刷脸设备“蜻蜓”在香港机场Duty Zero免税店投入使用，这也是支付宝刷脸支付首次出境，内地游客自此可以“刷脸买单”。而在此前，支付宝“刷脸”支付已覆盖超过300个城市。

市民在北京海淀公园的智能步道上行走。智能步道的起点、中间点、终点分别设有人脸识别杆，公众完成注册后，无需佩戴硬件设备，在步道内进行运动即可通过百度人脸识别技术自动记录运动数据。 新华社记者鞠焕宗摄

移动支付的一场“暗战”已经启幕。支付宝的刷脸支付设备“蜻蜓”像一盏台灯，灯泡的位置是书本大小的刷脸显示屏；微信刷脸支付的“青蛙”则可以直接接上POS机，代替原有的扫码枪即插即用地进行刷脸支

付。两家巨头为推广自己的刷脸支付可谓不遗余力，在微信方面，商家可以免费申领“青蛙”，在支付宝方面，尽管“蜻蜓”的售价达 2688 元，但从商家激活设备产生第一笔有效交易后，连续 30 天每天可根据使用用户数得到上限为 240 元的激励金。

刷脸支付最大的优势就在于便捷，消费者不用拿出任何设备，就可以完成支付。刷脸支付服务提供商小蚁科技 CEO 达声蔚坦言，刷脸支付的快速推广正来自于它对收银效率的提升。“手机支付平均需要 11 步，刷脸支付只需 1 步就可以完成。”去年年底，刷脸支付“落地”味多美的 300 多家门店。味多美首席信息官胡博表示：“刷脸支付与现在流行的现金和扫码支付相比，收银效率提升了近 60%。”

不过，对支付宝和微信来说，“暗战”还有自己的“小算盘”。对于支付宝来说，此前在线下扫码支付领域，其市场份额不断被微信所蚕食，其重要原因就在于同样作为“超级入口”，微信在用户手机上的打开率远远高于支付宝，但消费者一旦接受不用掏出手机的刷脸支付，这种“惯性”也将不复存在。而对于微信来讲，自然也要抵御这种“此消彼长”。中国连锁经营协会会长裴亮对此颇为感慨：“我国头部企业的零售创新已经进入了无人区，正在走别人不曾走过的路。”

一些人有疑问，刷脸支付首次使用时需要输入手机验证码，此后使用不用再输入密码，这安全吗？从支付宝和微信的刷脸支付设备来看，它们均使用了结构光摄像头和人工智能算法，据称能达到识别准确度 99.9%以上的金融级别安全等级。腾讯优图实验室总经理吴运声表示，腾讯优图研发的人脸识别算法是线上远程身份核实向线下场景的自然延伸。“目前投入应用的是腾讯优图的人脸识别祖母模型，1：1 条件下错误率仅为十亿分之一。此外，融合 3D 成像、近红外成像和 RGB 成像，人脸识别可以实现

高安全的活体检测技术，有效拦截照片、屏幕、面具的攻击，确保真人才能刷脸成功。”

落地多个场景

3 月 30 日，歌手林俊杰在湖北省黄石市举行个人演唱会现场，3 万多观众首次使用 35 台人脸识别闸机入场，验票实名制入场核验率高达 100%，人均核验通过速度在 6 秒以内。人脸识别不但快捷，还杜绝了黄牛的“倒票”行为。

安全领域曾是人脸识别应用最重要的场景，其市场份额占比 30%左右。但现在，人脸识别正在多个场景“落地开花”。

和刷脸支付一样，“刷脸”证明“我是我”，带来的是便利和效率。今年 4 月起，中国首条采用 3D 人脸识别闸机的地铁线路济南地铁 1 号线正式开启商业运营。通过刷脸识别，乘客可以在 2 秒内通过闸机，1 分钟内可通过 30 到 40 名乘客。而从今年 3 月起，菜鸟网络国内所有带摄像头的菜鸟驿站智能柜已陆续开通刷脸取件、刷脸寄件功能。菜鸟驿站智能柜高级工程师赵德山表示：“在此前的试点中，菜鸟智能柜已经产生了超过百万次刷脸取件记录。到目前，尚未发现误识导致误取包裹事件。”

“刷脸”的意义还不只于此。在北京、重庆等地，公租房使用了人脸识别的门禁系统，一旦发现多次出现的、未录入租户系统的人员，就将提醒物业人员现场跟进。这成为防止转租转借的“利器”，保证了只有录入系统的住户才能顺利刷脸进入。北京市住建委副主任邹劲松就表示：“目前，北京已经在 68 个公租房项目中安装人脸识别系统，未来将在全市公租房项目中全面铺开。”而在腾讯，人脸识别被用来为未成年人适度游戏“保驾护航”。对实名信息为成人，但在游戏中行为疑似未成年人的用

户，腾讯会要求用户进行刷脸验证，如果用户拒绝验证，或验证后发现与姓名信息不符，将被视为13岁以下的未成年人。

技术“一日千里”

“刷脸”时代为何此时来临？其背后是技术“一日千里”的快速发展和演进。最新数据显示，全球人脸识别算法的最高水平可以做到千万分之一误报率，相比于去年同期，全球人脸识别性能提升了80%。

我国的人脸识别技术更是领先全球。在美国国家标准与技术研究院公布的最新一次全球人脸识别算法测试结果中，依图科技、商汤科技、中国科学院深圳先进技术研究院3家中国团队占据了前5名。

从专利数量来看，2018年，我国人脸识别行业专利公开数量为5200项，同比增长93%。2019年1至2月，我国人脸识别专利公开量已经达到1174项。从资本市场来看，去年一年时间，主打计算机视觉的人工智能企业商汤科技、云从科技、旷视科技、依图科技共计发生了12起融资事件，说明人脸识别创业企业“长势喜人”。“4年前，人们见证了人工智能的人脸识别能力超过了人类。而在过去的4年里，人工智能的识别能力仍在指数级增长，算法精度又提升了10万倍。”依图科技首席执行官朱珑如是说。

人脸识别是否存在泄露隐私的风险？企业人士纷纷表示，“刷脸”不会记录、存储用户的身份信息。菜鸟运营专家明宇介绍，通过刷脸，用户不用线下留存身份信息，相关信息在云端受到最高标准的保护，站点人员接触不到，确保了个人隐私安全。但同样有学者表示，密码可以更换，但人脸却不能更换，因此一旦被黑客攻击，人脸识别系统可能会带来更为严重的安全问题。墨尔本大学数字隐私与安全研究员苏莱特·德雷福斯表

示："一旦人脸识别系统被黑客攻击，用户将无法从该系统退出，这有可能导致前所未有的安全问题。"（记者 陈静）

Appendix 5

海南省旅馆旅租场所实现人脸识别全覆盖

2019-04-16 08:11 来源：海南日报

省公安厅 4 月 15 日召开全省治安管理工作会议强调，强化治安风险防范化解，全力维护全省社会大局稳定；强化基层基础工作，创新优化"放管服"改革，出台居住证和落户等便民措施，不断增强人民群众获得感、幸福感、安全感。海南日报记者还从会上获悉，目前，我省在全国率先实现了全省范围内旅馆、旅租场所人脸识别全覆盖。

会议要求，进一步深化治安"放管服"改革，在全省各市县有条件的社区便利店、商超、政务窗口、人流密集场所投放 300 台 "智慧警务便民服务站"，为市民群众提供治安、户政、出入境、交管等业务的网上政务服务，实现全天候不间断贴近式服务，将警务便民服务延伸到社区。

据悉，过去的一年，全省公安机关治安部门坚持抓基层、打基础、强素质、上水平，坚持严打开路与源头治理相结合，管理创新便民服务与执法规范化相结合，推动我省治安管理工作的信息化、智能化和打防管控水平大幅度提升。我省在全国率先实现全省范围内旅馆、旅租场所人脸识别核验设备安装全覆盖，安装人脸识别核验设备 5559 家；推进散装汽油实名登记治安管理信息系统安装全覆盖，安装加油站 502 家，强化散装汽油动态监控，覆盖率达 100%。扎实开展扫黄禁赌、缉枪治爆、"利剑"等专项行动，全省共受理治安行政案件 50155 起，同比下降 15.8%，查处 48755

起，打击处理人员 30795 人，行政处罚 21810 人。（记者良子 特约记者宋洪涛 通讯员陈炜森）

Appendix 6

如厕还能体验人脸识别 景德镇“厕所革命”有特色

2019-04-13 08:47:09 来源： 江西日报

原标题：如厕还能体验智能人脸识别技术

景德镇市昌江区“厕所革命”有特色

智能人脸识别技术被运用到公厕中，如厕者只要将脸对准摄像识别区，机器下方很快就能自动吐出纸巾。4 月 11 日，位于景德镇市昌江区联想主题公园内的一座“第五空间”公厕，在微信朋友圈里吸引了许多人的关注。

这座占地约 120 平方米的公厕，分为男厕所、女厕所、第三卫生间等六部分。男、女卫生间内，空调、高低洗手台、自动喷香机等一应俱全。为了方便没有带手纸的市民如厕，卫生间入口处还设置了自动扫脸出纸机。特别值得一提的是，该公厕的第三卫生间内，设置了无障碍成人坐便位、残疾人报警器等设施。

将现代化、人性化、便民化设计理念融为一体，一改传统公厕功能单一的形象，是“第五空间”的最大特征。近年来，昌江区结合“双创双修”工作，先后建设了 13 座公园。为了解决居民在公园活动时遭遇的“如厕难”问题，从去年开始，结合“厕所革命”攻坚行动，该区启动“第五空间”公厕建设，截至目前已投资 160 万元建成了两座“第五空间”公厕。（记者王景萍 通讯员许荣崽）

Appendix 7

合肥推行公租房人脸识别系统

2019-04-02 08:18:38 来源： 安徽日报

记者从合肥市住房保障和房产管理局了解到，该市将在公租房项目中推行人脸识别系统，为防止转租、转借行为立起“防火墙”。

目前，合肥市蜀山区悠然居、卓然居公租房小区已经安装了人脸识别系统。小区住户可通过微信公众号、二维码扫描等方式注册，待物业公司审核住户为公租房承租人身份后，住户上传照片即可使用人脸识别功能，顺利进出小区。访客若要进入小区，住户可在系统中生成二维码发送给访客临时进入小区。

人脸识别系统是传统门禁方式的升级，以生物识别方式代替传统的刷卡，通过人脸抓拍、人脸识别门禁、智能分析、联网报警等系统的联动，能够实现事前预警、事中控制、事后追溯等。同时，人脸识别系统所收集的数据，在对承租人进出和房屋是否闲置等情况进行分析的同时，还能对公租房小区内孤老人员、精神残疾或需要监护居住的人员等进行特殊照顾。比如数据显示独居老人在一定时间未在园区出入，物业公司将立刻入户走访，以确保独居老年人的起居安全，预防意外发生。

安装运行人脸识别系统后，只有通过物业公司审核、完成人脸登记的人员才能出入公租房。该系统从技术上实现了对转租、转借、群租等违规使用公租房行为的管控。（记者 何珂）

Appendix 8

“智慧校园人脸识别”系统助力中央文化和旅游管理干部学院校园管理

2019-04-01 09:46:18 来源： 人民网-图片频道

3 月 27 日，陕西炬云信息科技有限公司完成了对中央文化和旅游管理干部学院“智慧校园动态人脸识别”系统平台的搭建。该系统集成了校园管理所涉及的众多功能模块，以“信息共享、集中控制”的方式，从统一网络平台、统一数据库、统一的身份认证体系等软件总体设计思路的技术实现考虑，使各管理系统、各读卡终端设备综合性能的智能化达到最佳系统设计，保证系统的前瞻性、开放性、安全性、稳定性、便捷性、适用性等。

人脸识别系统技术流程设计上，主要包括四个组成部分：人脸图像采集及检测、人脸图像预处理、人脸图像特征提取以及匹配与识别。有效地维护了校园秩序和安全，保障学校教学、科研工作地顺利进行，同时也提升了校园的安全环境，为学校的管理带来了高效和方便。

“智慧校园动态人脸识别”系统在中央文化和旅游管理干部学院的成功应用，解决了学校“按需、逐个、独立”的建设，有效地维护了校园秩序和安全，保障学校教学、科研工作地顺利进行，保证师生人身财产安全，营造安全、稳定、文明、健康的育人环境，为学校的管理带来了高效、方便与安全。我们也相信这样的科技应用也能让学院在众多院校信息化中脱颖而出并实现：高效管理+智慧落地+体验增强。

Appendix 9

3D 传感摄像头人脸识别率 99.9%

2019-03-30 08:58:57 来源： 科技日报

近日召开的“第十二届中国商业信息化行业大会暨2019中国智慧商业信息化展览会”上，由深圳蚂里奥技术有限公司发布的最新产品——首款MIPI 3D摄像头模组S1吸引了众人目光。

传统2D人脸识别由于无法记录脸部的深度信息，人脸数据并不完整，这也就给了虚假照片、视频或人脸硅胶面套以可乘之机。相比而言，3D传感摄像头进行人脸识别时，内置的点阵投影仪可投射出3万多个肉眼不可见的红外点到用户的脸部，在颜色、纹理、深度等方面的数据更丰富，安全性和精准性更高，识别速度更快。

蚂里奥首席产品官张兼告诉科技日报机者，MIPI 3D摄像头模组S1厚度仅5.83毫米，检测距离为0.3—1米；其拥有垂直大视角，可拍摄更多内容，适应较大身高范围，方便消费者进行人脸识别；此外，S1还加入了泛光灯，即使在暗光环境下，也可清晰识别人脸。

安全性方面，S1支持红外识别，进一步增强了防伪辨别能力。依托红外识别+RGB+深度识别的多模态生物识别及毫米级3D人脸测量精度，S1人脸识别率可达99.9%。（记者 操秀英）

Appendix 10

人脸识别“签到”即可“巡河”

2019-03-25 07:38:57 来源： 广州日报

佛山的河长通过人脸识别“签到”，就能在线上完成“巡河”工作?河涌水质不再依赖人工监测，就能实现24小时全天候智能监测、预警和治理？连日来，记者走访河湖长制管理信息系统与河涌医生健康服务平台的研发企业，了解环境治理背后的科技创新。

创新一：人脸识别“签到”完成在线“巡河”

去年，作为三防指挥一张图体系内的一个子系统，河湖长制管理信息系统在佛山上线。自此，佛山的河长、湖长有了一个从移动端“巡查”河、湖的工具。打开手机 APP 或微信小程序，通过人脸识别“签到”，河长、湖长不但可以直接掌握分管河、湖的水质情况。作为最早开发河湖长制管理信息系统的企业之一，广东广宇科技发展有限公司（以下简称“广宇科技”）凭借在三防指挥一张图体系多年积累的研发优势，将大数据、人工智能的技术运用到“治水”的领域。

“河湖长制管理信息系统解决了‘谁来监管监管者’的问题。”广宇科技负责人表示，污染源在哪里，河湖长有没有及时去处理，都会反馈到系统中。而区、镇也会结合自身环境治理的管理需求，在该系统基础上添加、完善更多的功能。该科技能够结合这些特定的需求，在应用层完成“插件式”的开发。借助“预防为主”的三防指挥一张图体系，河湖长制管理信息系统推动了各个单位之间“治水”信息的共享和利用。

创新二：从监测、溯源到治理污染源的智能治理

在禅城西四涌监测点，河水通过环保水质陆基监测站埋伏在水中的传感器，每隔两小时被自动抽取出来做“体检”。而类似这样连接禅城区综合治理云平台的全天候自动化监测站，在禅城有 10 个。广东奥博信息产业股份有限公司（以下简称“广东奥博”）相关负责人介绍说，这些监测站能够集取水采样、实时分析和数据上传功能为一体，发现数据超标便触发预警。

“陆基设备适合布置在区域交界的断面上，无人船、浮标站、环境巡查船等水基设备的运用则更灵活。”该负责人介绍说。陆基与水基设备的结合，可以实现实时监测、自动生成水质分析报告，分析各段流域水质等

级、达标情况等。再结合网格员的巡检，监管部门能够及时缩小排查范围，从而准确锁定污染源。

前瞻：水陆空天“四位一体”监测

“河涌医生服务平台与河湖长制管理信息系统有互补的作用。”广东奥博相关工作负责人介绍说，下一步，还将把空基、天基和水基、陆基的设备结合起来，来对更广阔流域的污染问题展开监测和预警。其中，空天设备的结合，将用河涌污染遥感时景监测和无人机河涌动态巡逻来丰富监测的场景与手段。现在，广东奥博的团队正在研究离群检测溯源的方法。这种方法区别于传统的企业排放监控，专门从分析同行业、同类型企业之间的排放差异入手，发现与合理排放区间差异较大可疑企业，从而能够快速锁定污染源头。这对跨部门的协调提出了新的要求。

此外，指纹溯源为“治水”提供了一种一体化的解决方案。借助溯源仪，采集污染源水质指纹特征，建立起污染源指纹数据库。这种指纹特征实际上是由大量化合物的数据沉淀所形成，可以把源头精准锁定到企业。当河涌发生污染事故时，在线比对污染源指纹，再展开现场核查，即可在21分钟内快速完成一次溯源任务。（记者杨博）

Appendix 11

“人脸识别”助93人成功寻亲

2019年06月20日10:20:32 来源：无锡市委宣传部

患有老年痴呆症、在外流浪8年的张老伯没有想到，无锡市救助管理站依靠先进的人脸识别技术，为他找到了失散已久的亲人。80岁的张老

伯原来居住在无锡市太湖街道，8年前的一天离家后便再也找不到回家的路，辗转流浪到江阴。江阴市救助管理站对其进行救助后，却一直无法找到其家人。直到2018年，无锡市救助管理站引入人脸识别技术后，经过比对，终于找到了张老伯的家属。

“近年来，我们依靠人脸识别等先进技术，成功帮助93名流浪人员找到了家人。”市救助管理站相关负责人介绍，滞留在该站的救助对象中，有相当数量的“无名氏”，这些人大多患有精神方面的疾病，或者存在智力障碍，无法说清自己的家庭住址、亲人联系方式等，其中有的人已在市救助管理站滞留较长时间。过去，市救助管理站通过公安人口信息比对、失踪人口信息查找、发现地周围群众走访等方式为他们寻亲，但收获不大。后来，又尝试在报纸刊登寻人启事，在电视台播放图文寻亲，通过全国救助寻亲网、公安DNA血样比对、手机“今日头条”开展寻亲等途径，但收效也不明显。

转机出现在2018年，市民政局与市公安局开展协作，充分利用先进的科学技术，将近年日益发展、成熟的人脸识别用于救助对象身份比对工作，终于取得突破。专家介绍，人脸识别，是对人脸特征进行分析计算并进行身份识别的一种生物识别技术。这种技术是用摄像机或摄像头采集含有人脸的照片或视频，对其中的人脸进行检测和跟踪，进而达到识别、辨认人脸的目的。

无锡市民政局与市公安局合作引入“人脸识别”技术，大大提高了寻亲的精准度与成功率。

市民政局相关负责人介绍，今年我市将进一步强化寻亲服务工作，与公安部门联合建立寻亲协作机制，全面运用公安人口管理信息系统、DNA鉴定、人脸识别等技术手段开展寻亲。各救助机构将建立专业化寻亲人才

队伍，综合运用语言学、心理学知识和“互联网＋”等技术力量手段开展常态化寻亲服务。 （挥戈）

Appendix 12

半年查了 8000 个 济南查酒驾用上大数据、人脸识别

2019 年 06 月 27 日 16:02:26 来源： 大众网 • 海报新闻

在交警查酒驾越来越严的当下，今年以来的半年内济南仍查出了 7900 多起酒驾、醉驾，比去年同期翻了一番还多。济南交警为了高压严查，用上了“酒驾预警分析系统”和人脸识别技术等手段，不再是简单的路口设卡蹲守。

来自济南交警支队的信息显示，今年以来截止 6 月 26 日济南市共查处酒驾醉驾 7989 起，其中酒驾 6120 起，醉驾 1869 起。7989 起这个数字比去年同期上升 136.8%，也就是翻了一番还多，此前侥幸避开检查的酒驾司机们，现在越来越多得浮出水面。

酒驾查处效率提高的背后，一些“黑科技”手段功不可没。一方面济南交警借助“酒驾预警分析系统”，通过分析此前酒驾引发交通事故和酒驾查处的大数据，找出酒驾高发区域和高发时段，并指导警力投放方案和出警时间。分析发现，近三年来午间（13 时至 15 时）的酒驾占比明显较大，警方及时加大午间查处力度，今年以来已查处午间酒驾、醉驾 2669 起，占查处总数的 35.23%，比去年同期增加了 60%。

另一方面，通过数据的梳理碰撞，交警重点关注有违法记录的高危驾驶人，特别是对济南市 525 名多次酒驾的驾驶人进行动态监控，利用二次识别、人脸识别技术，准确查缉违法车辆，实现了精准查缉。今年以来，

济南交警共查处二次酒驾 143 人，醉酒驾驶营运车 5 起。通过酒驾预警分析系统，交警还在传统守候式查缉的基础上增加了合围式查缉等方式，精准查缉 1507 起。

随着酒驾查处越来越严，代驾市场也明显升温。来自行业的统计数据显示，去年 12 月至今济南市各主要代驾平台的订单量比去年平均了上升35%，市民心中“开车不喝酒、喝酒不开车”的高压线绷得越来越紧。（记者 贺辉）

Appendix 13

天津市中研附院推出“人脸识别”预约挂号系统

2019-06-18 17:01:18 来源： 今晚报

记者从市中研院附属医院获悉，该院近日推出“人脸识别”预约挂号系统，患者只需“刷脸”就能轻松取号、候诊、看病。

“人脸识别”预约挂号系统借助互联网和人脸识别技术，帮助患者进行实名登记预约。患者需携带本人身份证，到服务中心窗口建档。随后持身份证到自助机进行预约取号，点击人脸识别按钮，只需面对摄像头，系统获取患者面部信息后，即可完成人脸识别核验，确认就医档案信息，进行取号操作。

“人脸识别”预约挂号可有效地遏制“黄牛”倒号现象，净化就医环境。该院还将把人脸识别挂号应用到医院各个科室，实现全流程覆盖，患者在就医各个环节都可通过刷脸完成身份验证和支付，就医更安全更便捷。（黄建高）

Appendix 14

新机场安检引入人脸识别技术

2019-06-14 来源： 北京日报

北京大兴国际机场打造全球超大型智慧机场，广泛应用了各项智慧型新技术。昨天，民航局召开新闻发布会，记者从发布会上了解到，大兴国际机场的自助值机设备覆盖率预计将达到 86%，自助托运设备覆盖率预计将达到 76%，安检通道均引入了人脸识别等智能新技术，旅客从进入航站楼一直到登机口，可实现全流程自助，无纸化通行，大大提升通行效率。

据介绍，打造智慧机场方面，大兴国际机场建设了 19 个平台的 68 个系统，以实现对机场全区域、全业务领域的覆盖和支撑。民航局机场司副司长张锐介绍，大兴国际机场全面采用了 RFID 行李追踪技术，可实现旅客行李全流程跟踪管理，旅客可通过手机 APP 实时掌握行李状态，将有效缓解旅客等待行李的焦虑感。

同时，大兴国际机场建立了统一的运行信息数据平台，纳入了各相关单位的系统数据信息，并整合大数据分析等技术，全面掌握航班运行状态与地面保障各环节的信息，实现信息精准掌握，运行智能决策，将总体提升机场运行效率。

随着我国民航业的快速发展，民用机场数量与机场业务量持续增加。数据显示，2018 年，民用机场年旅客吞吐量达到 12.6 亿人次，飞行起降量达到 1108.9 万架次，十年来的年均增长率分别达到 11%和 19%；同时，我国民用运输机场数量已经达到 236 个（不含港澳台），平均每年新增加 7 个运输机场；还有我国的千万级机场数量已经达到 37 个，3000 万级机场数量达到 10 个。

“然而，我国的千万级机场却普遍面临着容量饱和或者濒临饱和的问题；同时，旅客对民航便捷、高效、舒适出行的需求也迟迟无法得到满足。”张锐说，在此背景下，民航局加快推进以“平安机场、绿色机场、智慧机场、人文机场”为核心的“四型机场”建设，打造集内在品质和外在品位于一体的现代化民用机场。（记者 董禹含）

Appendix 15

微软删除人脸识别数据库，源于“伦理”识别

2019-06-12 06:49:36 来源： 新京报

人们崇尚的发展，含义更多地偏向了技术发展，却忽略了技术所带来的社会发展。

据报道，近日，微软已经悄然删除其最大的公开人脸识别数据库——MS Celeb。MS Celeb 数据库于 2016 年建立，微软描述其为世界上最大的公开面部识别数据集，拥有超过 1000 万张图像，将近 10 万人的面部信息。

根据资料统计，在微软删除该资料库前，已有多个商业组织在使用 MS Celeb 数据库，包括很多知名互联网企业。所以，此次微软删除这个数据库影响颇大。问题来了——微软为什么要删掉这些人脸数据？

最直接的考虑，就是担心侵犯公众隐私权、“数据权”，从而产生法律风险。

据了解，微软是通过“知识共享”许可，来抓取图像和视频中的人脸信息的。只不过，“知识共享”许可仅来自于图片和视频的版权所有者的

授权，而微软并不一定直接得到了照片与视频中人物的授权许可。所以，这些人脸所对应的人，有可能指控微软侵权，从而产生法律问题。

法律问题很重要，但微软删除这个数据库，恐怕还有更深层次的考虑。

人脸识别当然是一项具有很大市场价值的技术。首先，这能带来不少方便。消费者通过“刷脸”解锁手机、进行电子支付，是全球消费电子领域的大趋势。

其次，这还可以加强执法力度。人脸识别可用在追捕逃犯、重要场合快速安检等方面。

但也应看到，人脸识别有可能突破这些领域，侵犯公民权利。作为一家技术公司，微软本身一直在公开反对将这种技术作为政府监督的一种形式。

在 2018 年 12 月的一篇博客中，微软呼吁各公司建立保障措施，敦促各国政府立法，要求对面部识别技术进行独立测试，以确保准确性。今年 4 月份，微软还拒绝了加州一家执法机构要求在警车和身体摄像头上安装面部识别技术的要求。

不仅微软认识到这个问题，今年 1 月，旧金山提出了一项关于监视技术的行政法规——《停止秘密监视条例》，要求该市的政府部门在使用或购买监控技术前征求监事会的批准，并每年向监察委员会提交监视技术设备或服务的审计报告。

技术在飞速进步，其必然会对整个社会产生影响。在人脸识别这项快速变化的技术面前，社会必然会受到极大冲击。

而如今，人们崇尚的发展，含义更多地偏向了技术发展，却忽略了技术所带来的社会发展。微软删除人脸识别数据库，正是顾虑到技术发展对社会发展有可能的抑制。这对很多领域也是启示：面对一日千里的技术，是该放慢脚步，好好思考一下技术发展带来的各种社会效应了。

记者:刘远举（上海金融与法律研究院研究员）

Appendix 16

人脸识别让寻亲不再是大海捞针

2019-06-10 15:23:17 来源： 科技日报

仅凭一张婴幼儿时期的照片，能否找到被拐长达十年的儿童？目前人工智能广泛应用于各个领域，其在寻找走失儿童等公益场景中也开始担起重任。

近日，广州市慈善会、佳都科技等共同启动了“人工智能+慈善”战略合作，创建运用人工智能技术的寻亲平台——“AI 回佳”平台。此次打造的平台既能进行人脸识别，提高寻人效率，也能模拟人脸成长变化。“平台利用了人脸识别技术和全民随手拍的人脸库进行识别比对，从而协助失踪家庭寻找走失的亲人。”佳都集团执行总裁李旭说。

人脸识别＋人脸模拟算法 缩小寻亲范围

“人工智能在帮助寻亲方面的优势不言而喻。”第十三届全国人大代表、宝贝回家寻子网创始人张宝艳对此充满期待。她说：“以前寻亲，只能一张张翻看、对比照片，当看过成千上万张照片时，人就迷糊了，准确率低。目前，我们网站已登记超过 8 万份走失者资料，利用人工智能，能够瞬间从这些资料中找出匹配度最高的那份，极大地缩小了寻亲范围。”

而计算机视觉技术一直是佳都科技深耕的领域，目前已经形成了视频云+大数据、三景合一、商用智能人脸识别终端等一系列的AI成果。此次，佳都科技尝试将人工智能科技融入和应用到公益领域，携手广州市慈善会共同打造“AI回佳”平台，助力寻找走失儿童。

“平台采用了多算法融合引擎，通过多算法同时对同一张照片进行多维度识别，能大大提升识别准确率。”佳都科技副总裁刘斌介绍，平台具备人脸识别和人脸模拟算法两大核心技术。前者识别率高达99.9%，每秒十万次的人脸比对，如在海量寻亲数据中运用将大大节省人力成本，提高寻人效率；后者则利用AI算法模拟人脸的成长变化，帮助那些失踪多年的家庭生成小孩成年后的照片，从而帮助他们能够更有效地寻亲。

很多孩子在走失时只有几岁，在失踪多年后，孩子的容貌已经发生了变化，这无疑给寻亲带来了不小的阻碍。而人脸模拟技术正让这个问题得到解决。技术人员利用人脸模拟成长算法，可根据孩子幼年时期的照片模拟生成一张如今样貌的照片。

刘斌表示，人脸模拟是通过“已知模拟未知”，比人脸识别更具有技术挑战性。“我们这次在国内率先将人脸模拟算法的接口开放给公众，实现大规模场景下的广泛应用。不过人脸模拟主要为家属提供辅助性帮助，不能作为唯一标准。”

呼吁接入多维度数据 打通“数字孤岛”

“AI回佳”平台包括网站、微信公众号和微信小程序端口，包括“随手拍”和“找家人”两大模块。

见到身边有疑似被拐儿童或乞讨儿童，热心市民可拍下照片，上传到“随手拍”页面，帮助孩子寻亲。寻找小孩的父母可将照片传至“找家

人”页面。这是否会涉及到隐私问题呢？刘斌表示，上传到平台上的所有照片，在系统中只生成数字特征码，不会保留原图，且上传的照片仅开放给匹配相符的寻亲家庭看见，信息安全可以得到保障。

实际上，“AI 回佳”平台并非个例。已经有包括百度、腾讯、360、阿里等不少互联网公司把人工智能技术运用到打拐寻人方面，启动了寻亲项目。的优图人脸识别技术，已在福建省帮助警方找回走失人员 1091 名，发布“中国儿童失踪预警平台”、QQ 全城助力公众号；今日头条成立“头条寻人”项目组；line，上线“团圆”项目。

今年 5 月，中央电视台《等着我》栏目报道了腾讯优图实验室借力 AI，助力警方找回 7 名被拐超过 10 年的儿童，让 7 个家庭破镜重圆。

这背后依靠的就是迭代人脸检索技术，增强人脸识别能力，实现了在海量的人脸数据中快速对比、锁定，匹配出可能的失踪人口，毫秒级时间内便可完成千万级人脸检索。

“大数据之下，数据和数据之间要发生关联，价值才能最大化。”刘斌认为，仅靠一个“AI 回佳”平台，难以达到最佳效果。希望国内相关平台能有机整合、连接在一起，打通“数字孤岛”，接入更多维度的数据，通过数据融合为更多丢失儿童找到回家的路。

“每个寻人平台的算法略有不同。有时在腾讯上匹配不出来的，在百度上又能找出来。对丢失儿童父母来说，多一个平台，就多一份希望。”张宝艳呼吁更多的技术企业加入到公益慈善中。（记者 叶 青)

Appendix 17

人脸识别供纸机不只是解了公厕的围

2019 年 05 月 27 日 10:40:53 来源：无锡市委宣传部

早就听闻省内多个城市在推行智慧公厕，近期在南京街头就亲身体验了一把，温湿度实时显示、可用厕位实时显示等常规招数且不去说它，但人脸识别自动供纸机着实让人开了眼。供纸机立在公厕正中，进门前先把脸凑过去扫一扫，几秒钟不到纸就自动吐出来了。不够？手机扫机器上的二维码可以再免费领一次。观察了一下，绝大多数人都是只领一次。贪小便宜，扯了公厕很多纸带走的现象没发现，现在想这么做也难。

“厕所革命”搞了有好几年，绿化、卫生之类的面上问题不难解决，加大点投入、加强点管理就行，唯独这免费供纸问题让城市管理者犯了难。供应吧，纸品消耗量太大，浪费或是顺手牵羊现象比比皆是，有损城市形象，而且频繁加纸也是在加重保洁人员负担。不供应吧，貌似这“革命”不彻底、“星级”上不来，市民心里也有疙瘩，觉得有关方面太小气。人脸识别自动供纸机可算是解了公厕的围，既免费供了纸、方便了市民，又节约环保，展示了城市智慧、文明的一面。有数据显示，苏州、南京的一些公厕，用了这个自动供纸机后，每天耗纸量从 7 卷下降到 2 卷，节约的成本可不是小数目，给城市形象的加分也是有目共睹的。联想到商场、超市等商业机构以及机关单位、工厂等的内部厕所，也多采取传统的供纸方式，如果能推广自动供纸机，节约下来的成本将更多。

可以说，小小供纸机解的不只是公厕的围，还给人以启示，就是遇事要换个思路考虑问题、创新手段解决问题。在免不免费供纸的问题上，如果照传统的宣传教育路子死磕下去，估计会是道长久都难解的题。自动供纸机、自动烟雾报警器等智慧小能手的出现，解决了很多看似很小实则很大的难题。城市管理者要多一些开放创新思维，让智慧化手段渗透到城市更多角落，让市民实实在在享便利，让城市更显时尚和年轻态。（时晓）

Appendix 18

郑州市所有出租车将安装人脸识别系统

2019-05-25 08:48:53 来源： 郑州日报

记者从昨日举行的市出租汽车行业2019 年服务提升工作动员大会上获悉，根据最新发布的《郑州市出租汽车行业服务管理提升工作方案》，我市市区所有巡游车上将安装具备人脸识别、行为分析和音视频监控等新功能的终端设备，使用具备乘客评价、投诉和支付功能的二维码系统，实现对“人、车、企业”的科技化监管。

根据《方案》，我市还将建立日常考核机制，通过社会第三方专业机构的参与，对出租汽车企业和驾驶员进行考核，实行“红黑旗”和“红黑名单”制度，每季度推送至行业和省市征信平台，实现联合奖惩，并纳入年度服务质量信誉考核。

在月评比中，对表现突出的驾驶员进行考核加分，对排名前三的公司挂“红旗”；季考核评选出 30 名先进人物，每人奖励 2000 元，列入行业“红名单”；季考核排名前三位的企业各奖励 3000 元，并列入行业“红名单”。

在月评比中，对违反《郑州市客运出租汽车管理条例》规定的驾驶员进行行政处罚，对擅自改装计价器和在一个积分周期内因拒载、不使用计价器或不正确使用计价器、收高价、不服从站点管理等行为累计受到 3 次及以上处罚的驾驶员，吊销其从业资格证，五年内不得从事出租汽车营运，并列入当月驾驶员“黑名单”。

在季考核、年总结中，考核得分在 4 分及以下的驾驶员，将被列入行业重点监管对象，组织五日停业培训，考试合格后方可恢复营运。一个季度内被两次“黄牌”警告的公司挂“黑旗”，一个季度内被两次挂“黑旗”的公司，将被列入行业“黑名单”和重点监管对象。（记者 聂春洁）

Appendix 19

中科院重庆研究院牵头研发的“机场安检智能识别系统”实现全流程人脸识别

2019 年 05 月 21 日 15:07　来源：新华网

新华网重庆 5 月 21 日电

旅客仅需在安检验证时出示一次证件进行身份核验，就可全程“刷脸”通关。5 月 20 日，新华网从中科院重庆研究院获悉，近日中科院重庆研究院与中国民航管理干部学院签署了合作协议。由该院牵头的重点项目“机场安检智能识别系统”已实现机场全流程人脸识别，并将在全国推广。

在协议中，双方就深化合作达成共识：重庆研究院将针对民航行业发展中的重大关键性、基础性和共性技术问题，持续不断地将具有重要应用前景的科研成果进行系统化、配套化和工程化研究开发，为智慧机场建设提供成熟的技术路线和相关产品，搭建数据中心及技术测试平台，推动民航行业的科技进步和产业发展；推进智慧机场联盟的建设，完善合作机制，创新合作模式，拓展合作领域，联合实施重大科技项目，联合推进科技成果转移转化；双方将加强合作制定技术标准及应用规范。

据中科院重庆研究院智能安全技术中心主任石宇介绍，为满足民航行业“创新安检模式、优化安检流程，积极利用先进技术，加强对重点人、重

点物品的检查，提高安检准确率和效率”的要求，中国科学院于 2017 年 9 月启动实施了中国科学院科技成果转移转化重点专项（弘光专项）项目“机场安检智能识别系统”,重庆研究院智能安全技术研究中心联合智慧航安（北京）科技有限公司，承担该专项的研究与转移转化工作。

“安检人脸识别辅助验证系统，应用于安检通道前的验证环节，通过读取身份证登记照与现场持证人员的脸部进行比对验证，判断是否为本人。目前累计应用于全国 70 家机场的旅客安检，覆盖 618 条安检通道。”石宇说。

据悉，该院最新研发的人工辅助验证智慧安保系统，旅客仅需在安检验证时出示一次证件进行身份核验。成功后，安检通道的身份复核、登机口的旅客信息复核都可以“刷脸”完成。全程无需登机牌、二维码，现场人脸照片直接成为数字化安检验讫标识。该系统在呼和浩特白塔机场试运行期间，安检通道前的人脸识别闸机人均通关速度已达 6 秒以内，安检通道内的人脸识别复核工作可实现小孩独自“刷脸”过闸机，不论始发、中转还是经停旅客，在按有该系统的登机口都能实现“刷脸”登机。

此外，人包对应系统，应用于安检通道内，将行李与其所有人进行匹配，以备后续开箱检查等操作。动态布控系统，利用动态人脸识别技术，在实时高清视频中动态检测跟踪人脸，同时提取人脸特征上传服务器，分析各种人脸属性并与目标人物比对。当目标出现时可实时响应，同时，也可输入目标图片在历史记录中进行检索，形成目标行动轨迹。

据石宇介绍，这些系统的联动应用，将实现机场里的全场景“刷脸”：安检验证时“刷脸”过检，安检通道内刷脸复核、人包匹配。同时，X 光安检机判图人员刷脸上岗，定时换岗。通过安检通道进入封闭区后，“刷

脸”寻人。在中转联程柜台前，可以“刷脸”办理乘机手续、登机口“刷脸”登机。机场禁区内，相关人员“刷脸”进入。

“随着协议的签订，这一套应用流程将全国推广，人脸识别技术等智能技术将在民航领域广泛应用，为机场工作人员提供智能化的辅助，提升机场安全裕度的同时，为旅客的出行提升便捷度与舒适度。”石宇说。（静梓）

Appendix 20

人脸识别黑科技为大连国际马拉松赛保驾护航

2019-05-12 22:02:02 星期日 来源： 大麦网体育中心

5月12日，第32届大连国际马拉松赛中的半程马拉松和全程马拉松鸣枪开跑。2万余名来自世界各地的参赛者，从大连国际会议中心出发，沿着城市风景燃情奔跑。

据了解，大麦网作为本届大连国际马拉松赛的官方合作伙伴，为赛事提供的人脸识别黑科技成为一大亮点。据大麦网体育中心总经理尤佳介绍，本届大连国际马拉松赛解锁马拉松新玩法，首次引入人脸识别技术，并将其应用到“参赛物品领取”“选手检录”等选手服务场景，不仅优化了领物流程、提高了检录效率，同时尽可能地规避了替跑、蹭跑、号码布造假等行为，充分保障赛事的公平公正。据大麦网数据统计，5月12日比赛日当天，大麦网在全程和半程各检录区域共铺设66台人脸识别设备，拦截多名替跑者。

除引入人脸识别外，大麦网还运用互联网技术为大连国际马拉松赛事提供，包括：官网报名系统搭建、大数据分析和现场服务等多个方面的全链路服务，全方位提升赛事服务科技含量和参赛用户体验度。

据介绍，在赛前领取参赛包阶段，大麦网专门联动了支付宝，为参赛者提供电子身份证人脸信息采集的便捷服务。一旦遇到忘记携带身份证、身份证消磁、由于身份证照片与当前形象相差较大无法识别等多种突发情况，参赛者可在现场选择通过支付宝采集人脸信息生成电子身份证，从而避免了此前以人工解决方式进行信息采集的繁琐和不便。“据统计，现场有 10%的用户通过支付宝电子身份证核验领物，这一方式提升了赛事服务效率和参赛者体验度。”尤佳说。