Journal of US-China Public Administration, May-June 2021, Vol. 18, No. 3, 115-132
doi: 10.17265/1548-6591/2021.03.003

The Application of Facial Recognition in China and India: Potential Risks and Regulation Suggestions

Shufeng Zheng
Law School, Peking University, Beijing, China

Facial recognition technology has multiple functions and risks, and has been widely applied in China and India. The current practices in these two jurisdictions have given rise to multiple issues in the application process, including privacy infringements, errors, bias of the recognition results and risks of governmental surveillance. Based on the issues and current rules, governments should focus on both individual protection and participants' (i.e., companies and institutions that use this technology) regulation. For individual protection, legislators should use the rules regarding privacy and personal data protection to guarantee individuals' control over their information and neutralise the power difference between individuals and powerful technology users. For participants' regulation, this paper suggests that regulators use multiple mechanisms (including but not limited to laws) and hybridised regulation powers to influence participants' behaviours and to promise responsible use of facial recognition technology.

Keywords: facial recognition, privacy, personal data, post-regulatory state, technical standards

Introduction

With the 4th Industrial Revolution (Industry 4.0), the development of artificial intelligence (AI) technologies has become the differentiating factor in global competition. As Lee (2018) pointed out, AI has transitioned from a period of discovery (the 1980s and 1990s) to a period of implementation, marking a shift in reliance on strengths for AI development[1]. Although the most visionary AI innovations and algorithms originated from the United States, the large populations, technical resources, governmental support on AI development, and Internet industries have given China and India an edge in the period of implementation. Recognising AI's transformative potential, both the Chinese and Indian governments actively apply AI technologies in practices in their national overall develop plans[2]. They hope to improve their technology level

Shufeng Zheng, Ph.D. Candidate, Law School, Peking University, Beijing, China.

[1] According to him, visionary research may no longer be the essential element of technology development, instead, abundant data, a hypercompetitive business landscape, and a government that actively adapts public infrastructure with AI in mind function as main drivers for AI development.

[2] The Chinese government has put AI as the "new engine of economic development" and "a core driving force for a new round of industrial transformation", with the goal to develop the country into the world's frontiers of science and technology by 2030. See The State Council of the P. R. China, A Next Generation Artificial Intelligence Development Plan (Guofa, 2017, No. 3). China also put "developing intelligent and networked products, AI's support system, and intelligent manufacturing" as its major tasks to encouraging AI industries. Three-Year Action Plan after Artificial Intelligence Development Plan. Similarly, the Indian government's think-tank NITI Aayog released the national AI strategy calling to develop AI not only for economic and military growth but also for social inclusion, calling it, #AIforAll (See NITI Aayog, "National Strategy for Artificial Intelligence # AI FOR ALL") (June 2018).

in the process of applying technologies, following a model of "improve their technologies in the applying process", contradict to the traditional model of "innovation and then apply". Reliance training practices for AI's deep learning technologies partially support this model.

However, multiple issues have come to the fore during the application of controversial technologies. Facial recognition is a typical example. This paper first gives a brief outline of facial recognition and its features before focusing on application issues exposed in China and India. Finally, the paper proposes suggestions regarding the regulation of such technology.

Contours of Facial Recognition Technology

Facial recognition, as an essential area of AI[3], refers to technology capable of identifying or verifying a person from digital images or videos. It works by extracting a person's facial features and comparing them with existing images or recordings. More specifically, it performs steps of face detection, face alignment, feature extraction and face matching (see Figure 1).

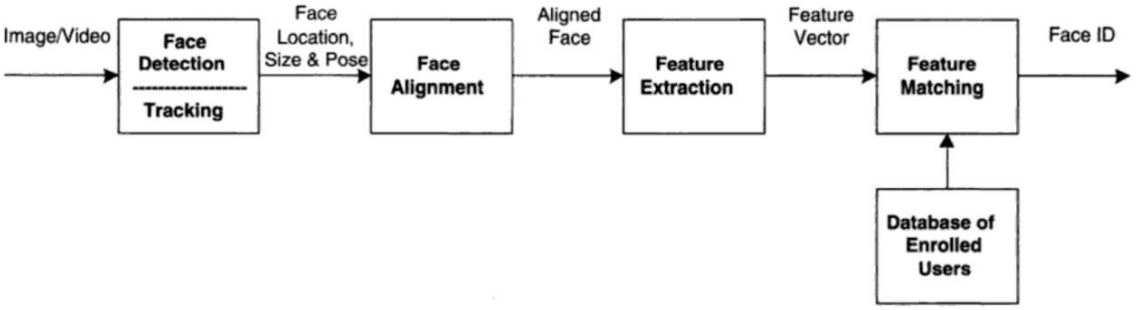

Figure 1. Face recognition processing flow (Brownlee, 2019).

Facial recognition has experienced a rapid evolution in the technical and practical fields over the last decade. It originated in the early 1960s when Woodrow Wilson Bledsoe created a system that could organise photographs of faces using the RAND Tablet (a graphical computer input device). After slowly evolving from manual detection to automatic processing[4], this technology developed rapidly in both technical and practical fields. According to the National Institute of Standards & Technology (NIST), significant improvements in accuracy of recognizing face have been achieved in the last five years, with an error rate of 0.2% in 2018,

[3] According to Cognilytica's report, "facial recognition and computer vision" is listed as one of the nine main AI areas. See Cognilytica Research, Worldwide AI Laws and Regulations 2020. Retrieved from https://www.cognilytica.com/2020/02/14/worldwide-ai-laws-and-regulations-2020/

[4] Initially, it requires manual work to extract the coordinates of features that to be used by computers for recognition (Later in the 1970s, Harmon, Goldstein, and Lesk made the manual facial recognition system more accurate.) In 1991, Pentland and Turk, based on the Eigenface approach from Sirovich and Kirby, found ways to detect faces within images, which was the first automatic face recognition attempt. Then, in the 1993-2000s periods, DARPA and NIST released the FERET program to encourage commercial facial recognitions. See relevant history introduction, Divyesh Dharaiya, "History of Facial Recognition Technology and Its Bright Future". 12 March 2020. Retrieved from https://readwrite.com/2020/03/12/history-of-facial-recognition-technology-and-its-bright-future/?__cf_chl_jschl_tk__=3aeca1a8d6f163427a9383f1c72bff83a367f3c0-1590640223-0-AVmIf-oYOsqLVjdn5WzpysWUptEdy-C-0DLf5h3pjiSMXtyfXSWlbGnd6W_m-5ULbBg58JS8ZdrMzfN38i802s0-JjwTBL0wmodRDviBpMgTpyQcsLiuU-7I_TTybhO0-ydHCV2k6t4Zc2VlYqmHWA7P97iA2a7QoWzj28fAKy-k2Q8h4jnVDEvJK3vj06ZMEKfihTo4vlZAHVmpKNH9TUTMUgIqoSBvhenaCB3uuTrtVrp9EeKf9WtbALY62C0bV02Aw_UJd5WnNK6qcVEYem32coc4ftAY7vxCDoUmMI7LxU4ytZ7hrhUjbWibDYSuMi6IpzR5WYIIE80Wwf69qYGR-u5ptWoOYG0ni9R-xFyLQ2TLjUx0TsGbb5frDQ59BJOQLkSk2FjJNvHFFrYWtTIuERdHCO2NVB8hyHGT0dBzcderBin4ARtw_cW3tSs9Gw

compared with 4% in 2014. Such improvements mainly result from the deployment of artificial neural network algorithms[5]. As a result of the improved accuracy, as well as the accumulation of data, enhanced computing power and sophisticated machine learning algorithms, facial recognition began to be incorporated into more practical digital applications in recent years. Since 2010, Facebook has used facial recognition to detect the individuals in photos uploaded by Facebook users. In 2011, the Panamanian government and the US Secretary of Homeland Security Janet Napolitano collaborated to authorise a pilot programme for facial recognition platform. Compared with traditional manual recognition or other biological recognition technologies (such as iris or fingerprint recognition), facial recognition does not require complicated equipment and can function only with cameras, which makes it a more appealing technology.

Facial recognition also allows multiple derivative functions based on feature analysis. As a biometric recognition technology, facial recognition was initially used to verify identities in security departments or in device management for physical and logical access. With the implementation of cameras and developments of facial analysis, facial recognition has been further adopted for flow control, surveillance, emotional analysis (based on expressions), digital entertainment (e.g., deep fakes based on facial replacement) and personalised services (Li & Jain, 2011). Unlike auto-driving technology applied only in a limited driving scenario, facial recognition is a fundamental technology that satisfies multiple purposes in various scenarios.

Based on its wide potential applications, typology of facial recognition is critical for governance analysis. Based on function, facial recognition can be classified as facial recognition for verification, identification, categorisation, and live facial recognition[6]. Facial recognition for verification purposes refers to "one-to-one" image comparison, where users compare the collected facial images to a recorded image to verify the referential person's identity. Facial recognition for identification purposes is a "one-to-many" image comparison, where a collected facial image is run against a database or a watch list of facial images to identify whether the referential person is listed in the database or the watch list. Facial recognition for categorisation is used to extract information about an individual's characteristics to group them according to gender, age, nationality, expression/emotion and so forth. Potential bias or error may happen in the categorisation process and further mislead decisions based on the classification result. Live facial recognition is used where facial images are extracted from live video cameras deployed in public spaces. Individuals may not be aware that their facial images are being collected and matched against a watch list. Thus, live facial recognition can be dangerous as people are neither aware nor informed of the potential risks and cannot avoid being exposed to widespread closed circuit television (CCTV) cameras and ambient video connections.

Status Quo of Facial Recognition in China and India

Active Applications

To make full use of facial recognition, both China and India have actively applied this technology.

On the governmental level, Indian government has designed nationwide facial recognition programmes. In January 2018, the Unique Identification Authority of India (UIDAI) announced that it would allow the use of facial recognition as one of the authentication modes of the Aadhaar, a national biometric database managed by

[5] Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases and Latest News. *Thales.* Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

[6] European Union Agency for Fundamental Rights. (2019). Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement. Retrieved from https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

UIDAI for citizen authentication[7]. One year later, the Indian government approved the automated facial recognition system (AFRS) to identify criminals and missing children. The responsible institute, the National Criminal Records Bureau (NCRB), has released a tender for AFRS to technology companies[8]. Similarly, the Chinese government has adopted facial recognition in public services to determine eligibility for pension payments, searching for criminals, and so on[9]. Despite criticism from the media, governmental deployment of facial recognition has brought several social benefits because facial recognition is an effective tool for countries with a large population and can compensate for a shortage of administrative staff. In India, there is an average of 144 police officers for every 100,000 citizens, compared to 318 per 100,000 citizens in the European Union[10]. Police in India have used facial recognition systems to find thousands of missing and trafficked children (Cuthbertson, 2018; Nagaraj, 2020). Similarly, the Chinese police have used facial recognition to catch criminals and locate missing children. The Indian government has also implemented a facial recognition pilot project near rivers to prevent people, especially children, from drowning[11].

In addition to governmental uses, facial recognition has also seeped into daily life scenarios, such as access control, digital payments, financial operations, and username and password alternatives. For example, the Indian government partnered with airline companies to build Digi Yatra, which allows passengers to use facial recognition for check-in, security checks and aircraft boarding[12]. In China, people can finish digital payments or financial transfers (Alipay), log into social networking accounts (WeChat), and retrieve parcels from delivery lockers (Fengchao) by scanning their faces. New functions, like facial detection (detecting a person using their face in any input image or frame) and emotion detection (detecting the emotions on a face) are gradually being applied to provide customised services, like personalised healthcare, shopping recommendations in shopping centres and face-based entertainment activities (Roux, 2019; Tan, 2019)[13]. Facial recognition is thus becoming ubiquitous in China and India. According to a report, every Chinese person, on average, is exposed to cameras more than 500 times per day (Yang, 2019). In India, the combination of facial recognition with CCTV also enables constant facial recognition in everyday life (Murali, 2019).

The applications of facial recognition in China and India are quite active compared with the EU and the US, which have remained cautious in applying facial recognition. Three cities in the US, for example, have put bans or moratoriums on governmental uses of facial recognition (Conger, Fausset, & Kovaleski, 2019; Ravani, 2019; Lannan, 2019)[14]. Microsoft deleted the biggest open database for facial recognition, MS Celeb, due to

---

[7] Aadhaar (English: foundation or base) is a 12-digit unique identity number that can be obtained voluntarily by residents or passport holders of India, based on their biometric and demographic data.

[8] Retrieved from https://www.sundayguardianlive.com/news/india-worlds-largest-auto-facial-recognition-system-2021

[9] Retrieved from https://www.sohu.com/a/245448721_100129841

[10] Retrieved from https://edition.cnn.com/2019/10/17/tech/india-facial-recognition-intl-hnk/index.html

[11] Anti-Drowning Facial Recognition Cameras Warn Kids not to Swim. *Sixth Tone*. August 30, 2018. Retrieved from https://www.sixthtone.com/ht_news/1002850/anti-drowning-facial-recognition-cameras-warn-kids-not-to-swim

[12] Digi Yatra—A New Digital Experience for Air Travellers. Retrieved from https://www.india.gov.in/spotlight/digi-yatra-new-digital-experience-air-travellers

[13] See "Creating Smarter Stores with Facial Recognition." *VIA Tech*. August 22, 2018. Retrieved from https://www.viatech.com/en/2018/08/facial-recognition-smarter-stores/; NEC "Improving Customer Interaction Through Greater Situational Awareness." Retrieved from https://www.necam.com/AdvancedRecognitionSystems/CustomerExperience/; Your Guide to Facial Recognition Technology in Healthcare. *The Medical Futurist*. November 19, 2019. Retrieved from https://medicalfuturist.com/your-guide-to-facial-recognition-technology-in-healthcare/. In 2019, one popular app Zao, using deep fake technology to replace actors' faces in videos with users' faces automatically. The app is banned shortly after, as it forces users to share their data in user policies.

[14] San Francisco, Summerville, and Oakland ban the use of facial recognition by law enforcement and other agencies, citing the technology's propensity to endanger civil rights as a major concern.

compliance concerns. In the EU, certain uses of this technology, such as in high schools for facial-recognition-based attendance registry, have constituted violations of General Data Protection Regulation (GDPR) (Edvardsen, 2019)[15].

Risks and Concerns

Despite its widespread application, facial recognition is still a risky technology. Multiple issues that have arisen are discussed in the following sections.

Privacy-intrusive uses. Wide application of facial recognition enables companies to collect individuals' data in daily scenarios, which infringes on privacy protection in the Digital Age. The risk involves two aspects.

Firstly, facial images collected through facial recognition technology are sensitive personal data that can directly help in identifying certain data subjects. As facial features are necessary for comparison, users of facial recognition cannot anonymise relevant data to avoid privacy infringements. The biometric databases formed in facial recognition therefore put data subjects' privacy at risk.

Secondly, knowledge and consent are seldom obtained in facial recognition practices. According to a study of several cities in China (including Beijing and Linfen), over 41% of interviewees agreed to use facial recognition and believed it could help improve security; still, approximately 40% held negative attitudes (the remaining interviewees were neutral)[16]. In 2018, one professor sued a zoo because it forced visitors to use facial recognition for authentication. The court held that the collection of information needs to be "lawful, just, and necessary", and the zoo's collection of facial images violated the requirement of necessity. The zoo was then ordered to delete facial information[17]. The Aadhaar, which collects facial recognition data in India, also faced many litigations against its linkage to compulsory public services[18]. The courts held that mandatory uses or refusal to provide services when people refuse to use Aadhaar are illegal. Privacy risks grow when applications use live facial recognition, in which individuals' data are collected unconsciously.

Errors and bias. Although facial recognition's accuracy has been improved in laboratory tests, its accuracy in practice is highly unstable and depends on equipment and algorithms. Traditionally, facial recognition works on 2D images to conduct feature extraction and comparison, which can be easily cheated (Xue, 2019). In a recent case in China, Fengchao Express used 2D facial recognition to enable receivers to open smart cabinets and take out their parcels by scanning their faces. Some students hacked the cabinets by simply using photos to replace the real person (Xue, 2019). A 3D model that includes information about facial geometry and gives a more accurate representation of facial features may help to solve such problems (Abate, Nappi, Riccio, & Sabatino, 2007). Equipment that uses low-pixel images reduces images' precision and leads to poor accuracy (Dixit, 2019). As mentioned, the convolutional neural networks that can improve accuracy only appeared five years ago and are not widely implemented[19].

---

[15] For example, the Swedish government fined a high school for its facial-recognition attendance registry as a violation of GDPR. The data protection authority for France, CNIL, declared it illegal to use facial recognition in schools based on privacy concerns. See "CNIL Bans High Schools' Facial-Recognition Programs." *IAPP*. October 29, 2019. Retrieved from https://iapp.org/news/a/cnil-bans-high-school-facial-recognition-programs/

[16] Ethics research group of Nandu artificial intelligence. (2019). Observation Report of Face Recognition Landing Scene (2019) (南都人工智能伦理课题组，人脸识别落地场景观察报告（2019）) (in Chinese).

[17] "Guobing v. Hangzhou Wild Zoo Co." civil judgement of the first instance (2019). Zhe 0111Min-Chu No.6971 (郭兵与杭州野生动物世界有限公司服务合同纠纷一审民事判决书（2019）浙 0111 民初 6971 号) (in Chinese).

[18] See "Kharak Singh vs. State of UP" and "M.P Sharma vs. Union of India", "Binoy Viswam v. Union of case India".

[19] NLST. (2018). NIST Evaluation Shows Advance in Face Recognition Software's Capabilities'. Retrieved from https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities

In addition to varying accuracy, bias raises additional concerns. NIST has confirmed that most algorithms exhibit demographic differences for both false negative rates (rejecting a correct match) and false positive rates (matching to the wrong person) (Grother, Ngan, & Hanaoka, 2019). Algorithms may exhibit biases based on gender, race, age, complexion and so on for two main reasons. Firstly, there is a lack of diversity in training data (that is, there is inadequate training data for certain groups, such as females and senior citizens). Secondly, there is bias in the watch lists that facial recognition matches against. If certain groups are over-represented in databases, the algorithm may identify and track people of those groups more frequently (Crumpler, 2020). The issue of facial recognition bias is critical for places where multiple nationalities coexist.

Amplified downstream consequences in automatic facial recognition systems. As facial recognition has developed, further operations and decisions have followed. For example, banks use facial recognition for identity verification to authorise financial transactions, and police use it to identify suspects and make arrests. The combination of facial recognition and further operations or decisions is even more evident in the Internet Age, where many real-world activities have been moved online and facial recognition has become the first step of authentication for numerous operations.

The connection of facial recognition with further operations or decisions could extend the effects of unreliable accuracy and lead to severe downstream consequences. Several cases in China have exposed these risks, where defendants either stole personal images to deceive Alipay's (digital payment app) face verification[20] or hacked face verification technology in bank apps[21]. The connection also presents the possibility of entrenching discrimination by flagging certain features as high risk or in need of further scrutiny.

Governmental surveillance and chilling effect. Governmental application of facial recognition—especially live facial recognition—may trigger fears of a power imbalance between the state and citizens because it enables governments to conduct camera-based surveillance. Governmental uses of facial recognition in certain scenarios like demonstrations may also lead to a chilling effect whereby individuals refrain from lawfully exercising their freedom of assembly and association due to fear of negative consequences (Ulmer & Siddiqui, 2020). With ubiquitous facial recognition technologies, people may change their behaviour, withdraw from social life, avoid visiting places under surveillance and so on, which weakens their capacity to live a dignified life. Although the Chinese and Indian governments have successfully used this technology to find lost children, detect criminals and improve service efficiency, the negative side effects of governmental surveillance are also worth attention.

Governance Dilemma of Stability Versus Growth

The AI era presents opportunities, as well as challenges. Using the opportunities of AI by actively applying facial recognition also creates the issues described above. Essentially, this dynamic is an extension of the stability versus growth dilemma that AI developers and governments have faced over the years (Kewalramani, 2018).

Choices of the EU and US. Hesitating between active application and total bans, the EU allows certain uses of facial recognition with ex-ante control. In drafting the White Paper on Artificial Intelligence, the EU

[20] Zhejiang Qvzhou Intermediate People's Court. (2019). Zhe 08 Xing-Zhong No. 333 (浙江省衢州市中级人民法院（2019）浙 08 刑终 333 号刑事判决书) (in Chinese).

[21] Fujian Xiamen Siming People's Court. (2019). Min 0203 Xing Chu No. 890 (福建省厦门市思明区人民法院（2019）闽 0203 刑初 890 号刑事判决书) (in Chinese); Fujian Xiamen Intermediate People's Court. (2019). Min 02 Xing Zhong No. 749 (福建省厦门市中级人民法院(2019)闽 02 刑终 749 号刑事裁定书) (in Chinese).

proposed a temporary five-year moratorium on uses of facial recognition by public and private entities (Stolton, 2020), which was later removed due to fears that the moratorium would stifle innovation and compromise national security (Espinoza, 2020). Instead, the EU finally classified facial recognition as a high-risk technology requiring prior assessment (including extra testing, certification and human oversight) before application[22]. Several countries are now conducting tests of facial recognition to prepare for government uses (Fussey & Murray, 2019) [23].

Although some cities, like Somerville and San Francisco[24], have put moratoriums on governmental uses of facial recognition, the US generally allows uses of facial recognition and puts more restrictions on commercial uses. Legislation at the state level, such as the Illinois Biometric Information Privacy Act (BIPA), Texas Biometric Privacy Act (2009) and Washington Biometric Privacy Protection (2017, known as Washington House Bill 1493), have put restrictions on the use of biometric recognition by private entities. Recently, there has been a move to introduce a national law called the "Commercial Facial Recognition Privacy Act of 2019" to restrict the private collection, use and sharing of facial recognition data without adequate notice and affirmative consent. The bill also seeks to prohibit the use of data to discriminate against a person or to repurpose it[25].

In commercial practices, although some companies have declared to stop using facial recognition, there are some other considerations behind such decisions that cannot be regarded as purely legal or ethical. For example, IBM declared that it would stop selling facial recognition related services[26]. However, it is also worth noting that it only declared that it would abandon general facial recognition business, which does not bring much revenue for IBM.

In conclusion, despite negative attitudes among citizens and the media, governments in the EU and US are exploring the possibility and feasibility of using facial recognition. The uses of facial recognition are allowed given the preconditions of privacy protection and with strong technology support.

Choices of India and China. As discussed, China and India have applied facial recognition in the private and public sectors.

Although the uses of facial recognition include risks of privacy infringement, errors and bias, and potential governmental surveillance, they also bring improvement on security management and other benefits. Social tolerance of these risks and acceptance of new technologies change with society and technology development and positively correlate with the benefits of using this technology (Bratman, 2002; Prosser, 1960; Solove, 2008;

---

[22] European Commission. (2020). White Paper on Artificial Intelligence—A European Approach to Excellence and Trust. COM(2020) 65 final, Brussels.

[23] For example, the police in the United Kingdom performed several tests in real-life situations, such as sports events, even using real watch lists. Other law enforcement agencies tested the accuracy of the technology in larger tests with volunteers, such as the police in Berlin, Germany or in Nice, France.
See South Wales Police's website. Facial Recognition Helps South Wales Police Become Smarter, Creating a Safer and Connected Community. Retrieved from afr.south-wales.police.uk/; Big Brother Watch. (2019). Joint Statement on Police and Private Company Use of Facial Recognition Surveillance in the UK; and Big Brother Watch. (2019). Face Off Campaign.

[24] Ordinance: Banning the usage of facial technology surveillance in Somerville. Amended in Committee 5/6/19 File No. 190110 Ordinance No. Administrative Code—Acquisition of Surveillance Technology (Stop Secret Surveillance Ordinance (05/06/2019)).

[25] While an official version of the bill has not yet been published, an unofficial version is available online at https://www.scribd.com/document/401931553/The-Commercial-Facial-Recognition-Privacy-Act

[26] See "IBM CEO's Letter to Congress on Racial Justice Reform." *IBM*. June 8, 2020. Retrieved from https://www.ibm.com/blogs/policy/facial-recognition-susset-racial-justice-reforms/

Westin, 1967; Schwartz, 2020)[27]. For policy makers, the main work is to minimise risks and promote legal uses while maximising social benefits. To do this, both China and India need to build a systematic governance approach targeting current applications and utilising local regulatory bases. Lack of proper governance may open the door to technology abuses and lead to blind optimism.

Proposed Governance of Facial Recognition

Based on facial recognition practices in China and India, this section proposes a governance structure for facial recognition focusing on two elements. On the one hand, regulators need to ensure that individuals have the ability to protect their rights to privacy and personal data against intrusive uses of facial recognition. On the other hand—and more importantly—regulators should stand out to regulate participants' behaviours. Participants in the industry of facial recognition include software developers, manufacturers of hardware products (e.g., cameras and image collectors), programme designers and end-users who apply facial recognition in their products and services (including both private companies and public institutions). These participants shall be the main objects for facial recognition governance, and regulators shall form a comprehensive governance system using mechanisms beyond legislation.

Individual Protection

Protection of privacy and personal data. Privacy and personal data protection offers individuals the right to sue for the illegal collection and use of their information, including the use of facial recognition without their consent. The protection and implementation of these rules determine whether individuals can protect themselves against intrusive uses.

Personal control in the EU and US. The protection of privacy and personal data mainly originated from the EU and US, and their experiences provided references for China and India[28].

In light of digitalisation and AI development, the EU protects individuals by offering data subject rights. The rights to be forgotten and data portability in the GDPR equips data subjects with the ability to control the uses of their personal data. In addition, informed consent for data collection and the requirement to promise data access also enhance data subjects' control over their information.

The US is devoted to promoting market development for data uses in the Digital Age and solves privacy infringement issues based on the value of protecting basic human rights. The right to privacy in the Constitution[29] and in legislation with supported precedents[30] enables individuals to bring lawsuits against entities that infringe this right. Informed consent is the precondition for data uses and collection. Some state-level legislation also supports private lawsuits against the illegal collection and uses of personal data. For example, the BIPA permits a private cause of action to collect biometric data without informed consent (Kracht, Mueller, Sotto, & Sterns, 2018)[31]. In January 2019, the Illinois Supreme Court in "Rosenbach v. Six Flags

---

[27] For example, the concept of privacy always changes with the development of technologies.

[28] Both proposed bills in China and India emphasize the importance of data subjects' consent for data collection and provide rights to exert personal-control, taking reference from GDPR and US rules.

[29] Relevant rights on facial recognition include Article 2 of the 14th Amendment (non-discrimination), Article 6 and Article 7 of the 14th Amendment (equal protection), Article 12 of the 4th Amendment (privacy), and Article 19 of 1st Amendment (speech).

[30] Relevant cases see "Griswold v. Connecticut", 381 U.S. 479 (1965); "Roe v. Wade", 410 U.S. 113, 153 (1973).

[31] Other bills allowing private right of action for violation of its biometric data privacy laws, include Biometric Information Privacy Act, 2017 Bill Text MI H.B. 5019; 2017 Bill Text NH H.B. 523 (Enacted on 15 May 2018); 2017 Bill Text AK H.B. 72; 2017 Bill Text MT H.B. 518.

Entertainment Corp." held that the plaintiffs do not need to suffer actual harm to sue under BIPA, further facilitating individuals' ability to initiate lawsuits.

In conclusion, privacy protection rules in the EU and US give individuals control over their personal data and information through three methods: (1) offering data subjects the right to control their data, (2) demanding informed consent for data collection and uses and, (3) allowing private prosecutions. These three elements constitute the foundation of the personal control model for data and privacy protection in the Digital Age and influence other jurisdictions in establishing relevant rules.

Current rules in China and India. Although China does not expressly protect privacy at a constitutional level[32], Article 110 of the Civil Code stipulates the right to privacy when listing all civil rights. As a general rule, it does not offer guidelines or requirements beyond listing the rights themselves. Article 1032 and Article 1034 of the Civil Code provide the right to privacy and the protection of personal information. More enforceable and detailed rules that protect individuals' privacy are reflected in department laws. For example, Articles 29, 50 and 56 of the Consumer Protection Law, Articles 12 and 45 of the Cybersecurity Law, Articles 20 and 30 of the Law on Commercial Banks and Article 1226 of the Civil Code outline confidentiality and non-intervention obligations for sellers, Internet service providers, financial institutions and hospitals. Individuals can sue for the breach of these obligations or privacy infringement as consumers, users or patients. In addition to privacy rights, individuals can also use portraiture rights to sue for the illegal collection and use of facial images[33]. Realising the emerging risks of privacy infringement and of the misuse of personal information in the Digital Age, legislators and scholars have worked to establish more systematic protection of privacy and personal information.

In India, the right to privacy was established in a judicial case which expanded the interpretation of the Indian Constitution. The Hon'ble Supreme Court of India declared in "Justice K.S. Puttaswamy (Retd) and Anr. v. Union of India" that the right to privacy is a fundamental right enshrined in Article 21 of the Constitution of India[34]. This case explicitly overruled previous judgments of the Supreme Court in "Kharak Singh vs. State of UP" and "M.P Sharma vs. Union of India", which held that there is no fundamental right to privacy under the Indian Constitution. However, according to Article 21 of the Constitution, the fundamental right to privacy is enforceable against the state and its instruments. Enforcing the right to privacy against private entities, according to the Supreme Court, may require legislative intervention[35]. The draft of the Personal Information Protection Law lists the right to delete one's information, the right to ask for explanation and the right to correct data.

Most privacy protection rules in India are scattered throughout department laws (opposed to the Constitution). Section 47 (ix) of the Consumer Protection Act (2019) provides relief to individuals whose personal information has been misused. According to the Information Technology Act (IT Act, 2000), facial images constitute sensitive personal data and are subject to restrictions for collection and use. Disclosure of personal information without the person's consent and negligent collection and handling of sensitive data are

[32] Many rules of Constitution Law in China are relevant to privacy protection. For example, the protection of personal dignity (Article 38), right against the unlawful search of, or intrusion into citizens' residence (Article 39), freedom of correspondence and secrecy of correspondence (Article 40) are connected with privacy protection.

[33] Article 110 of the Civil Code.

[34] Writ Petition (Civil) No. 494 of 2012.

[35] Article 21 of Indian Constitution Law "Protection of life and personal liberty—No person shall be deprived of his life or personal liberty except according to procedure established by law".

penalised under the IT Act[36]. However, obligations under the present laws only apply to "corporate" and therefore exclude most instances where government agencies interact with biometric data using facial recognition. The proposed Personal Data Protection Bill 2019 lists further rights, like the right to data portability and the right to withdraw consent.

Current rules in China and India focus on enabling individuals to sue against illegal data uses. Regulators have enhanced individuals' ability to control their information by guaranteeing new rights and requiring consent as a precondition. Such efforts also have taken their cue from approaches of the US and EU.

Beyond personal control of privacy and personal data protection. However, promising individuals the right to control their data is not enough to protect them in facial recognition scenarios. Firstly, given that live facial recognition collects people's data without their knowledge, people cannot exert control because they are unaware that their data is being collected. Secondly, individuals may face cognitive obstacles in deciding whether to use facial recognition and provide their facial image or not. To provide adequate information to individuals for data collection (e.g., the scope of collected data and future uses), product and service providers need to compile long and complicated user policies that are difficult for ordinary people to understand. Although measures have been taken to shorten and simplify user policies, the improvement in comprehension is limited (Calo, 2012; Sherman, 2018)[37]. Even with well-written user policies, free or essential services will lure users into submitting their facial images regardless of potential risks. Thirdly, individuals have little power in suing powerful facial recognition participants. As most participants are large institutions with professional lawyers and financial support, individuals may face obstacles in finding evidence due to the significant information asymmetry between big institutions and individuals.

In conclusion, requiring informed consent for data collection, providing data subject rights, and allowing private cause of action may not truly confer individuals with effective control over their data and privacy. In fact, once participants obtain data subjects' consent, the knowledge and consent requirements may become a shield for participants to use the collected data. As such, many scholars have called for adjustments of current laws to address the issues of the personal control model in privacy and data protection (Solove, 2013; Schwartz & Peifer, 2017).

To overcome the obstacles of personal control, legislators should enact changes including reversing the burden of proof to force participants to submit relevant evidence[38], removing the requirement of proving loss to offer damages following privacy infringements and promoting public interest actions/class actions in the field of privacy and data protection. In addition, scholars should incorporate cognitive study in designing knowledge and consent rules.

Participants' Regulation

Law enforcement and professional institutions may be better positioned than individuals to detect and regulate participants' infringing behaviours. Regulators, therefore, should focus more on regulating big companies and institutions that use facial recognition as industrial participants rather than equipping individuals

[36] Section 72A and section 43A of IT Act.

[37] Calo, M. R. (2012). Against Notice Skepticism in Privacy (and Elsewhere). *NOTRE DAME L. REV.*, *87*(3), 1027. (Studies show only marginal improvement in consumer understanding where privacy policies get expressed as tables, icons, or labels, assuming the consumer even reads them.).

[38] The reversion of burden of proof has been used in other cases, like trade secret disputes, where the plaintiff is hard to obtain proof from the defendants. See Article 32 of China Anti-Unfair Competition Law.

to fight against them. Considering the misuse of facial images in the facial recognition industry, legislation should place obligations on data collectors and users regarding the use of facial recognition and entitle professional institutions to detect and deter illegal uses. The magnitude of these obligations depends on the sensitivity of the data and the risks of the technologies involved. India has made an effort in this direction through Article 26 of the India Personal Data Protection Bill, which proposes a concept of data fiduciary based on the quantitative sensitivity of the personal data to be processed and the risks of the technology adopted. According to Articles 26–28, data fiduciaries shall undertake protection assessments, periodic reviews of data protection measures and audits of data policies and behaviours, as well as establish professional data agencies. Similarly, China has placed multiple data obligations on big collectors in the Internet. The Cybersecurity Law (2016) and the proposed Measures for the Administration of Data Security, for example, place obligations on network operators to protect users' personal information and to allow administrative institutions to impose relevant regulations. This tendency of shifting regulating focus to technology users should be followed in the field of facial recognition.

A broader scheme of participants' regulation and the role of law inside. Legislation has always been a powerful tool in regulating behaviours, but it faces limitations in AI governance. According to Gasser and Almeida (2017), rules in AI governance can be classified into three layers, namely technical, ethical, and social and legal, which form in chronological order (see Figure 2). They pointed out that as the legal layer concerns the most fundamental rules for legal matters in AI industries (liability distribution for AI infringement, legal status of AI, etc.), rules in this layer are formed at a later stage when the technologies have been widely applied and the legal relationships are clear enough for legislators to adjust. Therefore, legislators shall place legal rules on uses of facial recognition only when the risks and solutions are clear. In light of the rapid evolution of facial recognition, state laws cannot provide many fixed rules because of changing practices (Gasser & Almeida, 2017)[39], nor can states overcome the long legislative hearing process to apply quick responses to emerging issues.

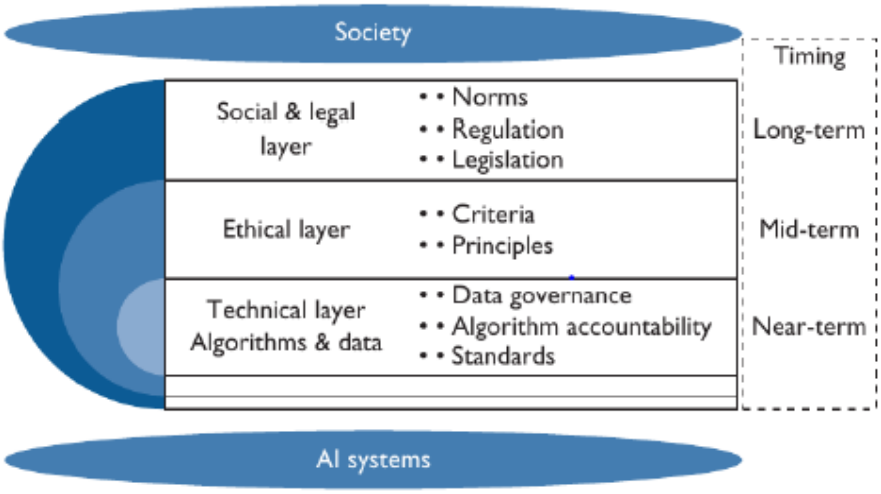

Figure 2. Layered model for AI governance (Gasser & Almeida, 2017).

[39] As rules in social & legal layer concerns the most fundamental rules adjusting new legal relationships brought by AI (liability distribution for AI infringement, legal status on AI, etc.), they will form later when the technologies have been widely applied, and market interests are clear for legislations to adjust.

To compensate for the defects of state legislation power, Colin (2004) proposed "the post-regulatory state", which shifts the focus of analysis from state law to the broader range of norms and mechanisms through which control is asserted or achieved indirectly. Such norms vary from minimum standards for codes of conduct and corporations' internal rules to institutional reviews and tests. The matrix of hierarchical regulation power further extends from legislators, courts and government institutions to industrial associations, standard-setting organizations, agencies (e.g., accreditation bodies, credit rating agencies) and private companies (Colin, 2004)[40]. The norms and multiple players avoid the elaborate procedures and high social costs of legislation and form part of a broader scheme of regulation that includes behaviour-monitoring and -modifying mechanisms.

Legislation may have a new role in the post-regulatory state. Although laws may face difficulties in regulating behaviour directly, they can regulate behaviour indirectly (Lessig, 1998). Specifically, legislators can exert legal liabilities on companies to force them to conduct self-regulation, and authorize institutions to exert *ex officio* powers to conduct accreditations and reviews, which are discussed in the following sections.

Participants' regulation: enforced self-regulation. ***Benefits and issues of companies' self-regulation.*** Companies enjoy more advantages in dealing with emerging issues of facial recognition. With technology personnel, companies have a greater technical capacity to spot problems, explore improvements that can reduce issues (e.g. errors, bias and security) and promote responsible uses of facial recognition technology (Crumpler, 2020). Apple, for example, has proven that it is technically feasible to run machine-learning models of facial recognition on a device rather than in the cloud (Portnoy, Gebhart, & Grant, 2016), which enables users to keep personal data locally and avoid granting access to developers. Apart from technical advantages, as market players, companies also have the latest information about technical and industry development, enabling them to make quick adjustments within the fast-changing industry and to avoid procrastinations.

However, companies' self-interested nature and short-sightedness prevent them from voluntarily solving technology defects, taking security measures, and ceasing infringing activities. Firstly, most right-infringing activities, such as selling image data and using cheap but unstable technologies, carry alluring short-term benefits. Although in the long term such activities cause legal risks and reduce service quality, these can be ignored due to companies' short term goals or desire for quick money. Secondly, additional security measures limit companies' opportunities to use data and add extra costs by imposing more limitations and requiring extra work. For example, as mentioned above, although running facial recognition on local devices instead of through the cloud can improve data security, it also requires business operators to renounce the default model of using the cloud for large-scale data processing, which helps companies to collect data and speed up services. Thirdly, improving technical accuracy demands more cost. For example, using diversity data for algorithm training can help avoid potential bias and improve the accuracy of facial recognition, but it demands more costs and time for data collection. In conclusion, companies are not well-positioned to make the trade-off between losses and gains in using facial recognition technology.

Legal pressure for enforced self-regulation. Regulators should put extra legal consideration into forcing AI developers and adopters to incorporate safety features and to internalise the external costs of AI systems

[40] For other papers discussing the importance of private or social institutions in controlling risk-related behaviour, see Anleu, S. L. R., Mazerolle, L. G., & Presser, L. (2000). Third-Party Policing and Insurance: The Case of Market-Based Crime Prevention. *Law and Policy, 22*, 72; Heimer, C. (2001). Insuring More, Ensuring Less: The Costs and Benefits of Private' Regulation Through Insurance. In T. Baker and J. Simon (Eds), *Embracing Risk: The Changing Culture of Insurance and Responsibility*. Chicago: Chicago University Press; Richardson, B. J. (2003). Diffusing Environmental Regulation through the Financial Services Sector: Reforms in the EU and Other Jurisdictions. *Maastricht Journal of European and Comparative Law, 10*(3), 233-264.

(Scherer, 2016). By establishing an enforced self-regulation system, regulators can require participants to place data protection and non-discrimination requirements at the centre of their technical specifications (Braithwaite, 1982; European Union Agency for Fundamental Rights, 2019)[41].

The most potent tool for the enforced self-regulation model is legal liability. In the field of intellectual property, assigning legal liability to Internet service providers (ISPs; e.g. YouTube, Baidu Wenku, Facebook) for not performing minimum due obligations has helped to force ISPs to deter online piracy and develop internal regulations to prevent users from uploading pirated works. To combat rampant online piracy and counterfeiting, Article 1195 of the Civil Code and Article 45 of the E-Commerce Law in China place indirect infringement liability on ISPs for not paying enough attention to checking their platforms' content. Leading online platforms, such as Taobao, Baidu Wenku, and so on have developed AI technologies and complaint systems to detect infringing content and reduce online piracy in fear of possible liability. With proper legal pressure, practitioners could develop technology solutions against infringement.

In the field of facial recognition, legal pressure can be exerted through joint liability. Although upstream participants, like software developers, manufacturers of hardware products, and programme designers do not infringe individuals' rights, they provide tools and financially benefit from downstream uses that may infringe individuals' rights. Legislators can exert joint liability on upstream designers for downstream infringement uses when they develop technologies with the knowledge of technical defects or that enable infringement. Under such legal pressure, technology companies will tighten supply chain management and focus on developing technology solutions that minimise illegal uses (Scherer, 2016)[42]. In addition, the liability for end-users who apply facial recognition without individuals' consent or use technologies with high bias should also be covered in legislation.

Guidelines for participants: Technology standards. In addition to legal pressure, it is necessary to provide references for involved parties regarding technology design and uses. The Chinese government actively establishes technology standards for practices. Starting in 2011, the Chinese National Information Security Standardisation Technical Committee (TC 260) and the Telecommunication Terminal Industry Forum Association (TAF) have made several technical standards concerning uses of facial recognition (see Figure 3) (Price, 2018; Kewalramani , 2018)[43].

Rather than establishing general rules for practical disputes, technical standards provide detailed technical requirements and direct instructions for developing and using facial recognition. The standards effectively set out the best practices expected by regulators and supplement China's existing data protection rules, which are more general without detailed guidelines.

---

[41] Braithwaite proposed enforced self-regulation model for corporate crime control, this paper transport the idea of enforced self-regulation to technology governance. European Union Agency for Fundamental Rights holds that legal pressures and outsource pressure could be used to influence companies' behaviours.

[42] Scherer proposed to create a liability system under which the designers, manufacturers, and sellers of agency-certified AI programs would be subject to limited tort liability, while uncertified programs that are offered for commercial sale or use would be subject to strict joint and several liability.

[43] Not restricted in the domestic market, China also promotes the international standard establishment. In April 2018, the First Meeting of an International Committee held in Beijing set up voluntary international standards on AI. However, the questions are whether facial recognition is the proper area to build industry standard without compulsory effect and whether the international relationship will affect the participation of other countries. As pointed by Takshashila Institution, the impact of such early steps in China's march for leadership in AI standards is likely to be limited if the nationalistic narrative and security concerns grow prominent.

Releasing institution	Standard's name	Content
TC 260	Information Technology—Personal Information Security Specification (GB/T 35273-2020)	Provide the definition of and collection rules for personal sensitive information.
TC 260	Public Security—Face Recognition Application—Technical Requirements for Face Images (GB/T 35678-2017)	Provide requirements for the format, content and comparison of images.
TC 260	Information Technology—Biometric Identification Data Interchange Format (GB/T 33767.5-2018)	Provide the requirements on the uses of biometric data.
TAF	Security Evaluation Method on TEE Based Mobile Device Face Recognition (TAF-WG4-AS0026-V1.0.0:2018)	Provide measures to avoid data tampering, the requirement of disclosure and anti-fake tests.

Figure 3. Technical standards concerning uses of facial recognition.

However, there is still much room for improvement under existing standards. Current standards mainly focus on the protection of personal data and anti-fake tests, without addressing issues of unstable accuracy rates and potential bias. Future standards need to provide minimum accuracy rate requirements for different activities based on their importance and risks and could alleviate potential bias by establishing bias tests and diversity requirements (age, gender, ethnicity, etc.) for training data (Crumpler, 2020)[44]. In addition, current standards are national recommended standards and are not binding for participants[45]. To enhance their influence, court judges could use these standards as a reference in deciding whether involved parties in a lawsuit have paid due diligence.

Participants' regulation: Institutional regulation. Governments should play a more important role in regulating the uses of AI technologies as there are no fixed practices and the technologies are still under development. Specifically, the governments can act to provide environments for technology development, promote industrial collaborations, and conduct necessary security tests and reviews. Governmental practices in the area of self-driving cars present a successful model for government regulation of AI technologies. In China, the Ministry of Transport, the Ministry of Industry and Information Technology (MIIT), and the Ministry of Public Security (MoPS)[46] have enforced multiple rules related to granting test licenses and setting up test zones covering players from the Internet and Connection Technology (ICT) and mobile Internet business.

However, neither China nor India has a clearly responsible department to regulate the uses of facial recognition technology. Current departments relevant to facial recognition are mainly data protection departments. In China, the Cyberspace Administration of China (CAC), the MIIT, and the MoPS conduct reviews of personal data protection in online apps (Luo, 2017)[47]. TC 260, as mentioned above, released technical standards concerning the uses of facial recognition, but most of which mainly focus on the collection and use of facial images. In India, the Ministry of Electronics and Information Technology (which administer the IT Act) and UIDAI (which manages Aadhaar) are entitled to regulate the use of facial recognition when

[44] EU, for example, recently proposed that a regulatory framework for high-risk AI systems like facial recognition, includes requirements that training data be "sufficiently broad", and reflect "all relevant dimensions of gender, ethnicity and other possible grounds of prohibited discrimination". Training data audits to confirm the quality of training datasets could become an important tool for addressing the risks of bias in facial recognition.

[45] Standards in China start with "GT/B" refer to national recommend standards that have no compulsory effect.

[46] See Security released the Specification for Road Test Management of Intelligent Network Vehicle (Trail) (《智能网联汽车道路测试管理规范（试行）》(in Chinese)), released by the three departments which clarify the division of regulation.

[47] In 2017, the CAC, the MIIT, the MoPS, and the National Information Security Standardization Technical Committee (NISSTC) reviewed the privacy protection of over 10 major online products. One year later, experts group leading by NISSTC conducted the second round review for over 40 products' privacy clauses.

participants leak or illegally use personal data. The Indian Personal Data Protection Bill also proposes the creation of a Data Protection Authority of India entitled to regulate data uses.

The currently disjointed administrations are not adequate for dealing with the multiple issues of the facial recognition industry. Firstly, current administrations only regulate personal data protection, while low accuracy, potential bias and the risks of governmental surveillance are left without regulation. Secondly, as administrations also need to regulate the governmental uses of facial recognition, there are no measures to keep independence of such administration. The close connection of the regulating administration with governmental departments who use facial recognition technology shall prevent the administration from engaging in effective and fair supervision. Thirdly, unlike the area of self-driving cars, where the technology only be applied in one industry, facial recognition is applied across communication devices, public transportation hubs (train stations, airports, etc.), online services (e.g., digital payment platforms, social media networks), enforcement tools (e.g., policies), and public service providers. The widely scattered applications bring additional obstacles to comprehensive and systematic regulation and necessitate a more specialised institution.

Establishing an independent institution and its requirements. It is necessary to establish an independent institution for the close monitoring and comprehensive regulation of emerging technologies, especially facial recognition.

This institution can perform tests or regular reviews about technical accuracy, bias risks and security issues and can promote cooperation among institutions to deter illegal uses. Legislators and administrative systems need to authorise an institution or workgroup to conduct inspection and enforcement activities. An independent institution can also support the establishment of self-regulations for facial recognition participants, as well as release and update technical standards as references.

Such an institution requires specialisation and expertise to deal with technical issues, as well as independence in order to make objective decisions and maintain neutrality.

Specialisation and expertise are essential for dealing with technical issues. The institution or workgroup should recruit experts on relevant technologies with practical experience and should collaborate with outside practitioners to stay up-to-date on emerging and changing technologies.

Independence is also critical to ensure that the institution can "not only solve problems but [can] rely on neutral criteria for the solution of problems" (Hart, Jr. & Sacks, 1994) to prevent influence from lobby groups or governmental departments that use facial recognition. Independence can be achieved by keeping financial and human resource management independent from other government departments. However, such independence comes at the price of alienation from other institutions, which may lead to obstacles in collaborative enforcement. Administrative enforcement plays a vital role in cracking down on illegal uses of facial recognition as it is efficient and flexible[48]. Compared with individual lawsuits and criminal prosecutions, administrative authorities have resources for activity detection, proof collection, and damage tracing and have flexible tools covering from heavy penalties, removal of the product from shelves to service moratoriums. As facial recognition is used in multiple areas, cross-department cooperation for administrative enforcement is necessary for cross-industrial regulation. Entitlement to conduct enforcement activities and fixed collaboration

[48] Chinese government traditionally used "campaign-style" enforcement to solve infringing content in online platforms and the typical example would be "Sword Net Action" series aiming on cracking down internet piracy content. The success story proves the strong power for administrative authorities to against scattered and anonymous infringement activities.

obligations and mechanisms are also necessary. Thus, it is critical to establish department-level coordination and a comprehensive governance framework to oversee facial recognition deployment.

Participants' regulation: confronting potential public & private surveillance partnership. While it is necessary for the government to establish regulations for risky technology, the fact that the government can use facial recognition for its own surveillance purposes creates a disincentive to conduct effective regulations[49]. This dynamic is more important for China and India where the governments have widely implemented facial recognition with technical companies' help[50]. Such cooperation underscores the deep linkages between private enterprises and the state in terms of facial recognition.

For governmental uses, non-discriminatory regulations are insufficient. The last section highlighted the importance of independence for the regulatory institution to avoid external influence. The institution shall non-discriminately review and assess the uses of facial recognition by private and public entities. As governments use facial recognition in law enforcement activities, errors may lead to the arrest of innocent people; hence, the requirements for accuracy rate and bias risks in governmental uses should be higher than in other uses.

In addition to the higher requirements and non-discriminatory regulations, transparency is critical for governmental uses of facial recognition. As states may seek to exempt themselves from regulation by turning to the rhetoric of an emergency situation (i.e., the need for broad powers to respond quickly to a fast-developing situation, etc.), external supervision is necessary to assess the rationality of those exemptions. Therefore, transparency and detailed information disclosure for governmental uses is necessary to implement social supervision and accountability. Disclosure includes the scope and restrictions of facial recognition uses, technical specifications and parties involved. The public tender for AFRS in India includes a disclosure requirement, and sustained disclosure of the implementation and application process is also necessary to reduce any possible public and private collusion. The Chinese government should also take measures to build an information disclosure system. Sufficient information is a precondition for public supervision.

Conclusions

This paper discussed the potential issues that may expose in applying facial recognition, which cover problems with privacy and data protection, unstable accuracy rates, potential bias, amplified downstream consequences in automatic facial recognition systems and risks of government surveillance. China and India need to integrate multiple norms and rules to form a comprehensive and systematic regulation for using new technologies. In addition to enhancing personal protection, policymakers should emphasise direct control over participants. This paper aims to start a discussion regarding the regulation of technology applications by outlining potential issues and a sector-specific governance framework. More conversation is expected in this area on issues like the intervention of autonomy, political influences and boundaries between privacy and security[51].

---

[49] The Public/Private Surveillance Partnership. *Schneier on Security*. August 5, 2013. Retrieved from https://www.schneier.com/blog/archives/2013/08/the_publicpriva_1.html

[50] The cooperation of governments and private corporations has become a common practice in facial recognition industry. Indian NCRB released a tender for an Automated Facial Recognition System to seek cooperative corporations. In China, private companies, like Hangzhou Hikvision Digital Technology, Zhejiang Dahua Technology, Intellifusion, etc., also participate in the governmental facial recognition programs by providing technical support.

[51] For more discussions about the ethical, political, and legal aspect of facial recognition, see Berle, I. (2020). *Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images*. Cham: Springer.

References

Abate, F. A., Nappi, M., Riccio, D., & Sabatino, G. (2007). 2D and 3D Face Recognition: A Survey. *Pattern Recognition Letter, 28*(14).

Braithwaite, J. (1982). Enforced Self-Regulation: A New Strategy for Corporate Crime Control. *Michigan Law Review, 80*(7), 1466.

Bratman, E. B. (2002). Brandies and Warren's the Right to Privacy and the Birth of the Right to Privacy. *Tennessee Law Reivew, 69*, 623.

Brownlee, J. (2019). A Gentle Introduction to Deep Learning for Face Recognition. *Machine Learning Mastery.* Retrieved from https://machinelearningmastery.com/introduction-to-deep-learning-for-face-recognition/

Calo, M. R. (2012). Against Notice Skepticism in Privacy (and Elsewhere). *NOTRE DAME L. REV., 87*(3), 1027.

Colin, S. (2004). Regulation in the Age of Governance: The Rise of the Post Regulatory State. In J. Jordana and D. Levi-Faur (Eds), *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance*. Cheltenham: Edward Elgar Publishing.

Conger, K., Fausset, R., & Kovaleski, S. F. (2019). San Francisco Bans Facial Recognition Technology. *The New York Times*. Retrieved from https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Crumpler, W. (2020). The Problem of Bias in Facial Recognition. *CSIS*. Retrieved from https://www.csis.org/blogs/technology-policy-blog/problem-bias-facial-recognition

Cuthbertson, A. (2018). Indian Police Trace 3,000 Missing Children in Just Four Days Using Facial Recognition Technology. *Independent*. Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html

Dixit, P. (2019). India is Creating a National Facial Recognition System, and Critics Are Afraid of What Will Happen Next. BuzzFeed News. Retrieved from https://www.buzzfeednews.com/article/pranavdixit/india-is-creating-a-national-facial-recognition-system-and

Edvardsen, S. (2019). How to Interpret Sweden's First GDPR Fine on Facial Recognition in School. *IAPP*. Retrieved from https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/

Espinoza, J. (2020). EU Backs Away From Call for Blanket Ban on Facial Recognition Tech. *Financial Times*. Retrieved from https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5

European Union Agency for Fundamental Rights. (2019). Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement. Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

Fussey, P., & Murray, D. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. University of Essex, Human Rights Centre.

Gasser, U., & Almeida, V. A. F. (2017). A Layered Model for AI Governance. *IEEE Internet Computing, 21*(6), 58-62. DOI:10.1109/mic.2017.4180835.

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NISTIR 8280. doi: 10.6028/nist.ir.8280.

Hart, Jr., H. M., & Sacks, A. M. (1994). *The Legal Process: Basic Problems in the Making and Application of Law*. New York: Foundation Press.

Kewalramani, M. (2018). Takshashila Working Paper—China's Quest for AI Leadership: Prospects and Challenges. Retrieved from http://takshashila.org.in/wp-content/uploads/2018/10/Chinas-Quest-for-AI-Leadership-Takshashila-Institution-3.pdf

Kracht, T. M., Mueller, M. J., Sotto, L. J., & Sterns, D. (2018). Biometric, Information Protection: The Stage Is Set for Expansion of Claims. *Lexis Practice Advisor Journal, Spring*.

Lannan, K. (2019). Somerville Bans Government Use Of Facial Recognition Tech. *WBUR*. Retrieved from https://www.wbur.org/bostonomix/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech

Lee, K. F. (2018). What China Can Teach the US about Artificial Intelligence—Visionary Research Is No Longer the Most Important Element of Progress. *The New York Times.* Retrieved from https://www.nytimes.com/2018/09/22/opinion/sunday/ai-china-united-states.html

Lessig, L. (1998). The New Chicago School. *The Journal of Legal Studies, 27*(2), 661-691.

Li, S. Z., & Jain, A. K. (Eds). (2011). *Handbook of Face Recognition* (2nd ed.). London: Springer.

Luo, Y. (2017). Chinese Agencies Announce Plan to Audit Privacy Policies of Ten Popular Online Services. *Inside Privacy*. Retrieved from https://www.insideprivacy.com/international/china/chinese-agencies-announce-plan-to-audit-privacy-policies-of-ten-popular-online-services/

Murali, A. (2019). The Big Eye: The Tech Is All Ready for Mass Surveillance in India. *Factordaily*. Retrieved from https://factordaily.com/face-recognition-mass-surveillance-in-india/

Nagaraj, A. (2020). Indian Police Use Facial Recognition App to Reunite Families with Lost Children. *Reuters.* Retrieved from https://www.reuters.com/article/us-india-crime-children/indian-police-use-facial-recognition-app-to-reunite-families-with-lost-children-idUSKBN2081CU

Portnoy, E., Gebhart, G., & Grant, S. (2016). Facial Recognition, Differential Privacy, and Trade-Offs in Apple's Latest OS Releases. *EFF*. Retrieved from https://www.eff.org/deeplinks/2016/09/facial-recognition-differential-privacy-and-trade-offs-apples-latest-os-releases

Price, A. (2018). First International Standards committee for entire AI Ecosystem. *E-tech.* Retrieved from https://iecetech.org/Technical-Committees/2018-03/First-International-Standardscommittee-for-entire-AI-ecosystem

Prosser, W. L. (1960). Privacy. *California Law Review, 48*, 383-423.

Ravani, S. (2019). Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns. *San Francisco Chronicle.* Retrieved from https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php

Roux, M. (2019). How Facial Recognition Is Used in Healthcare. *Sight Corp*. Retrieved from https://sightcorp.com/blog/how-facial-recognition-is-used-in-healthcare/

Scherer, M. U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology, 29*(2).

Schwartz, P. M. (2000). Internet Privacy and the State. *Connecticut Law Review, 32*, 815.

Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic Data Privacy Law. *Geo. L. J., 115*, 123.

Sherman, E. (2008). Privacy Policies Are Great—For PhDs. *CBS News*. Retrieved from https://www.cbsnews.com/news/privacy-policies-are-great-for-phds/

Solove, D. J. (2008). *Understanding Privacy.* Cambridge, MA: Harvard University Press.

Solove, D. J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. *Harv. L. Rev., 126*, 1880-1903.

Stolton, S. (2020). LEAK: Commission Considers Facial Recognition Ban in AI "White Paper''. *EURACTIV*. Retrieved from https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/

Tan, J. A. (2019). Face App 2.0? This New Chinese App Is Cautionary Tale for Personal Privacy. Retrieved from https://vulcanpost.com/674186/zao-app-privacy/

Ulmer, A., & Siddiqui, Z. (2020). India's Use of Facial Recognition Tech During Protests Causes Stir. *REUTERS*. Retrieved from https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ

Westin, A. F. (1967). *Privacy and Freedom*. New York: Athenum.

Xue, Y. J. (2019). Facial-Recognition Smart Lockers Hacked by Fourth-Graders. *Six Tone.* Retrieved from https://www.sixthtone.com/news/1004698/facial-recognition-smart-lockers-hacked-by-fourth-graders

Yang, Z. J. (2019). The Cross Road of Facial Recognition: Facial Panic (人脸识别十字路口：脸的恐慌) (in Chinese). *Inewsweek.* Retrieved from http://www.inewsweek.cn/life/2019-10-21/7329.shtml