UNIVERSITY OF PENNSYLVANIA
JOURNAL OF LAW AND SOCIAL CHANGE
Volume 25, Number 2 2021

FACIAL RECOGNITION IN CHINA: CURRENT STATUS, COMPARATIVE APPROACH AND THE ROAD AHEAD

BY YAN LUO[*] & RUI GUO[**]

Abstract. In this paper we examine China's implementation of facial recognition technology offer a set of legislative and policy recommendations. As the most widely adopted artificial intelligence technology, facial recognition is broadly adopted by companies, residential communities, public parks, schools, etc. There are growing concerns among the public about facial recognition, but a comprehensive regulatory framework is yet to be developed. By comparing the China's approach with the regulatory frameworks in Europe and the US, we discuss the road ahead for China in terms of regulating facial recognition.

[*] Covington & Burling LLP Beijing Office, Partner yluo@cov.com

[**] Rui Guo, S.J.D., corresponding author; Associate Professor of Law, the Law School of Renmin University of China (RUC), affiliated with the Institute of Law and Technology. Director of Centre for Social Responsibility and Governance at Institute of Law and Technology, RUC, China. rguo@ruc.edu.cn. The authors would like to express their thanks to Chris Lin and Vicky Liu for their legal research and contributions to earlier drafts of this article.

INTRODUCTION

In China, facial recognition is undisputedly the most widely adopted artificial intelligence ("AI") technology, having been applied in a wide range of sectors for a variety of purposes, ranging from facilitating identification to improving efficiency.[1] The Chinese government, in recognition of the efficiency gain that facial recognition can create in both public and private sectors, has attached great importance to this technology's research, development, deployment, and commercialization.[2] As a result, facial recognition touches upon almost every aspect of an individual's life in China—for example, facial recognition has been widely used in containing the COVID-19 outbreak by verifying identity without person-to-person contact.[3]

Against this background, there are growing concerns in China about the widespread use of facial recognition as it increases in popularity across almost every sector.[4] A large number of media reports point out that facial recognition technology, as used in the private sector, is prone to problems that include lack of transparency and issues with cybersecurity, such as data leakage.[5] Concerns are also raised from a regulatory standpoint; a report from a multi-agency task force recently published an article highlighting widespread privacy issues indicated in a survey of mobile applications using facial recognition in China. Issues identified include forcing users to provide facial information, a lack of clear rules for information collection, and an inability for data subjects to withdraw consent to the collection and use of facial information.[6]

Despite all the controversy, at present, there is no comprehensive regulatory framework to

[1] *See* Lauren Dudley, China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash, THE DIPLOMAT (Mar. 7, 2020), https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash [https://perma.cc/ND2P-AHHX]. "Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analysing patterns based on the person's facial contours." WORLD ECONOMIC FORUM, A FRAMEWORK FOR RESPONSIBLE LIMITS ON FACIAL RECOGNITION USE CASE: FLOW MANAGEMENT 16 (2021).

[2] *See*, *e.g.*, Cujin Xin Yidai Rengong Zhineng Chanye Fazhan San Nian Xingdong Jihua (促进新一代人工智能产业发展三年行动计划) [Three-Year Action Plan to Develop a New Generation of the Artificial Intelligence Industry] (promulgated by MIIT, Dec. 14, 2017), http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c5960820/part/5960845.docx [https://perma.cc/N8RK-A7EF] [hereinafter Three-Year AI Plan].

[3] Qunxin Feng & Zhifang Chen, Yiqing Jiasu Ren Lian Shibie Luodi: Duo Di Shidian AI Menjin, Jumin Shua Lian Heyan Jiankang Ma (疫情加速人脸识别落地：多地试点 AI 门禁，居民刷脸核验健康码) [COVID-19 Results in Increased Adoption of AI: Pilot AI Access Control is Implemented in Many Locations, Residents Check Their Health through Facial Scans], AI Qianshao Zhan (AI 前哨站) [AI OUTPOST] (Mar. 22, 2020), https://mp.weixin.qq.com/s/0kUzDlzg8n095LSEhLSDIA [https://perma.cc/A7SU-QPFV].

[4] *See*, *e.g.*, Jingti! Ren Lian Shibie Biehou de "Mangqu" (警惕！人脸识别背后的’盲区’) [Alert! The "Blind Spot" of Facial Recognition], CHINA YOUTH DAILY (Jan. 7, 2020), http://www.xinhuanet.com/2020-01/07/c_1125428533.htm [https://perma.cc/T63F-BEQA].

[5] *See, e.g.*, Ren Lian Shibie Luodi Changjing Guancha: Jishu Lanyong, Yingyong Mangqu, Qi Cheng Daxin Xinxi Xielou (人脸识别落地场景观察：技术滥用、应用盲区、七成担心信息泄露) [Observation of Facial Recognition Implementation: Abuse of Technology, Blind Spots of Applications, 70% of Users Concerned About Data Breaches], CBDIO (Jan. 7, 2020), https://kuaibao.qq.com/s/20200107A0I4BF00?refer=spider [https://perma.cc/N8U4-T2NE].

[6] *See* Meiyoule Xuanze Quan he Zhiqing Quan, Ren Lian Ren Bie Hai Zhide Xinren Ma? (没有了选择权和知情权，人脸人别还值得信任吗？) [Without the Right of Choice or the Right to be Informed, Can Facial Recognition be Trusted?], CYBERSPACE ADMINISTRATION OF CHINA (Feb. 20, 2020), http://www.cac.gov.cn/2020-02/20/c_1583740234425125.htm [https://perma.cc/F8W8-UQUS].

guide use of facial recognition in China by entities that range from government agencies responsible for public security or providing public services, state-owned enterprises that provide utilities and essential services, to private entities that are looking to capture the commercial benefit of this new technology. While the government is making efforts to address this issue—for example, in the Personal Information Protection Law ("PIPL"), [7] which dedicates an article to regulating the use facial recognition—current laws and regulations related to facial recognition are fragmented and ambiguous and individuals are often not provided with a valid choice to opt out of the deployment of this technology. Also, as shown by early cases, individuals have limited likelihood to obtain relief unless specific rights and interests are violated. Although recent judgments demonstrate that the judicial community is increasingly aware of the importance of personal information protection, this burden could still be hard to prove.[8]

In contrast, in the past few years, the conversation around facial recognition in Europe and the United States ("US") has expanded from the narrow discussion of "notice and consent" from a privacy standpoint to perimeters and safeguards around a wider range of use cases in both public and privacy sectors. Indeed, both Europe and the US have (1) identified looming issues with possible intrusions into individual privacy, the potential for bias, and inaccurate results resulting from the technology, as well as (2) drafted or enacted corresponding legislation that places a heavy emphasis on weighing public versus individual rights and ensuring appropriate public oversight.

Given the above, this paper will (1) examine the current implementation status of facial recognition in China and touch upon the reasons for its popularity through an overview of use cases; (2) outline the current regulatory framework in Europe and the US; and finally, (3) attempt to put forward a set of recommendations for regulating facial recognition technology in China using a comparative analysis with the existing European and US frameworks.

I. EXPLAINING THE ANALYTICAL FRAMEWORK

Although some of the past literature examining the regulatory framework for the use of facial recognition technology has touched on the margins of appropriate use, such as the need for sufficient

[7] Zhonghua Renmin Gongheguo Geren Xinxi Baohufa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China ("PIPL")] (promulgated by the Standing Comm. Nat'l People's Cong. Aug. 20, 2021, effective on Nov. 1, 2021), art. 26 [hereinafter PIPL]. The PIPL also categorizes individual biometric characteristics as sensitive personal information. *Id.* art. 28. In order to process sensitive personal information, the processor needs to notify and obtain consent from personal information subject. *Id.* art. 29-30.

[8] Though rare, the use of facial recognition technology also has led to some civil and administrative law disputes, such as the use of the technology in universities, park management, zoos, and subways, as well as pertaining to leakage of facial information in connection with online payment tools using facial recognition technology. *See*, *e.g.*, Zhongguo Ren Lian Shibie Di Yi An Hangzhou Yi Dongwuyuan Bei Qisu (中国人脸识别第一案 杭州一动物园被起诉) [The First Facial Recognition Case in China: A Hangzhou Zoo was Sued], BEIJING YOUTH DAILY (Nov. 4, 2019), http://www.xinhuanet.com/legal/2019-11/04/c_1125188289.htm [https://perma.cc/LG4C-A3HV]. Most recently, there have also been criminal cases involving the use of fake facial information to infringe on citizens' property rights. *See*, *e.g.*, Zhangfu Deng Qin Fan Gongmin Geren Xinxi, Zhapian An (张富等侵犯公民个人信息、诈骗案) [Zhang Fu and Other Violations of Citizens' Personal Information], 2019 Z08 XZ NO. 333 (Quzhou Intermediate People's Ct. of Zhejiang Province Nov. 18, 2019); "Renlian Shibie Diyi An" Zai Hangzhou Pan Le! ("人脸识别第一案"在杭州判了！) [The First Case about Facial Recognition is Adjudicated in Hangzhou], RENMINWANG (Nov. 23, 2020), http://leaders.people.com.cn/n1/2020/1123/c58278-31940450.html [https://perma.cc/2GLT-92SQ].

oversight,[9] it primarily focuses on the privacy aspect and the use of the "notice and choice" framework for obtaining data subject consent.[10] This correctly reflects how a large body of existing law uses the "notice and choice" framework as a cornerstone for deploying facial recognition technology, whereby data subjects are presented with a private entity's terms that explain rules for collection and usage and have a choice whether to accept such terms.[11]

However, in recent years, and particularly in 2019 and 2020, Europe and the US have shaped the discussion on use parameters pertaining to facial recognition technology by a wider range of entities such as government agencies and other public bodies—not just private companies. Because public and private use cases may diverge with respect to purposes for use, it is important to examine how requirements pertaining to facial recognition in both areas might be different.

In Europe, regulators have focused their efforts on creating a broad, unified framework to govern public and private sector use of this technology, with European countries furnishing supplementary or country-specific guidance. In contrast, private sector use of facial recognition is generally subject to privacy rules related to biometric data in the US, but local- and state-level legislators have issued specific guidelines on appropriate use primarily in the public sector. Of note, in both Europe and the US, legislators have focused on transparency in the form of public oversight, balancing the need for the technology against individual rights, and defining specific circumstances for appropriate use.

In China, the current discussions around use parameters of this new technology have not yet fully reflected the widespread use in both private and public sectors. While China has some generally applicable privacy rules that address the collection and use of biometric data, it is unclear whether these rules are enforceable in cases where government agencies or state-owned enterprises providing utilities and essential services deploy this technology.[12] Individuals usually have far less power to opt out of such collection and use, and it is hard to obtain any relief if there is misuse or harm.[13] Despite the lack

[9] *See, e.g.*, Kirill Levashov, *The Rise of a New Type of Surveillance for which the Law Wasn't Ready*, 15 COLUM. SCI. & TECH. L. REV. 164, 192 (2013).

[10] *See, e.g.*, Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. SCI. & TECH. L. 88, 90-107 (2017); Robert Warner & Robert Sloan, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 370 (2014); Elias Wright, Comment, *The Future of Facial Recognition is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 611, 611 (2019).

[11] Warner & Sloan, *supra* note 10, at 374.

[12] For example, Beijing Subway has introduced a facial recognition system for security checks, despite controversy incited by earlier efforts in 2019. *See* Alistair Baker-Brian, Are These 'Fast Lanes' the Future of Beijing Subway Stations? (Dec. 28, 2021), https://www.thatsmags.com/beijing/post/33844/are-these-fast-lanes-the-future-of-beijing-subway-stations [https://perma.cc/ZM93-Z38D]; Rui Guo, *Ren Lian Shibie, Pingdeng Bauhu Yu Qiyue Shehui* (人脸识别、平等保护与契约社会)[*Face Recognition, Equal Protection and the Social Contract*], RULE OF LAW DAILY (Dec. 13, 2019), https://www.sohu.com/a/359726235_99923264 [https://perma.cc/ZH8Q-VE8N].

[13] For example—and discussed further below—Beijing's Notice on Further Strengthening of Supervision and Administration of Subletting and Leasing Public Rental Housing requires the use of facial recognition technology to monitor entryways in public housing without any further detail for implementation. *See, e.g.*, Guanyu Jinyibu Jiaqiang Gonggong Zulin Zhufang Zhuang Zu Zhuanjie Xingwei Jiandu Guanli Gongzuo de Tongzhi (关于进一步加强公共租赁住房转租转借行为监督管理工作的通知，京建法【2018】23 号) [Notice on Further Strengthening of Supervision and Administration of Subletting and Leasing Public Rental Housing, Beijing Construction Regulation No.23 [2018]] (Promulgated by Beijing Comm. of Housing and Urban-Rural Dev., Oct. 24, 2018) [hereinafter Beijing Housing Notice].

of use parameters and specific guidance, current Chinese rules governing use of facial recognition in the public sector generally encourages greater use and integration of the technology, leaving out important concerns of how to strike a balance between individual interests and public needs.

As recent legislation trends in Europe and the United States have revealed, focusing solely on privacy protection under concepts such as the "notice and choice" framework provided to individuals vis-a-vis companies in commercial transactions cannot adequately encompass the full extent of necessary governance for facial recognition technology. Instead, it is important to discuss appropriate use parameters for how facial recognition can be deployed in both public and private sectors. This need is clearly recognized by the Chinese government, as it has proposed new language in the PIPL aiming to set out ground rules for the use of facial recognition technologies. Yet, it is unclear to what extent the new rules can be enforced and whether such safeguards would be sufficient to prevent widespread abuse.

This article aims to address this knowledge gap by analyzing the current status of facial recognition technology in China, comparing the China's approach with the regulatory frameworks in Europe and the US, and discussing the road ahead for China in terms of regulating facial recognition.

II. CURRENT STATUS OF FACIAL RECOGNITION IN CHINA: FROM USE CASES TO REGULATORY FRAMEWORK

Over the past few years, the Chinese government set out ambitious goals in the development of facial recognition, as evidenced by many policy documents issued by various government agencies.[14] For example, the Ministry of Industry and Information Technology's AI strategy, issued in 2017 and entitled the *Three-Year Action Plan to Develop a New Generation of the Artificial Intelligence Industry* ("Three-Year AI Plan"), states that by 2020, the effective detection rate in complex dynamic scenarios should exceed 97%, and the correction rate should exceed 90%.[15]

With the government's strong endorsement in mind, this section examines specific use cases in public and private sectors and discusses the role government regulations play in deploying this technology.

[14] For example, the Ministry of Civil Affairs and the National Development and Reform Commission explicitly promoted the application of AI in civil affairs in the 13th Five-Year Plan for the Development of Civil Affairs, issued by the Ministry of Civil Affairs and the National Development and Reform Commission. Minzheng Shiye Fazhan Di Shisange Wunian Guihua (民政事业发展第十三个五年规划，民发【2016】107 号) [13th Five-Year Plan for the Development of Civil Affairs, Civil Aff. No.107 [2016]] (promulgated by Ministry Civil Aff. and NDRC, July 6, 2016). The General Office of the National Development and Reform Commission also stipulated in the Notice on the Organization and Implementation of the New Generation of Information Infrastructure Construction Project and the "Internet Plus" Major Project in 2017 that the infrastructure of face recognition should be strengthened. Guanyu Zuzhi Shishi 2017 Nian Xin Yidai Xinxi Jichu Sheshi Jianshe Gongcheng he "Hulianwang+" Zhongda Gongcheng de Tongzhi (关于组织实施 2017 年新一代信息基础设施建设工程和"互联网+"重大工程的通知, 发改办高技【2016】2710 号) [Notice on the Organization and Implementation of the New Generation of Information Infrastructure Construction Project and the "Internet Plus" Major Project in 2017, NDRC No. 2710 [2016]] (promulgated by NDRC, Dec. 23, 2016).

[15] Three-Year AI Plan, *supra* note 2, art. 2(5).

A. Widespread Use Cases

1. Use Cases in Public Sectors

The most prominent example of facial recognition use in the public sector is identifying citizens for law enforcement purposes, such as tracking and pursuing criminal suspects. The deployment of facial recognition technology in public spaces such as airports, train stations, or at public events such as concert, has led to the widely-reported arrests of many criminal suspects.[16] Also, it has been reported that police officers in the city of Zhengzhou have been equipped with sunglasses that contain facial recognition technology, which has already led to the arrest of seven people suspected of crimes ranging from human trafficking to hit-and-run incidents.[17] Indeed, the efficiency of Zhengzhou's facial recognition sunglasses—which can "identify faces from a database of 10,000 in 100 milliseconds"—is highlighted when considering the possibility that the aforementioned arrests may have required much more manpower and time without the availability of such technology.[18]

In additional to using facial recognition to pursue criminals, the government also designated facial recognition as the "go-to" technology in many regulations that would require public bodies to perform identity verification. Facial recognition is strongly encouraged, even mandated in many cases, to facilitate identify verification in many day-to-day administrative matters such as notarization, obtaining driver licenses, or providing social benefits to residents. A few recent examples include:

· In September 2017, the Ministry of Justice stipulated that a party requesting notarization shall undergo identity verification through methods such as facial recognition, which would be cross-checked against information contained in the Ministry of Public Security's databases.[19]

· In May 2018, the Guangdong Province created a WeChat Mini Program to provide government services, including those pertaining to birth certificates, residence

[16] For example, Wu Xieyu, a suspect in the murder of his mother, had been pursued by the police for years without success, but was arrested soon after at Chongqing Jiangbei airport, which had upgraded its facial recognition systems. Pinghui Zhuang, *Chinese Student Wanted for Killing Mother Captured After Three Years on the Run*, PEOPLE'S DAILY (Apr. 26, 2019), https://wap.peopleapp.com/article/4103611/3961671 [https://perma.cc/DZD9-4QHL]. In addition, numerous criminal suspects were captured at various Jacky Cheung concerts through facial recognition technology. Simone McCarthy, *China's "Crime-Fighting" Pop Star Jacky Cheung Adds 12 Crooks, Two Drones to His Tally*, S. CHINA MORNING POST (Sep. 25, 2018), https://www.scmp.com/news/china/society/article/2165566/chinas-crime-fighting-pop-star-jacky-cheung-adds-12-crooks-two [perma.cc/6Y48-Y7RZ].

[17] Neil Conner, *Chinese Police Using Facial Recognition Glasses to Identify Suspects*, TELEGRAPH (Feb. 7, 2018), https://www.telegraph.co.uk/news/2018/02/07/chinese-police-using-facial-recognition-glasses-identify-suspects [perma.cc/3EN7-QCAV].

[18] Tara F. Chan, *Chinese Police are Using Facial-recognition Glasses to Scan Travelers*, BUS. INSIDER (Feb. 7, 2018), https://www.businessinsider.com/china-police-using-facial-recognition-glasses-2018-2?r=US&IR=T [perma.cc/ELA4-2AH7].

[19] Sifa Bu Bangong Ting Guanyu Fabu Gongzheng Zhiye Zhidao Anli de Tongzhi (司法部办公厅关于发布公证执业指导案例的通知) [Notice of the Office of the Ministry of Justice on Practical Guidance for Notarization] (promulgated by the Ministry of Justice, Sep. 25, 2017), art. 6.

permits, and exit/entry certificates.[20] Users are encouraged to use facial recognition to access the services provided.[21]

· In April 2019, the General Administration of Customs permitted facial recognition technology to be used at Customs' registration desks.[22]

· In January 2020, the Ministry of Public Security required the Traffic Management Department's online traffic schools to verify user identity through technical means, "such as facial recognition." [23] Moreover, where the Traffic Management Department organizes on-site education of traffic laws and related knowledge, the driver's identity shall similarly be verified through facial recognition technology.[24]

· In February 2020, for purposes of monitoring and containing COVID-19, Ant Financial launched a QR code system that assigns users one of three color codes to denote the status of their health and allows them to "obtain their codes by entering their name, national identity number and registering with facial recognition."[25]

Note that in these regulations, use parameters or specific guidance are not discussed with respect to how facial recognition is deployed. Additionally, none of the promulgated rules address security measures to protect facial information.

2. Hybrid Use

With the strong support by the government, state-owned enterprises in various industries have begun to use facial recognition technology to conduct identity verification for a wide range of uses. For example, state-owned enterprises are encouraged to use facial recognition technology largely for streamlining identity verification:

· 12306 China Railway's ("12306") privacy policy notifies users that certain biometric information, such as a facial scan, is required where users would like to log in to their

[20] Guangdong: Xiaocheng Xu Qiaodong Da Gaige (广东：小程序撬动大改革) [Guangdong: mini-app leads to big reform] GUANGMING DAILY (Dec. 12, 2019), http://cpc.people.com.cn/n1/2019/1212/c415067-31503048.html [perma.cc/SDV3-5NMR].

[21] *Id.*

[22] Haiguan Jianguan Zuoye Changsuo (Changdi) Jiankong Shexiangtou Shezhi Guifan (海关监管作业场所（场地）监控摄像头设置规范) [Customs Worksite Supervision (Property) Surveillance Setup Specifications] (promulgated by General Admin. Customs, Apr. 22, 2019).

[23] Jieshou Jiaotong Anquan Jiaoyu Jianmian Daolu Jiaotong Anquan Weifa Xingwei Jifen Gongzuo Guifan (Shixing) (接受交通安全教育减免道路交通安全违法行为记分工作规范（试行）) [Rules on Accepting Traffic Safety Education to Reduce Illegal Traffic Behavior (Trial)] (promulgated by the Ministry of Pub. Sec., Jan. 14, 2020), art. 12.

[24] *Id.* art. 16(2).

[25] Minghe Hu, *Beijing Rolls Out Colour-Coded QR System for Coronavirus Tracking Despite Concerns Over Privacy, Inaccurate Ratings*, S. CHINA MORNING POST (Mar. 2, 2020), https://www.scmp.com/tech/apps-social/article/3064574/beijing-rolls-out-colour-coded-qr-system-coronavirus-tracking [perma.cc/5R65-SXK8].

accounts through facial recognition.[26] Facial recognition can also be used to retrieve account passwords.[27]

· The People's Bank of China ("PBC") issued rules on facial recognition technology for bank account verification. Since 2016, PBC required banks to comply with verification procedures of client identity for certain types of bank accounts, with assistance by technical means, "including facial recognition technology." [28] In addition, PBC encouraged banks to use technical means such as facial recognition to assist in reading, collecting, and verifying client information during the process of opening an account.[29]

· In January 2019, the Beijing Municipal Commission required the Beijing housing construction plan to incorporate facial recognition technology in public housing projects, such as in entryways to prevent unauthorized access.[30]

· On February 13, 2019, the National Health Commission encouraged pilot medical institutions to use facial recognition technology to strengthen management of nurses.[31]

· Since 2018, facial recognition has become the foundation of the "smart city" in Shanghai. Shanghai's Municipal Government requires the installation of AI equipment in various public areas and residential spaces. As a result, facial recognition devices have been installed in elevators in residential areas, which has caused controversy amongst Shanghai residents.[32]

Other examples also include tracking behavior of relevant personnel in essential services, managing parks, supervising medical insurance, supervising public transportation, and completing real

[26] *Yinsi Quan Zhengce (隐私权政策) [Privacy Policy]*, RAILWAY 12306 (Aug. 20, 2021), https://kyfw.12306.cn/otn/gonggao/PrivacyPolicy.html [perma.cc/N2YY-S9ZF].

[27] *Id.*

[28] Zhongguo Renmin Yinhang Guanyu Luoshi Geren Yinhang Zhanghu Fenlei Guanli Zhidu de Tongzhi (中国人民银行关于落实个人银行账户分类管理制度的通知) [Notice of the People's Bank of China on Implementing the Rules for the Categorized Management of Individual Bank Accounts] (promulgated by People's Bank China, Nov. 25, 2016, effective on Dec. 1, 2016).

[29] Zhongguo Renmin Yinhang Guanyu Youhua Qiye Kaihu Fuwu de Zhidao Yijian (中国人民银行关于优化企业开户服务的指导意见) [Guiding Opinions of the People's Bank of China on Optimizing the Account Opening Services for Enterprises] (promulgated by People's Bank China, Dec. 20, 2017, effective Dec. 31, 2017).

[30] Beijing Housing Notice, *supra* note 13.

[31] "Hulianwang + Huli Fuwu" Shidian Gongzuo ("互联网＋护理服务"试点工作) ["Internet + Nursing Services" Pilot Job] (promulgated by the Nat'l Health Comm'n, Feb. 13, 2019), art. 3(1).

[32] *Shanghai Tuiguang Xiaoqu Dianti Ren Lian Shibie Guanggao Zhihuan Moshi Yu Yinsi Baohu Yin Zhengyi* (上海推广小区电梯人脸识别 广告置换模式与隐私保护引争议) [*Shanghai's Promotion of Facial Recognition in Community Elevators Regarding Replacement Modes and Privacy Protections Results in Controversy*], CAIXIN (Oct. 16, 2019), http://china.caixin.com/2019-10-16/101471840.html [https://perma.cc/2K27-3QX9].

estate registration. [33]

Again, the above instances of use do not set forth any guidance on permissible use parameters or security measures, but rather broadly require integration or increased use of facial recognition technology.

3. Commercial Use

In light of government support and, at times, government mandate, many private companies opt to use facial recognition technology to enhance their business operations' efficiency.

Companies in various industries have started to apply facial recognition technology to manage user authentication.[34] For example, on September 10, 2018, the Ministry of Transport and Ministry of Public Security jointly called for ride-sharing platforms to vet drivers by background checks and use facial recognition to verify driver identity prior to being dispatched to users. [35] However, they did not discuss use parameters or recommendations for security measures.

In addition, on January 9, 2019, China Netcasting Services Association issued the Short Internet Video Platform Management Specification ("Internet Video Specification"), setting forth rules specific to online video platforms.[36] The Internet Video Specification requires the use of technical measures like facial recognition for account verification and management, but does not specify how the technology may be appropriately deployed.[37]

Mobile phone users in China registering new SIM cards must submit to facial recognition scans. According to the Ministry of Industry and Information Technology, beginning on December 1, 2019, telecom companies must fully implement the technical measures "of portrait comparison

[33] The Chinese government has issued several policy documents on the application of facial recognition, all without discussing circumstances or rules for appropriate use. *See, e.g.*, Zhongguo Renming Yinhang Guanyu Youhua Qiye Kaihu Fuwu de Yijian (中国人民银行关于优化企业开户服务的指导意见) [Guiding Opinions of the People's Bank of China on Optimizing the Account Opening Services for Enterprises] (promulgated by the People's Bank China, Dec. 31, 2017, effective Dec. 31, 2017); Guojia Linye he Caoyuan Ju Guanyu Cujin Linye he Caoyuan Rengong Zhineng Fazhan de Zhidao Yijian (国家林业和草原局关于促进林业和草原人工智能发展的指导意见) [Guiding Opinions of the National Forestry and Grasslands Administration on the Development of Artificial Intellgience for Forestry and Grasslands] (promulgated by the Nat. Forestry Grasslands Admin., Nov. 21, 2019, effective Nov. 21, 2019); Guowuyuan Bangong Ting Guanyu Bufen Difang Youhua Ying Shang Huanjing Dianxing Zuofa de Tongbao (国务院办公厅关于部分地方优化营商环境典型做法的通报) [Circular of the State Council's Office Regarding Best Practices to Optimize Business in Certain Areas] (promulgated by the State Council, Jul. 24, 2018, effective Jul. 24, 2018).

[34] *See, e.g.*, *Didi Zhengzai Yong AI Jishu Dui Siji Jinxing Quan Fangwei "Jiankong"* (滴滴正在用 *AI* 技术对司机进行全方位"监控") [*Didi is Using AI Technology to Comprehensively Monitor Drivers*], TMTPOST (May 12, 2019), https://www.tmtpost.com/nictation/3939157.html [https://perma.cc/H8WP-PZ7Q].

[35] Jiaotong Yunshu Bu Bangong Ting, Gongan Bu Bangong Ting Guanyu Jinyibu Jiaqiang Wangluo Yuyue Chuzu Qiche he Siren Xiao Keche He Cheng Anquan Guanli de Jinji Tongzhi (交通运输部办公厅、公安部办公厅关于进一步加强网络预约出租汽车和私人小客车合乘安全管理的紧急通知) [Urgent Notice of the General Office of the Ministry of Transport and the General Office of the Ministry of Public Security on Further Strengthening the Safety Administration of Online Car-Hailing and Private Passenger Car Sharing] (promulgated by the Ministry Transp. and Ministry Pub. Sec., Sep. 10, 2018), art. 3.

[36] Wangluo Duan Shipin Pingtai Guanli Guifan (网络短视频平台管理规范) [Short Internet Video Platform Management Specification] (promulgated by China Netcasting Serv. Ass'n., Jan. 9, 2019, effective Jan. 9, 2019).

[37] *Id.* art. 4(2).

between a user's facial features and his or her identification card"; only when the portrait comparison is consistent can the user proceed with network access. [38]

Other examples include e-commerce and social platforms which use facial recognition for online payment services,[39] mobile phones which use facial recognition as a method of unlocking the device,[40] and businesses across all sectors that use facial recognition to monitor employee attendance.[41]

B. *Regulatory Framework*

As discussed above, to govern such widespread deployment of facial recognition, Chinese regulators have published national and sector-specific rules, though specificities pertaining to use parameters remain sparse and largely focus on use of this technology by the private sector. The newly enacted PIPL, for the first time, contains restrictions on the deployment of facial recognition for both public and private purposes and tightens collection and usage of all sensitive personal information, including but not limited to facial data.

1. (Draft) National Standards

On March 6, 2020, China's National Information Security Standardization Technical Committee ("TC260") released the final version of the Personal Information Security Standard, which, in practice, applies mainly to entities in the private sector.[42] While the Personal Information Security Standard sets forth privacy requirements for collecting and processing personal information, it also includes security requirements for protecting biometric information, including facial information.[43] Specifically, the Personal Information Security Standard forbids personal information controllers from storing facial information in its original image form, though they are instead allowed to store summaries of such information.[44] However, personal information controllers are allowed to use the original facial images for authentication or verification purposes at the end terminal, e.g., user's device, only when

[38] *Gongxinbu Xin Gui Shishi: 12 Yue 1 Ri Qi Ban Ka Xu "Ren Lian Shibie"* (工信部新规实施：*12*月 *1*日起办卡需*"*人脸识别*"*) [*China's Ministry of Industry and Information Technology's New Implementing Regulation: Beginning From Dec. 1, Application for Cards Requires "Facial Recognition"*], SOHU TECH. (Dec. 2, 2019), https://www.sohu.com/a/357849569_115565 [https://perma.cc/A54G-GHVJ].

[39] *Ren Lian Shibie Zhifu Zenme Jiu Huole* (人脸识别支付怎么就火了) [*How Did Payment via Facial Recognition Become Popular*], BEIJING YOUTH DAILY (Sep. 7, 2017), http://www.xinhuanet.com/fortune/2017-09/07/c_1121618680.htm [https://perma.cc/42QV-TKFG].

[40] *Pingguo Xin Shouji Caiyong Ren Lian Shibie Gangmei Zhi Hu Guoshi: Zhongguo Liang Nian Qian Jiu Kaishi Yongle* (苹果新手机采用人脸识别 港媒直呼过时：中国两年前就开始用了) [*New Apple Phones Use Facial Recognition and Hong Kong Media Notes it is Outdated: China Began Using Such Technology Two Years Ago*], REFERENCE NEWS NETWORK (Sep. 19, 2017), http://www.xinhuanet.com//world/2017-09/19/c_129707298.htm [https://perma.cc/55BV-Y6SS].

[41] *Zhongtie Si Ju Wu Gongsi Quanmian Tuixing Rne Lian Shibie Kaoqin Zhidu* (中铁四局五公司全面推行人脸识别考勤制度) [*China Railway No. 4 Bureau Group No. 5 Engineering Company Fully Implements Facial Recognition Technology*], CTCECC (Jul. 25, 2013), http://www.ctcecc.com/content-807-6176-1.html [https://perma.cc/DE88-GMLD].

[42] Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 个人信息安全规范) [Information Security Technology – Personal Information Security Specification] (promulgated by the Nat'l Info. Sec. Standard Tech. Comm, Mar. 6, 2020, effective Oct. 1, 2020).

[43] *Id.* art. 5.4, 6.3.

[44] *Id.* art. 6.3(c)(1).

they subsequently delete the images.[45] While it is widely believed that government agencies are encouraged to review the Personal Information Security Standard when they are enforcing the Cybersecurity Law against companies, it is unclear whether the public sector is bound by the Personal Information Security Standard's requirements when they are deploying facial recognition technology to perform public functions.[46]

On April 22, 2021, TC260 released the draft *Information Security Technology - Security Requirements of Facial Recognition Data* ("Draft Standard") for public comments.[47] This Draft Standard introduces detailed security requirements for the processing of facial recognition data by companies conducting "facial verification" (to verify the authenticity of an individual's identity) and "facial identification" (to identify an individual).[48] Facial recognition data is defined as "facial images and data that are generated from facial images, which can be used alone or jointly with other information to identify a natural person."[49] The Draft Standard also specifically require companies to comply with the requirements under other data protection national standards if they only process "face images" for statistics, testing and analytics purposes.[50]

Under the Draft Standard, companies using facial recognition to verify and identify an individual must fulfill the following requirements:

> · facial recognition shall not be used unless it would significantly improve the level of security and convenience of the verification and identification process comparing with other alternative methods[51];
>
> · facial recognition shall not be used to identify children under 14 years old unless in special circumstances (not further explained in the Draft Standard)[52];
>
> · an alternative identification method that does not use facial recognition shall be provided to individuals[53];
>
> · the company must obtain informed consent from individuals[54]; and
>
> · facial recognition data shall not be used for purposes other than security. Such other purposes include, but are not limited to, the evaluation or prediction of an

[45] *Id.* art. 6.3(c)(2)-(3).

[46] *Cf. id.* art. 1.

[47] Xinxi Anquan Jishu Rennian Shibie Shuju Anquan Yaoqiu (信息安全技术 人脸识别数据安全要求) [Information Security Technology - Security Requirements for Facial Recognition Data] (released for public comments on Apr. 22, 2021, https://www.tc260.org.cn/front/postDetail.html?id=20210423175440)

[48] *Id.* art. 4.

[49] *Id.* art. 3.3.

[50] *Id.* art. 4(c).

[51] *Id.* art. 5(f)(1).

[52] *Id.* art. 5(f)(2).

[53] *Id.* art. 5(f)(3).

[54] *Id.* art. 5(f)(4).

individual's work performance, health condition, interests, and preferences.[55]

The Draft Standard still awaits finalization as of October 2021.

2. Sector-Based Rules

Although regulators stopped short of furnishing general guidance on usage parameters, some trade associations have been seen making attempts to draft sector-based guidelines to regulate the use of facial recognition.

The most notable example are the usage parameters defined in a framework of self-governance within the finance industry. In an effort to establish rules for self-governance with respect to deploying facial recognition technology that would allow consumers to make payments, the Payment and Clearing Association of China began piloting the Self-Regulatory Agreement for Offline Facial Recognition Payment Industry ("PCAC Self-Regulatory Agreement") on January 20, 2020.[56] Like the Personal Information Security Standard, the PCAC Self-Regulatory Agreement focuses on technical and security measures for protecting facial information.[57] Importantly, members to the PCAC Self-Regulatory Agreement shall encrypt the original facial information when storing it and such information should be separated from an individual's financial records.[58] Moreover, all members shall manage the potential risks of facial recognition payments by establishing a monitoring system for suspicious transactions,[59] setting limitations on the amount of funds that can be transferred through facial recognition,[60] as well as developing channels for consumer feedback or complaints.[61]

3. Personal Information Protection Law

On August 20, 2021, the National People's Congress enacted the PIPL, which will be country's first comprehensive law in the area of personal information protection once it takes in effect on November 1, 2021. Article 26 of the PIPL sets restrictions on facial recognition usages by stating that "[t]he installation of image collection and personal identity recognition devices in public venues is permissible if it is necessary to safeguard public security, to comply with relevant regulations of the state, and to set prominent notices."[62] It also states that "the personal images and personal identification information to be collected can only be used for the purpose of safeguarding public security and shall not be disclosed or provided to others, except where individuals' specific consent is obtained or the

[55] *Id.* art. 5(f)(5).

[56] Ren Lian Ren Bie Xian Xia Zhifu Hangye Zilu Gongyue (Shixing) (人脸认别线下支付行业自律公约（试行）) [Self-Regulatory Agreement for Offline Facial Recognition Payment Industry (trial)] (promulgated by the Payment Clearing Ass'n. China, Jan. 20, 2020).

[57] *See, e.g.*, *id.* art. 6, art. 17.

[58] *Id.* art. 6.

[59] *Id.* art. 17.

[60] *Id.* art. 19.

[61] *Id.* art. 24.

[62] PIPL, *supra* note 7, art. 26.

laws and administrative regulations stipulate otherwise."[63]

The PIPL categorizes biometric characteristics as sensitive information, which requires the personal information processor to obtain consent and explain the necessity and impact to the personal information subject.[64]

4. Private Litigation and Judicial Interpretation

The first facial recognition dispute in China was resolved at Fuyang District People's Court in Hangzhou on November 20th. The plaintiff in this case claimed that it was a breach of contract for a zoo to change entrance method for annual pass-holders from fingerprint recognition to facial recognition. The Court explained that Chinese law emphasizes that the supervision and management of personal information processing and personal information collection needs to be legal, justified, and necessary. Further, the Court mentioned that personal information collectors shall obtain consent from individuals and ensure the safety of personal information being collected. In this case, the zoo provided notice that certain personal information is to be collected when the plaintiff made decision to become an annual-pass member. The plaintiff was well-informed before providing his personal information, thus the zoo did not violate personal information protection requirements. However, the Court stated that the zoo breached the contract by unilaterally changing the entrance method. The Court required the zoo to compensate the plaintiff and delete all of his facial information.[65]

On June 8, 2021, the Supreme People's Court issued a judicial interpretation on facial recognition related cases. The judicial interpretation defines the facial information as "biometric information" specified under article 1034 of the Civil Code. It also stipulated that without proper authorization of laws or administrative regulations, it is an infringement of individuals' personal rights for business places or public places—hotels, shopping malls, banks, transport stations, airports, sports venues, entertainment venues—to use facial recognition technology to verify, identify, or analyze faces. It also stated that homeowners or property users should have alternative means to verify identity if property management companies use a facial recognition system to manage entrance or exit of the property. The judicial interpretation also clarified the meaning of consent for processing facial information. In addition, the Court also listed exemptions from civil liability, such as processing facial information in response to an emergency in public health work, or using facial recognition technology in public places for the purpose of maintaining public security.[66]

[63] *Id.*

[64] *Id.* art. 28-30.

[65] "Renlian Shibie Diyi An," *supra* note 8.

[66] Zuigao Renmín Fayuan Guanyu Shenli Shiyong Ren Lian Shibie Jishu Chuli Geren Xinxi Xiangguan Minshi Anjian Shiyong Falu Ruogan Wenti De Guiding (关于审理使用人脸识别技术处理个人信息 相关民事案件适用法律若干问题的规定)[*Provisions on Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to the Use of Facial Recognition Technologies to Process Personal Information*, Judicial Interpretation No. 15 [2021]] (promulgated by the Judicial Comm. Sup. People's Ct., June 8, 2021, effective Aug. 1, 2021).

III. REGULATING FACIAL RECOGNITION IN EUROPE AND THE UNITED STATES

A. Europe

1. Uniform Framework of Public and Commercial Use in the European Union

The European Commission envisions a broad regulatory framework applicable to public and private entities, noting in particular that "[i]t is also essential to make sure that the private sector is fully involved in setting the research and innovation agenda and provides the necessary level of co-investment."[67] In other words, the European Commission plans to further develop binding and non-binding regulatory frameworks governing facial recognition technology across the public and private sectors. Importantly, however, although an examination of case law and Member State guidance reveals that certain factors dictating appropriate usage of such technology already exist,[68] the European Commission remains at an exploratory stage with respect to appropriate policy approach to AI, and by extension, facial recognition technology.[69]

Presently, at the European Union ("EU") level, the General Data Protection Regulation ("GDPR")—and the Police and Criminal Justice Directive, the GDPR's counterpart directed towards law enforcement entities—largely remains the legal framework under which facial recognition technology is deployed, focusing primarily on its privacy aspects.[70] Indeed, because facial information "is particularly sensitive since it makes it possible to uniquely identify an individual,"[71] the technology falls under Article 9 of the GDPR, which sets forth requirements for processing special categories of personal information and includes facial information under the broader scope of biometric information.[72] In October 2019, the European Data Protection Supervisor ("EDPS") also affirmed the applicability of the GDPR to facial recognition technology.[73] However, further specificity with respect to regulation and use parameters remain absent, with the EDPS first questioning the validity of facial recognition technology usage by noting that "[n]ow is the moment for the EU, as it discusses the ethics of AI and the need for regulation, to determine whether[—]if ever[—]facial recognition technology can

[67] *On Artificial Intelligence – A European Approach to Excellence and Trust*, at 7, COM (2020) 65 final (Feb. 19, 2020) [hereinafter AI White Paper].

[68] *See, e.g.*, *Facial Recognition in School Renders Sweden's First GDPR Fine*, EUR. DATA PROT. BD. (Aug. 22, 2019), https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en [https://perma.cc/2SN9-ZFT9] [hereinafter Sweden FRT Fine].

[69] *See id.* at 1.

[70] DIDER BAICHÈRE, ASSEMBLÉE NATIONALE, FACIAL RECOGNITION 2 (2019), https://www2.assemblee-nationale.fr/content/download/179314/1794787/version/2/file/Note%20Reconnaissance%20Faciale%20-%20EN.pdf [https://perma.cc/X6G6-5FQS]; *"Law Enforcement Directive": What Are We Talking About?*, CNIL (June 2, 2021), https://www.cnil.fr/en/law-enforcement-directive-what-are-we-talking-about [https://perma.cc/YP22-ZAW5].

[71] Baichère, *supra* note 70, at 2.

[72] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, art. 9, O.J. (L 119).

[73] Wojciech Wiewiórowski, *Facial Recognition: A Solution in Search of a Problem?*, EUR. DATA PROT. SUPERVISOR (Oct. 28, 2019), https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en [https://perma.cc/8ZW4-5VQW].

be permitted in a democratic society," and if so, "we turn to questions of how and safeguards and accountability to be put in place."[74]

a. Current Non-binding Requirements

The European Commission desires a "human-centric approach" to AI, which encompasses facial recognition technology across the public and private sectors, whereby AI shall be "trustworthy."[75] To that end, on April 8, 2019, the High-Level Expert Group on AI set forth non-binding guidelines to assess and ensure the proper use of AI ("EC Non-Binding AI Guidelines").[76] The EC Non-Binding AI Guidelines promote rules and principles including (1) human oversight of AI operations,[77] (2) reliable design against attacks or intrusions,[78] (3) transparency,[79] and (4) eliminating potential for bias or discrimination against certain groups of data subjects. [80]

On January 23, 2020, the European Parliament's Internal Market and Consumer Protection Committee also approved a resolution specifically pertaining to consumer protection with respect to the use of AI technology ("Draft AI Consumer Protection Resolution").[81] Though brief, the Draft AI Consumer Protection Resolution, in pertinent part, mirrors the EC Non-Binding AI Requirements as well as the EC White Paper and calls for commercial use of AI to be tempered by human oversight, which can override any AI decision-making.[82] Moreover, companies shall have procedures in place to remedy any errors in AI processing.[83]

b. Proposed Regulatory Framework

The European Commission issued a series of documents in February 2020 detailing the overall strategy and approach to AI for the EU.[84] The Commission's documents provide broad principles for deploying facial recognition technology, but, like the EC Non-Binding AI Requirements, stop short of mandating specific safeguards and measures for accountability around facial recognition technology.[85] Indeed, on February 19, 2020, the European Commission released a white paper

[74] *Id.*

[75] *Building Trust in Human-Centric Artificial Intelligence*, at 1-2, COM (2019) 168 final (Apr. 8, 2019) [hereinafter Building Trust in AI].

[76] *Id.* at 3. *See also* ETHICS GUIDELINES FOR TRUSTWORTHY AI, HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (2019), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 [https://perma.cc/6J4M-5V8U].

[77] Building Trust in AI, *supra* note 75, at 4.

[78] *Id.* at 4-5.

[79] *Id.* at 5.

[80] *Id.* at 6.

[81] Draft Motion for a Resolution on Automated Decision-Making Processes: Ensuring Consumer Protection, and Free Movement of Goods and Services (2019/2915(RSP)), EUR. PARL. DOC. (COM 0094) (2020).

[82] *Id.* at 5.

[83] *Id.* at 5-6.

[84] *See, e.g.*, AI White Paper, *supra* note 67.

[85] *See generally id.*

addressing, among other topics, the need for a regulatory framework that can better account for and govern the developments in AI.[86] Importantly, the Commission calls for a "partnership between the private and the public sector," in which the proposed framework would apply across both sectors.[87]

2. Case Law related to Public Use in European Countries and Member States

While legislative action pertaining to facial recognition technology remains in early, exploratory stages at the EU level, certain EU Member States have issued guidance on facial recognition use through case law and legislation. Major themes for appropriate use standards in various jurisdictions explored below include the need to: (1) minimize intrusiveness, (2) strike an appropriate balance between individual and community interests (e.g., having limitations on time and place of deployment), (3) have a legitimate or important purpose for use, and (4) have appropriate oversight of use.

a. Sweden: Prohibition of Use in Schools

On August 22, 2019, the European Data Protection Board announced that the Swedish Data Protection Authority ("DPA") issued a fine to a Swedish public high school for using facial recognition technology to monitor and track student attendance.[88] The school deployed such technology in only one class and for a limited amount of time.[89] Nevertheless, the Swedish regulator determined that the use was inappropriate because attendance could have been monitored in a less intrusive manner, students had a certain degree of privacy expectations when in the classroom, sensitive personal information was being processed, and the school did not perform an impact assessment—which includes communication with the regulator.[90]

b. United Kingdom: Use by Law Enforcement in Public Places

On February 10, 2020, the United Kingdom's Committee on Standards in Public Life issued its report on Artificial Intelligence and Public Standards to address how public bodies deliver public

[86] *Id.* at 10.

[87] *Id.* at 3. The AI White Paper builds on the non-binding requirements the Commission drafted in 2019, with overlapping principles such as the need for human oversight, robustness of systems, and transparency. *Id.* at 18. For high-risk AI, which includes facial recognition technology, the AI White Paper uses the existing legislative framework to broadly identify appropriate use parameters, with a note that very limited grounds exist for processing biometric information. *Id.* at 22. For example, under the GDPR, processing such information must be "subject to the requirements of proportionality, [and] respect for the essence of the right to data protection and appropriate safeguards." *Id.* Alongside data protection rules, the AI White Paper also affirms the applicability of the Charter of Fundamental Rights to AI biometric identification, in which usage is appropriate only "where such use is duly justified, proportionate and subject to adequate safeguards." *Id.*

[88] Sweden FRT Fine, *supra* note 68. *See also* Sofia Edvardsen, *How to Interpret Sweden's First GDPR Fine on Facial Recognition in School*, IAPP (Aug. 27, 2019), https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/ [https://perma.cc/X5MA-HRQE].

[89] Sweden FRT Fine, *supra* note 68.

[90] *Facial Recognition: School ID Checks Lead to GDPR Fine*, BBC (Aug. 27, 2019), https://www.bbc.com/news/technology-49489154 [https://perma.cc/3TX2-JDHM].

services using AI.[91] However, the real landmark development for facial recognition technology lies in the UK's law enforcement sector.

On September 4, 2019, the High Court of Justice in London issued a judgment on the use of facial recognition technology for crime surveillance by the South Wales Police ("SWP").[92] The plaintiff, whose face was recorded by the technology, brought suit, alleging, in part, violation of his rights under Article 8 § 1 of the European Convention of Human Rights ("ECHR"),[93] which grants the right to privacy.[94]

When examining whether the SWP's use of facial recognition technology interfered with plaintiff's rights under the ECHR, the court weighed the following four factors: (1) whether the purpose of use was important enough to limit a fundamental right, (2) whether the purpose was rationally related to the end goal, (3) whether a less intrusive measure was available, and (4) whether a fair balance existed between the rights of the individual and community interests.[95]

The court ultimately found in favor of SWP.[96] Indeed, SWP used such technology to locate suspects[97] and manage possible criminal damage during large-scale public events.[98] Moreover, SWP's usage was not considered intrusive, because facial information was processed and discarded almost instantaneously and there were no complaints nor wrongful arrests.[99] The court also noted that SWP achieved a fair balance between individual and community rights because the specific usage purpose was limited in time and area.[100]

However, the UK Information Commissioner's Office ("ICO") offered its opinion, rebuking this ruling, calling for statutory rules to bind government use of facial recognition technology, and calling for requirements that law enforcement demonstrate the technology is "strictly necessary, balanced and effective" in each use context.[101]

c. France: Specified Guidelines for Use

On November 15, 2019, the Commission Nationale de l'informatique et des Libertés ("CNIL") issued guidance directed at French public entities that planned to implement facial

[91] *See* COMM. ON STANDARDS IN PUB. LIFE, ARTIFICIAL INTELLIGENCE AND PUBLIC STANDARDS: A REVIEW BY THE COMM. ON STANDARDS IN PUB. LIFE 4 (2020).

[92] R. (Bridges) v. Chief Constable of South Wales Police, [2019] EWHC (Admin) 2341, WLR(D) 496 (U.K.).

[93] *Id.* para. 19.

[94] Eur. Conv. on H. R., art. 8 § 1, 2, Nov. 4, 1950, E.T.S. No. 005; R. (Bridges), [2019] EWHC (Admin) 2341, para. 19.

[95] *Id.* para. 98.

[96] *Id.* para. 99-108.

[97] *Id.* para. 11.

[98] *See id.* para. 13.

[99] *Id.* para. 101.

[100] *Id.*

[101] Elizabeth Denham, *Blog: Live Facial Recognition Technology – Police Forces Need to Slow Down and Justify its Use*, INFO. COMM'R. OFF. (Oct. 31, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/live-facial-recognition-technology-police-forces-need-to-slow-down-and-justify-its-use [https://perma.cc/PT5C-64JJ].

recognition technology for experimental use.[102] Citing concerns regarding reliability and potential biases with respect to gender and skin color, the CNIL sets forth three requirements to adhere to when deploying this technology.[103] First, facial recognition technology can be used only when (1) a method of authentication exists to ensure reliability and (2) no less intrusive means are available.[104] CNIL further lists examples of potentially acceptable usage—which includes accessing public services (e.g., tax accounts, health insurance accounts, vehicle registrations, etc.) and automated identity verification systems at travel hubs—and unacceptable usage, such as in schools.[105] Second, experimental usage of facial recognition technology must respect individual rights.[106] This requirement contains principles common in data privacy laws, in which individuals must (1) provide consent to processing of their facial information, (2) receive control over their information, and (3) receive clear, comprehensive, and accessible information.[107] Third, experimental usage is only allowed under a precise timeline, with a "rigorous methodology" detailing the objectives for use and criteria for success.[108]

3. Commercial Use

The increasing use of facial recognition technology in the private sector has come under scrutiny by DPAs in various European countries and Member States. Notably, in August 2019, the ICO launched an investigation into the use of facial recognition technology in King's Cross, London, noting that "any organisations wanting to use facial recognition technology must comply with the law - and they must do so in a fair, transparent and accountable way. They must have documented how and why they believe their use of the technology is legal, proportionate and justified."[109] Moreover, in March 2020, Swedish DPA ("IMY") launched an investigation into the usage of Clearview AI, a tool that applied facial recognition technology to over three billion photographs obtained from social media platforms, such as Facebook, Twitter, and YouTube.[110] The IMY concluded that "Cleaview AI has been used by the Police on a number of occasions" and that "the Police has not fulfilled its obligations as a data controller on a number of accounts with regards to the use of Clearview AI."[111] The Police was fined by IMY for its failure to comply with the Criminal Data Act and it was required to (i) inform data subjects whose data has been disclosed to Clearview AI (if confidentiality rules allow) and (ii) make

[102] Kristof Van Quathem & Anna Oberschelp de Meneses, *French Supervisory Authority Publishes Guidance on Facial Recognition*, COVINGTON: INSIDE PRIVACY (Nov. 18, 2019), https://www.insideprivacy.com/data-privacy/french-supervisory-authority-publishes-guidance-on-facial-recognition [https://perma.cc/3LF3-MC3Z].

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Statement: Live Facial Recognition Technology in King's Cross*, INFO. COMM'R. OFF. (Aug. 14, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/ [https://perma.cc/PK56-BT5W].

[110] *Police Unlawfully Used Facial Recognition App*, https://www.imy.se/en/news/police-unlawfully-used-facial-recognition-app/.

[111] *Id.*

sure that Clearview AI deletes all the data it receives from the Police.[112]

Meanwhile, the Danish DPA's approval of facial recognition for a soccer stadium marks one of the first instances of valid private sector use. On July 13, 2019, Danish soccer club Brøndby IF announced that, beginning in July 2019 and with the approval of the Danish DPA, it would deploy facial recognition technology at Brøndby Stadium to identify individuals banned from attending soccer matches held at the stadium.[113] This development is notable, because "it appears to be one of Europe's first large-scale, private systems created and vetted in the era of GDPR."[114] The Danish DPA has provided that, in accordance with Article 9 of the GDPR, Brøndby Stadium's "processing . . . to enforce a private ban list is necessary for reasons of substantial public interest, and . . . the processing is proportionate to the aim pursued."[115] Moreover, the DPA stressed that facial recognition technology "would allow for more effective enforcement of the ban list compared to manual checks, and that this could reduce the queues at the stadium entrances, lowering the risk of public unrest from impatient football fans standing in queues."[116]

B. United States

As opposed to the uniform framework for facial recognition technology in Europe, the US largely does not regulate such technology at the federal level for public and commercial use—state and local level governments have set forth some regulatory schemes governing the public sector.[117] To assuage concerns of possible civil rights intrusions that may follow from mass surveillance technology, local governments, in particular, have been enacting legislation pertaining to the circumstances under which facial recognition can be used.[118]

1. Public Use

While federal laws generally have not set forth use parameters for facial recognition

[112] *Id.*

[113] Jesper Lund, *Danish DPA Approves Automated Facial Recognition*, EDRI (Jun. 19, 2019), https://edri.org/danish-dpa-approves-automated-facial-recognition [https://perma.cc/Z99A-KF98]. Specifically, facial recognition would be implemented in the form of cameras at Brøndby Stadium's entrances and used to identify individuals banned from attending soccer matches held at the stadium, which has a vandalism and general mayhem connected with certain matchups. *Id.*; Sidsel Overgaard, *A Soccer Team in Denmark is Using Facial Recognition to Stop Unruly Fans*, NPR (Oct. 21, 2019), https://www.npr.org/2019/10/21/770280447/a-soccer-team-in-denmark-is-using-facial-recognition-to-stop-unruly-fans [https://perma.cc/5XJP-QBR5]. The ban list contains approximately fifty individuals, and the facial recognition technology would screen an average of fourteen-thousand per soccer match. Lund, *supra*. Strict parameters for use would also be in place, which includes (1) deleting captured facial images at the end of the game day, (2) ensuring that the system is not connected to the Internet, and (3) implementing a cross-check to prevent false positives. Overgaard, *supra*.

[114] Overgaard, *supra* note 113.

[115] Lund, *supra* note 113.

[116] *Id.*

[117] Overgaard, *supra* note 113.

[118] *See, e.g.*, Steve Milne, *Davis to Regulate Hi-Tech Surveillance*, CAPITAL PUBLIC RADIO (Mar. 21, 2018), http://www.capradio.org/articles/2018/03/21/davis-to-regulate-hi-tech-surveillance [https://perma.cc/7CMU-PSUK].

technology,[119] states, local agencies, and cities across the US—including San Francisco and Oakland in California as well as Somerville, Massachusetts—are increasingly addressing the issue on a sliding scale of imposing limitations or conditions on usage by city agencies or banning such technology entirely.[120] Reasons for restrictions on facial recognition technology range from the need for better understanding and training prior to usage[121] to a concern that such technology may not be accurate.[122]

Aside from a blanket ban or moratorium on usage of facial recognition technology, an examination of state statutes, city ordinances, and other local policies governing such technology under the broader umbrella of public surveillance reveals four additional—and at times, overlapping—approaches that have emerged: (1) limiting the circumstances that facial recognition can be used, (2) evaluating the technology against predefined principles or guidelines for appropriate usage, (3) ensuring public engagement and approval as a prerequisite to deployment of the technology, and (4) stipulating comprehensive requirements that combine aspects of the aforementioned three approaches.

a. Use Subject to Public Oversight

In March 2018, the city of Davis, California passed the "Surveillance Technology Ordinance," which sets limitations on the use of surveillance technology—including facial recognition technology—by city agencies, with the purpose of "impos[ing] safeguards to protect civil liberties and civil rights."[123] The Surveillance Technology Ordinance places significant power in the hands of the city council, entrusting it to evaluate appropriate use of the technology.[124]

As a threshold matter, use of such technology for a purpose not yet approved or procurement of new technology by city agencies is subject to a public hearing and city council approval, which balances the need to "investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City."[125] The city agency shall first submit to the city council a Surveillance Impact Report, which includes locations for deployment of facial recognition technologies and their potential impact

[119] For example, at the federal level, foreign individuals seeking entry to the US may be required to provide certain verification information, including biometric identifiers, though the relevant sections within the Code of Federal Regulations are silent as to implementation, i.e., circumstances or parameters government actors must abide by when collecting such information. *See generally* 8 C.F.R. § 235.1(f) (2013).

[120] Susan Crawford, *Facial Recognition Laws are Literally all Over the Map*, WIRED (Dec. 16. 2019), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map [https://perma.cc/VXS5-WNWR].

[121] Jessie Balmert, *Ohio Cuts Off Access to Facial-Recognition Database – For Now*, CINCINNATI ENQUIRER (Aug. 14, 2019), https://eu.cincinnati.com/story/news/politics/2019/08/14/ohio-cuts-off-access-facial-recognition-database-temporarily/2006517001 [https://perma.cc/7854-WKLE] ("Ohio Attorney General Dave Yost said . . . that he wants to train local police before giving them access to the system. Until then, he will reduce the number of users from 4,549 to fewer than 20 state investigators.").

[122] Letter from Rebecca Kaplan, Oakland City Council President, to Members of the City Council and Members of the Public (June 6, 2019), https://oakland.legistar.com/View.ashx?M=F&ID=7313849&GUID=19E37810-7388-432F-8764-F4213347FBD2 [https://perma.cc/B5AG-KC2C] ("[F]ace recognition technology runs the risk of making Oakland residents less safe as the misidentification of individuals could lead to the misuse of force, false incarceration, and minority-based persecution").

[123] DAVIS, CAL., MUNICIPAL CODE art. 26.07.010 (2018); Milne, *supra* note 118.

[124] *See, e.g.,* DAVIS, CAL., MUNICIPAL CODE art. 26.07.030, 26.07.060.

[125] *Id.* art. 26.07.030.

on civil liberties and civil rights,[126] and a Surveillance Use Policy, which includes a framework of rules for use and safeguards against unauthorized access to information.[127] In addition, city agencies using such technology must submit an Annual Surveillance Report each fiscal year, detailing information including complaints about usage, crime statistics, and specifics regarding where the technology was deployed or installed.[128] The city council must again balance the need to investigate crimes against civil liberties.[129]

Despite the restrictions, however, the Surveillance Technology Ordinance allows for the procurement or use of surveillance technology under exigent circumstances, albeit under temporary conditions.[130] Under exigent circumstances, the city agency seeking to procure or use such technology is bound by certain requirements including: (1) using the technology to respond only to the situation at hand, (2) ceasing use of the technology upon resolution of the situation, (3) keeping only relevant information, and (4) reporting usage of the technology to the city council upon resolution of the situation.[131]

i. Use (or Prohibitions) Under Specified Circumstances

State and local governments have issued guidance on instances where facial recognition may or may not be appropriate. On October 8, 2019, California governor Gavin Newsom signed Assembly Bill 1215 ("AB 1215") to amend the California Penal Code, specifically imposing a temporary ban throughout California on the use of facial recognition technology in law enforcement body-worn cameras.[132] Conversely, on July 25, 2019, the Detroit's Board of Police Commissioners issued an Updated Facial Recognition Directive 307.5 draft proposal ("Draft Facial Recognition Directive") to "establish acceptable use for the Detroit Police Department's . . . facial recognition software,"[133] whereby: (1) the technology can only be used on still images of individuals,[134] (2) the technology may be used to support an ongoing criminal investigation of violent crime or home invasion,[135] subject to reasonable suspicion that use of the technology on a particular person will provide relevant information on such crimes,[136] and (3) access to facial recognition technology is limited and requires usage approval as well as manual confirmation of images at varying stages of the investigation.[137]

[126] *Id.* art. 26.07.020, 26.07.030.

[127] *Id.* art. 26.07.020, 26.07.030.

[128] *Id.* art. 26.07.020, 26.07.060(a).

[129] *Id.* art. 26.07.060(b).

[130] *Id.* art. 26.07.050.

[131] *Id.*

[132] CAL. PENAL. CODE § 832.19 (2020).

[133] DETROIT BOARD OF POLICE COMMISSIONERS, UPDATED FACIAL RECOGNITION DIRECTIVE 307.5 (2019).

[134] *Id.* § 307.5-1.

[135] *Id.* § 307.5-2.

[136] *Id.* § 307.5-3.

[137] *See, e.g.*, *id.* § 307.5-4(1).

ii. Use Subject to Established Principles

On December 10, 2019, the Port of Seattle, a government agency overseeing Seattle's maritime and aviation facilities, adopted a motion setting forth seven guiding principles ("Biometric Principles") for use of biometric technology that includes "the unique features of an individual's face" at facilities in the Port of Seattle.[138] The Biometric Principles were drafted after consultation with numerous parties, such as federal agencies, airlines, and immigration groups, and in response to U.S. Customs and Border Protection's use of facial recognition technology for international arrivals.[139]

As applied to facial recognition technology, usage should be "only for a clear intended purpose that furthers a specific operational need," and not for mass surveillance purposes.[140] Moreover, facial information should not be retained longer than necessary and should not be used or sold for commercial purposes without data subject consent.[141] Importantly, visitors to the Port of Seattle should have an option to opt-out of being subject to the technology.[142] To address concerns of possible discrimination or bias inherent within the technology (e.g., age, gender, race, etc.), the Biometric Principles require safeguards to ensure that facial recognition technology is accurate and not discriminatory against certain demographics.[143] The Biometric Principles also consider the need for accountability by requiring publicly-available reports on the performance and effectiveness of such technology.[144] Lastly, the Biometric Principles contain an ethics component for users of the technology, stating specifically that the Port of Seattle and affiliates should adhere to "key moral principles that include privacy, honesty, fairness, equality, dignity, diversity, and individual rights."[145]

iii. Comprehensive Approach

On March 12, 2020, Washington state's House and Senate ratified SB 6280 ("Washington FRT Bill"), a bill considered by legislators to be "one of the first and most comprehensive laws to regulate facial recognition technology in the nation,"[146] targeting state and local use of such technology.[147] Key highlights of the Washington FRT Bill include the need for government agencies to

[138] PORT OF SEATTLE, MOTION 2019-13 (2019).

[139] *Port of Seattle Becomes First U.S. Port to Adopt Principles Limiting Facial Recognition*, PORT OF SEATTLE (Dec. 11, 2019), https://www.portseattle.org/news/port-seattle-becomes-first-us-port-adopt-principles-limiting-facial-recognition [https://perma.cc/45PT-AZ84].

[140] MOTION 2019-13, *supra* note 126, at 1-2.

[141] *Id.* at 2.

[142] *Id.*

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] Khari Johnson, *Washington Privacy Act Fails Again, but State Legislature Passes Facial Recognition Regulation*, VENTUREBEAT (Mar. 12, 2020), https://venturebeat.com/2020/03/12/washington-privacy-act-fails-in-state-legislature-again [https://perma.cc/BB9W-FYUT]; Mariella Moon, *Washington State Approves Stronger Facial Recognition Regulations*, ENGADGET (Mar. 13, 2020), https://www.engadget.com/2020-03-13-washington-facial-recognition-regulations.html [https://perma.cc/W4CU-EYQN].

[147] ESSB 6280 FINAL S.B. REP., 66th Leg., at 2, (Wash. 2020).

file with a legislative authority a notice of intent to use facial recognition technology[148] and an accountability report, which must include: (1) the proposed use of the technology;[149] (2) a data management policy that includes how and when the technology will be deployed, data integrity and retention policies;[150] and (3) a "description of any potential impacts . . . on civil rights and liberties, . . . and the specific steps the agency will take to mitigate the potential impacts and prevent unauthorized use."[151] The Washington FRT Bill also notes that, where the technology is used "to make decisions that produce legal effects" concerning consumers, such as financial services or employment, human review should be available to assess the decisions.[152] Additionally, government agencies may not use the technology for surveillance unless (1) a warrant is obtained, (2) exigent circumstances exist, or (3) a court order is obtained to assist in locating a missing person or identify a deceased person.[153] With respect to law enforcement, the Washington FRT Bill state and local law enforcement agencies may not use findings derived from facial recognition technology alone to establish probable cause.[154] Finally, the Washington FRT Bill prohibits using facial recognition technology on individuals "based on their religious, political, or social views or activities, participation in a particular noncriminal organization or lawful event, or actual or perceived race, ethnicity, citizenship, place of origin, immigration status, age, disability, gender, gender identity, sexual orientation, or other characteristic protected by law."[155]

2. Commercial Use

In the commercial sector, there are presently no laws that specifically address use parameters for facial recognition technology, though three states—Illinois, Texas, and Washington—have enacted legislation governing the collection and use of biometric information, which generally encompasses facial recognition technology.[156] Such state statutes, however, govern facial recognition technology from an information privacy perspective, which implements a "Notice and Choice" framework, whereby data subjects are presented with a private entity's terms that explain rules for collection and usage and have a choice whether to accept such terms.[157]

With the dearth of legislation governing appropriate use of facial recognition technology, government agencies have responded by releasing best practice principles and codes of conduct on use of facial recognition technology. For example, the Federal Trade Commission issued a 2012 staff report

[148] S.B. 6280, 66th Leg., 2020 Regular Sess. § 3(1) (Wash. 2020).

[149] *Id.* § 3(2)(c)(i).

[150] *Id.* § 3(2)(d)(i)-(iii).

[151] *Id.* § 3(2)(d)(vii)(g).

[152] *Id.* § 5.

[153] *Id.* § 11(1)(a)-(c).

[154] *Id.* § 11(5).

[155] *Id.* § 11(2).

[156] James Fullmer, *Proposed South Carolina Biometric Legislation Could Break New Ground*, JD SUPRA (Jan. 31, 2020), https://www.jdsupra.com/legalnews/proposed-south-carolina-biometric-56026 [https://perma.cc/MVD2-XDQ8]. *But cf.* INSIDE PRIVACY, *Washington Becomes the Third State with a Biometric Law*, INSIDE PRIVACY (May 31, 2017), https://www.insideprivacy.com/united-states/state-legislatures/washington-becomes-the-third-state-with-a-biometric-law [https://perma.cc/5HM8-2N77] (noting that "Washington's definition does not specifically provide for a 'scan of hand or face geometry'" . . . suggesting that the statute will have limited application in the context of facial recognition technology").

[157] Warner & Sloan, *supra* note 10, at 373-74.

on best practices for facial recognition technology in the commercial sector.[158] Similarly, the National Telecommunications and Information Administration began a privacy multistakeholder process to develop a voluntary code of conduct for facial recognition technology, culminating in a set of guidelines in 2016 entitled, "Privacy Best Practice Recommendations for Commercial Facial Recognition Use."[159] However, these recommendations and guidelines also focus on privacy considerations with respect to "Notice and Choice" and do not set forth allowable use perimeters.[160]

Notwithstanding the above, companies like Microsoft have responded to government regulators' relative lack of guidance on facial recognition technology by proposing, in part, to adhere to self-regulatory principles until legislative action sets clear boundaries for usage.[161] Indeed, Microsoft has already developed certain principles that include the need to minimize bias and discrimination which may be inherent in the technology, as well as accountability in the form of manual review of facial identifications and the establishment of communication channels for data subjects to voice their concerns.[162] Crucially, Microsoft's principles also address the area of law enforcement within the arena of public use, noting that such of the technology is appropriate under only three scenarios: (1) where there are laws that regulate parameters for use in public areas, (2) where a court order authorizes use to surveil a specified individual in a public space, and (3) where there is imminent risk of harm to a person.[163]

IV. CONCLUSION – WHAT IS THE ROAD AHEAD FOR CHINA?

Despite the widely shared questioning of China's use of facial recognition for surveillance and control by international observers, Chinese legislators are not pressured to reduce such use. Domestically, as recent research shows, Chinese citizens seem to favor convenience and improved security, just like citizens from Germany, the UK, and the US.[164] To be sure, facial recognition has been used in China far more extensively than in EU and the US. It also means that the lack of a comprehensive framework to address infringement of individual rights and other negative impacts have

[158] *See generally* FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (2012).

[159] NAT'L TELECOMM. & INFO. ADMIN., PRIVACY MULTISTAKEHOLDER MEETINGS REGARDING FACIAL RECOGNITION TECHNOLOGY: FEBRUARY – JUNE 2014 (2013), https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-meetings-regarding-facial-recognition-technology-feb [https://perma.cc/YV96-HNBR]; CONSUMER FED'N OF AM., *Statement on NTIA Privacy Best Practice Recommendations for Commercial Facial Recognition Use* (Jun. 15, 2016), https://consumerfed.org/press_release/statement-ntia-privacy-best-practice-recommendations-commercial-facial-recognition-use [https://perma.cc/5ERX-GGF3].

[160] *Id.*

[161] *See* Brad Smith, *Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility*, MICROSOFT (Jul. 13, 2018), https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility [https://perma.cc/5ECL-VXZ2].

[162] *See* MICROSOFT, SIX PRINCIPLES FOR DEVELOPING AND DEPLOYING FACIAL RECOGNITION TECHNOLOGY (2018), https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf [https://perma.cc/2DH4-AQXY].

[163] *Id.*

[164] *See* Kostka et al., *Between Privacy and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the UK and the US*, 30 PUB. UNDERSTANDING SCIENCE 671, 683 (2021), https://journals.sagepub.com/doi/pdf/10.1177/09636625211001555 [https://perma.cc/W3GE-2LUN].

caused tangible negative consequences.[165] Chinese legislators are pressured to handle the negative consequences, which builds up social tensions and endangers the acceptance of the technology. Tensions continue to grow due to the mandatory usage of facial recognition in many fields, such as telecom companies' requirement for mobile phone users to submit to facial recognition scans when registering new SIM cards and the deployment of facial recognition in the subway stations.[166] The need for a comprehensive regulatory framework to guide the use of facial recognition can also be seen in the unusual attention that a pending case between a Hangzhou resident and a wildlife park has attracted, where the wildlife park required ticket-holders to submit to facial recognition technology in order to enter into the park, a requirement that was viewed as disproportionate by the plaintiff.[167] The court's decision was widely viewed as inadequately addressing the core issue.[168] The judicial interpretation issued by Chinese Supreme People's Court could be seen as a further response to the need to address the issue.

Banning facial recognition does not appear to be a viable choice for Chinese legislators, given there has no precedent that they made laws to roll back from a policy to encourage the use of any technology made by other government branches. Their policy views seem to be vindicated by the lessons learned in other countries. The recent bans or moratoriums on facial recognition by some local authorities in the US have caused consequences that regulators did not intend.[169]

[165] Society is reluctant to accept facial recognition-based payment methods due to worries regarding privacy and security. *See* Mo Zhang & Yuhan Chen, *Yidong Zhifu Yonghu Dui Shengwu Shibie Jieshou Qu Wending* (移动支付用户对生物识别接受趋稳定) [Mobile Payment Users' Acceptance of Biometrics Stablizes], PEOPLE'S DAILY (Jan. 14, 2020), http://money.people.com.cn/n1/2020/0114/c42877-31547626.html [https://perma.cc/N7WE-RBZN]; Shua Lian Zhifu Anquan Yinhuan Yin Ren Shensi, *Sheng Wen Shibie Dongtai Youshi Tuxian* (刷脸支付安全隐患引人深思，声纹识别「动态」优势凸显) [The Dangers of Facial Recognition Payments are Thought-Provoking, the Advantages of Dynamic Voice Recognition are Highlighted], JIQIZHIXIN (Oct. 10, 2019), https://www.jiqizhixin.com/articles/2019-10-09-12 [https://perma.cc/WK2F-BZ3N].

[166] *Beijing Subway to Use Facial Recognition Technology*, CHINA DAILY (Oct. 29, 2019), https://www.chinadaily.com.cn/a/201910/29/WS5db7d16fa310cf3e35574357.html [https://perma.cc/EY6J-JDYZ]; Echo Xie, *China Launches Facial Recognition for Mobile Phone Users*, S. CHINA MORNING POST (Dec. 1, 2019), https://www.scmp.com/news/china/politics/article/3040134/china-launches-facial-recognition-mobile-phone-users [https://perma.cc/5WTU-5QFJ].

[167] Kerry Allen, *China Facial Recognition: Law Professor Sues Wildlife Park*, BBC (Nov. 8, 2019), https://www.bbc.com/news/world-asia-china-50324342 [https://perma.cc/F8CE-6JRV].

[168] The official website of the Supreme People's Court reported on the decision. *See Yu Jianhua Zhong Fa, "Ren Lian Shibie Di Yi An" Ershen Xuanpan* (*"人脸识别第一案"二审宣判*) [*"Facial Recognition First Case" Sentenced in the Second Instance*], PEOPLE'S CT. NEWS (Apr. 10, 2021), https://www.chinacourt.org/article/detail/2021/04/id/5956124.shtml [https://perma.cc/KRN3-KAR8]. The public discussion questioned the court's opinion that the park authority's mandatory facial recognition requirement was not included in the contract, and the court declined to review its legal validity. *See, e.g.*, *"Ren Lian Shibie Di Yi An" Guo Bing Shenqing Zaishen, Cheng "Yuan Panjue Falu Shiyong Cuowu"* ("人脸识别第一案"郭兵申请再审，称"原判决法律适用错误") [*Guo Bing, the "First Case of Face Recognition," Applied for a Retrial, Saying that "the Original Judgment Law Applied Incorrectly*]*,"* S. METROPOLIS DAILY (Apr. 11, 2021), https://www.sohu.com/a/465863565_161795 [https://perma.cc/2FC4-TD2P].

[169] For instance, San Francisco's ban of government use of facial recognition technology inadvertently made it illegal for city employees to use iPhones with Face ID. *See* Bani Sapra, *San Francisco is Changing its Facial Recognition Ban After it Accidentally Made the iPhones it Gave to City Employees Illegal*, Bus. INSIDER (Dec. 19, 2019), https://www.businessinsider.com/san-francisco-amended-its-facial-recognition-ban-2019-12 [https://perma.cc/2VJ5-7EAC]. Some claim Illinois's Biometric Information Privacy Act (BIPA) resulted in unintended, overreaching restrictions on business practices. *See* Lauren Harrison, *When Do Privacy*

What IS the Road Ahead for China?

Given the negative consequences and the social tensions with the deployment of facial recognition, Chinese legislators need to make rules that establish basic rights for individuals. These rules, in addition to guiding the commercial collection, use, and security of biometric data through a more robust privacy regime, should also address a number of key issues specific to public use of facial recognition in China. For example, there should be discussions about the government's access, including local governments, to commercial databases that contain detailed geolocation data about individuals derived from facial recognition systems operated by a wide range of service providers, ranging from telecom providers to banks to ride-hailing platforms. In addition, oversight of appropriate law enforcement activities, such as detailed approval procedures before the deployment, as well as judicial remedies after the fact, should also be included in the rulemaking discussions. Finally, questions about transparency of public uses should also be discussed -for example, whether the deployment of such a technology in public space should be disclosed, whether details of the deployment such as information on which government agencies are deploying it, what are the types of data collected and processed, and how long such data will be retained. Without these discussions, it is unlikely that a comprehensive framework could be developed.

In addition to formal rulemaking, the Chinese standardization authority has started to explore a risk management approach towards the deployment of AI technologies, which include facial recognition. In 2018, it published a white paper recommending a tailored risk-management system for activities with various risk levels.[170] This risk-based framework could further support the formal rulemaking process in China by allowing regulators to assess the risks associated with various uses and ensure that public or private entities looking to deploy this technology understand these risks and build up governance structures and protocols to manage them.[171]

Regulations Go Too Far?, GOV'T TECH. MAG., https://www.govtech.com/opinion/when-do-privacy-regulations-go-too-far.html (last visited Nov. 26, 2021). *See also* Jack Lavin, Letter to the Editor, *Flawed Illinois Law Protecting Biometric Data Leads to Frivolous Lawsuits Against Businesses*, CHI. SUN-TIMES (Mar. 31, 2021), https://chicago.suntimes.com/2021/3/31/22360388/bipa-biometric-information-privacy-act-illinois-chamber-of-commerce [https://perma.cc/BC6Z-W65N]. *But see* Editorial, *Don't Gut Illinois Law That Prohibits the Secret Sale of Our Fingerprints and Other Biometric Information*, CHI. SUN-TIMES (Mar. 16, 2021), https://chicago.suntimes.com/2021/3/16/22334405/biometric-protection-bipa-illinois-law-legislation-editorial [https://perma.cc/HJQ6-ML2B].

[170] CHINA ELEC. STANDARDIZATION INST., RENGONG ZHINENG BIAOZHUNHUA BAIPISHU (2018 BAN) (人工智能标准化白皮书 (2018 版)) [WHITE PAPER ON STANDARDIZATION OF ARTIFICIAL INTELLIGENCE (2018 EDITION)], 42-54 (2018).

[171] A recent guideline, issued on January 5, 2021 by the Secretariat of National Information Security Standardization Technical Committee ("TC 260"), the Practice Guidelines for Cybersecurity Standards - Guidance for Ethical Security Risk Prevention of Artificial Intelligence, is a step further towards forming a risk-based framework. This guideline offers relevant business organizations, academic institutions, and individuals to carry out artificial intelligence research and development, design and manufacturing, deployment and application and other related activities. *See* SECRETARIAT OF NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE, WANGLUO ANQUAN BIAOZHUN SHIJIAN ZHINAN – RENGONG ZHINENG LUNLI ANQUAN FENGXIAN FANGFAN ZHIYIN (网络安全标准实践指南 – 人工智能伦理安全风险防范指引) [PRACTICE GUIDELINES FOR CYBERSECURITY STANDARDS – GUIDANCE FOR ETHICAL SECURITY RISK PREVENTION OF ARTIFICIAL INTELLIGENCE] (2010), https://www.tc260.org.cn/file/zn10.pdf [https://perma.cc/N6HE-Y6WM].