null • Summer 2021

Public Debate on Facial Recognition Technologies in China

Tristan G. Brown[1], Alexander Statman[2], Celine Sui[3]

[1]History Faculty, Massachusetts Institute of Technology,
[2]School of Law, University of California, Los Angeles,
[3]Department of History of Science, Medicine, and Technology, Johns Hopkins University

Published on: Aug 10, 2021

DOI: 10.21428/2c646de5.37712c5c

ABSTRACT

China's ascent on the global stage in the fields of artificial intelligence (AI) and facial recognition has been widely noted in Western-language scholarship and media. Much of the attention has focused on the applications of these technologies in government security systems and their geopolitical implications. Here, we seek to explore the private and domestic uses of facial recognition. What dynamics inform popular debates about the use and applications of these technologies in China, and how do they fit into a more global picture? We present a series of cases from the past three years in which facial recognition software attracted media attention in legal, commercial, and educational settings. Acknowledging that China is far too large and diverse for there to be just one dynamic at play, we propose that while debates about facial recognition have indeed become more common, there is still broad-based public support for uses that promise increased security or convenience. The state has been selectively receptive to limited critique, but typically in a manner that preserves its active role in shaping the contours of public discussion.

Keywords: *facial recognition, Chinese law, social media*

Tristan G. Brown
History Faculty, Massachusetts Institute of Technology

Alexander Statman
School of Law, University of California, Los Angeles

Celine Sui
Department of History of Science, Medicine, and Technology, Johns Hopkins University

Learning Objectives

- Introducing students to the diversity of ways that facial recognition is debated in global contexts, particularly around discussions of "beneficial" and "harmful" uses of technology.

- Bringing China into the conversation about technology and ethics for students so that they understand what's broadly similar between China's case and those of other countries, as well as what's different.
- Encouraging students to consider tension between ethics and law through the case of facial recognition technology.
- Getting students to think about the circumstances under which publics notice and voice concerns against certain technologies, as well as the risks and rewards of participation in debates surrounding them.
- Allowing students to critically examine the role that governments could play in shaping the narratives around the ethical implications of deploying emerging technologies by both state and private actors.

Introduction

In January of 2021, the results of a survey about facial recognition appeared on the Chinese-language news website Beijing News Think Tank. The survey found that, out of the 1,515 anonymous respondents to a questionnaire, over 87 percent opposed the use of facial recognition technology for payments in commercial settings such as malls and retail streets, citing as a principal reason their mistrust in the private companies that supplied the facial recognition algorithms. English-language articles covering the survey's results soon followed, with one titled "Facial Recognition Is Used in China for Everything from Refuse Collection to Toilet Roll Dispensers and Its Citizens Are Growing Increasingly Alarmed, Survey Shows."[1] A similar survey from 2019, covering 6,152 respondents, found that approximately 80 percent of respondents were concerned about personal data protection in relation to facial recognition. The results of this survey were also reported in English-language media, and with similar conclusions (for example: "China Survey Shows High Concern over Facial Recognition Abuse").[2]

A reader following the media trail in English might reasonably assume that the results of these small-batch surveys were indicative of increasing concern in China about the "surveillance state." While acknowledging this possibility, we suggest an alternative reading in which public concern is primarily directed toward specific kinds of private uses, indicating that the ultimate authority of the state to use facial recognition technology is broadly accepted. Our goal is to identify instances of public debate about facial recognition in China and to offer some preliminary observations about the contexts in which it occurs and the ways in which the state responds. We also seek to

place these analyses in a broader global context to help illuminate what is and what is not specific to the Chinese case.

Facial recognition technologies in China have been adopted not only by state institutions but also by a wide range of private enterprises. They are today woven into digital payments, hospital waiting rooms, housing complexes, transportation systems, and urban policing.[3] Facial recognition technologies are widely appreciated by the general public when they are understood as providing increased convenience and security: for example, faster, cashless commercial payments, or skipping the security queue at metros, libraries, train stations, airports, and so on. On the other hand, challenges are more likely to occur when facial recognition is deployed by for-profit companies in ways that are perceived to interfere directly in individuals' daily lives without saving them time or increasing their security. Indeed, one commentator has called the corporate collection of biometric data in China a "free for all."[4] An important caveat comes from source bias: debates that are permitted to remain online may align with the central government's objectives, so are much more likely to capture challenges to commercial uses of the technology than those of the state. Nevertheless, this fact is itself significant, because it reveals how the state controls the narrative about facial recognition technologies by allowing limited protest and dissent.

In China as in other countries, different legal standards apply to the public and private uses of facial recognition. State security organs can essentially collect any information deemed necessary in public places or when investigating a crime. By comparison to the United States, there is a relatively weaker system of privacy laws protecting citizens from police investigation and criminal procedure laws regulating the actions of law enforcement.[5] Police do have a duty to keep personal information—including biometric information—confidential, but the constraints on how they collect or use it internally are minimal. For this reason, most public debate in China about facial recognition rather concerns its use by private organizations, including for-profit businesses and residential complexes. That said, the role of private organizations aligns with the state in different ways. Their use of facial recognition technology tends to be accepted most when it contributes to two state priorities widely accepted as legitimate: increased security and general convenience.

A central theme of domestic Chinese media is public safety at the local level. With frequent reports on mass shootings in the United States, political turmoil elsewhere, and the global spread of Covid-19, it is not rare to encounter the view that China "is the safest country in the world."[6] Without interrogating the accuracy or transparency

of the country's official crime statistics, it is safe to say that this focus on "public safety" has become an especially important part of the national narrative under the leadership of Xi Jinping. The widespread rollout of facial recognition technology by public security organs in the country have in fact been correlated with official directives toward improving public safety.

The rollout of facial recognition technologies has also been framed and understood as enhancing user convenience, especially in the case of cashless payments, which are today ubiquitous in China. In other instances, facial recognition allows individuals to go about their business with less disruption due to identity checks that already occur anyway. In the United States after the September 11 terrorism attacks, increased security measures often resulted in inconvenience for passengers traveling in airports or attending large venues. Something similar exists in China, where security checkpoints are common in metro systems and train systems. Since facial recognition technology can make security checks both quicker and more thorough, these government uses of facial recognition technology are sometimes cited as increasing security and convenience at the same time—which is a powerful narrative arc to foster support for its adoption.

The Development and Regulation of Facial Recognition in China and Beyond

The development of facial recognition technology in China has followed a pathway from early pioneers, through state support for new breakthroughs, to full national rollout. In the 1980s and 1990s, many of the current leaders in the industry, such as Tang Xiao'ou □□□ who received his PhD from MIT in 1996, completed their degrees abroad before returning to lay the foundation for improvements of existing models and later technological breakthroughs.[7] As early as 1989, the Ministry of Public Security commissioned Su Guangda □□□, Tsinghua University Professor of Electrical Engineering, to undertake a research project called the "Computer Portrait Combination System." After many years of academic labor, Su's integrated facial recognition system was nationally tested in 2005, with the first facial database containing over ten million faces completed by the 2008 Beijing Olympic Games.[8]

The year 2014 marked major advances in facial recognition technology globally. In March of that year, Facebook announced that its DeepFace algorithm, which for the first time integrated deep learning with facial verification to identify humans in digital images, reached a record accuracy rate of 97.35 percent on the Labeled Faces in the

Wild benchmark.[9] That same year, Tang Xiao'ou □□□ led a research team at the Chinese University of Hong Kong to surpass Facebook's record with an accuracy rate of 98.52 percent, marking the first time that artificial intelligence (AI) surpassed human-level performance.[10] In October of 2014, Tang monetized the algorithms by founding SenseTime, which went on to become the world's most valuable artificial intelligence company in the late 2010s.[11]

The technological breakthroughs of the mid-2010s provided avenues for the mass use of facial recognition, including new mechanisms for state surveillance. There has been a complex picture emerging across the country, with major private capital investments in AI startups, the development of technical infrastructure that supports mass data collection, the widespread use of facial recognition in the public and commercial sectors, and most notoriously, the state rollout of the technology to monitor and police minority ethnic groups. In 2016, Chen Quanguo □□□ was appointed as Communist Party Secretary of the Xinjiang Uyghur Autonomous Region from his previous post in Tibet. His tenure has seen the creation of what the state refers to officially as "Xinjiang Vocational Education and Training Centers" in the region, as well as the widespread rollout of facial recognition technologies to police the area.[12] This usage is usually grouped together in government reports with discussions of public security. Its full extent is unknown, both to the public and to academic observers.

While there is yet no law specifically regulating the use of facial recognition in China, a variety of existing laws, including the 2020 Civil Code and the 2017 Cybersecurity Law, have been cited by Chinese courts in decisions to regulate the private collection and distribution of individuals' facial data. Also important are the Personal Information Security Standards, which are noncompulsory guidelines issued for the benefit of both state and nonstate actors. Current legal custom may become more explicit in 2021, if a newly proposed law, the Personal Information Protection Law (PIPL), which concerns the commercial use of facial recognition technologies, is passed.[13]

This proposed law would have two important consequences. First, it would restrict the use of facial recognition data collection in commercial public venues to circumstances where it is in the interests of "public security" as defined by the state. Second, it would require that signage is installed to make clear that such collection is occurring and prevent the further distribution of the information without explicit consent.[14] But there are important caveats to each provision: the boundaries of public security are amorphous, and public consent for such measures has not historically been difficult to

attain. An additional section even places some restrictions on state organs, which "may not exceed the scope or extent necessary to fulfill their statutory duties and responsibilities"—though it must be remembered that determining such scope and extent remains the state's unique prerogative.[15] In sum, the proposed law would make it easier for the state to crack down on private uses of the technology, while addressing the public's concerns about certain abuses of personal data.[16]

China's use of facial recognition is not simply a Chinese story. American companies have become involved in ethical debates about China's use of facial recognition as they attempt to navigate their own uses of it, and legal standards across the board remain murky. In 2019, four US-based researchers wrote to the publisher Wiley to retract a scientific paper containing algorithms that had been used to track members of the Uyghur ethnic group in China.[17] MIT in particular has come under scrutiny for its associations with AI companies, such as SenseTime and iFLYTEK, which have allegedly deployed such technologies against ethnic minorities within China.[18] Cases such as these have dominated Western media coverage of China's facial recognition rollout; needless to say, coverage within China has been different. While Western reports have largely questioned private technology companies collaborating with the Chinese state for surveillance purposes, Chinese domestic discussion has often demanded increased state oversight over private companies. Our aim is not to interrogate which emphasis is legally or ethically desirable, but rather to introduce audiences to the diversity of ways this technology has been debated in global contexts.

One assumption common to media reports in Western countries is that China's rollout of facial recognition is uniquely dystopian. Yet, the legal and regulatory problems China faces as well as the ambiguities surrounding them are in the abstract not so different from the United States or Europe. In the United States, for example, some states make it illegal for private enterprises to use a person's facial biometric data without their consent, while others do not. The European Union and European Economic Area's General Data Protection Regulation (GDPR), in effect since May 2018, safeguards personal biometric data for EU citizens both in Europe and abroad and prevents their data from being transferred to a third country. But even in Europe, it remains undetermined whether the regulations appertain to biometric data transferred into the EU from non-European citizens abroad, how it applies to "transient" (not personally identifiable) data, and how it extends to academic research contexts.[19]

The major differences between China and US cases concern their respective constitutional frameworks and relatedly, the terms of the public debate. In the United States, the Bill of Rights bakes legal protection of the individual from the state into the Constitution. Public debate often reflects this reality, as seen from the recent political controversies over vaccine passports. Debates in the United States have also touched upon the important issue of race, particularly in relation to algorithmic unfairness in facial recognition technologies.[20] This dimension has been generally absent in domestic discussions within China, the use of the technology on minority groups notwithstanding. Furthermore, US courts are to some degree independent from the political system, which is not the case in China. The terms and emphases of possible debate are different, and some aspects of China's facial recognition rollout, particularly in the context of public security, have been relatively off-limits to public discussion. Nevertheless, state law and the legal system, as we will see below, does really matter in China, even if it is intrinsically intertwined with the party-state, and it is unwise to assume that China represents a national example that cannot offer lessons and reflections for Western countries on the subject of facial recognition.

In recent years, there have been several major incidents involving facial recognition within China that sparked considerable domestic discussion. We profile four such cases. Each of these cases was widely discussed in state-owned media or on state-monitored social media, which are the major venues for Chinese citizens to access news and analysis. Each case therefore represents a controversy that the central government is willing to countenance, if not condone. For this reason, it should be assumed that they do not reflect the full range of private opinion. Nonetheless, the four following cases are of interest because they show the wide social spectrum of issues related to facial recognition in China today: from its uses in business, education, and security, to its discussion in traditional broadcast news, online social media, and the legal system. What these uses and discussions on the whole suggest is that some apparent skeptics of facial recognition may actually be in favor of more central government oversight and regulation—not less. This explains why certain discussions of facial recognition technology are taken seriously and more often than not addressed by the government.

Case Study One: A Wildlife Park

In 2019, a law professor at Zhejiang Polytechnic University, Guo Bing □□, sued the Hangzhou Wildlife Park, a private business located in Zhejiang Province, for allegedly violating the country's consumer protection law by collecting visitors' individual data

through facial recognition. In past years, Professor Guo had used fingerprints to enter the park's premises, but in October of 2019, he learned that it had become mandatory for guests to register using the organization's facial recognition system. That is, the enterprise shifted to a facial recognition system to record visitors entering the park. Following the widely reported acceptance of Guo's case by the Fuyang District People's Court in Hangzhou, the court ruled that the park had to refund his membership fee and delete all of his facial data—including his original photograph—from their visitor log information system.[21] An additional ruling on Guo's case issued by the same court ordered the zoo to further delete Guo's fingerprint data, which had been previously collected with his given consent.[22]

Guo's case has been identified by Chinese domestic media as the "first court case involving the use of facial recognition in China."[23] The case was expected to hinge on the Personal Information Security Standards, which involved the question of whether the park had acted in accordance with the three principles of "legality, validity, and necessity" for the private collection of personal data from consumers. However, in its final ruling, the court largely sidestepped these broader questions, centering instead around contractual obligations and user consent. The court simply ordered the park to delete the facial information that had been collected, on the principle that the park's shift from fingerprint identification to facial recognition—which Guo did not accept—breached the existing service contract represented by his annual park membership card.[24] The rulings did not prohibit the park from collecting facial data, though the park had apparently moved to a voluntary opt-in, opt-out system even before the case was heard by the district court. The court also denied Guo's substantive claim that collecting facial information without his permission constituted a violation of the three principles. It is worth stressing the limited implications of this single case, which did not address the conditions under which facial recognition technology could be deployed by private enterprises. What it did indicate is only that under certain circumstances, private parties should obtain consent before collecting facial recognition data.

The "first facial recognition case" in China attracted significant attention on the Chinese internet. This attention is itself significant, as we may surmise from its remaining online that the state allowed a degree of debate on the matter, thus raising the domestic public's awareness of the state's oversight of data protection and user consent. Aforementioned surveys have revealed specific public concerns over the potential lack of proper contractual procedures in facial data collection by private

enterprises.[25] In this case, the state, as represented by the courts, played the role of social protector by enforcing a degree of consumer protection, and then encouraged a broader conversation about it. Though legal experts have expressed reservations over the legal impact of this ruling, from a political perspective there was widespread support for the court's decision among citizen commentators, as seen in the following comments on the Chinese social media website, Weibo. (See Figure 1.) It appears therefore that citizens might be less concerned about establishing general legal conditions under which facial recognition activities can take place than in ensuring that they have some measure of say with regard to their own participation.[26]

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

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

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

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

Figure 1. Top responses on Weibo to news report on the court's decision regarding uses of facial recognition technology at the Hangzhou Wildlife Park.

Case Study Two: Monitoring Students

In 2019, China Pharmaceutical University, a public institution of higher education located in Jiangsu province, rolled out a facial recognition system in some classrooms to monitor student attendance and classroom performance. It was quite extensive and powerful, even able to detect students dozing off in class. Local pushback followed, with student members of the school community and other online commentators expressing skepticism about the proposal. Despite this pushback, the university stayed firm. The spokesperson justified its plans with a vague reference to public security, claiming that the university constituted a public space in which comprehensive

surveillance was warranted.[27] In this case, too, the state's action was limited, though on balance it seems to have sided slightly more with the party using facial recognition technology. The Ministry of Education in Beijing ultimately responded with the promise to roll out such a plan with caution, and as of the time of writing, the system was still being rolled out.[28]

Online pushback against the measure revealed that opposition was particularly strong to the use of facial recognition in the classroom setting. These cameras went beyond merely identifying students. They were intended rather as a disciplinary tool to monitor student behaviors, such as class attendance, and emotions, such as levels of attention. Some students equated the presence of advanced surveillance technology in the classrooms to educational prisons. Other commentators questioned the necessity of monitoring university students, who had already demonstrated self-discipline through their years of preparing for China's rigorous college entrance examination, the *Gaokao*. Some criticized the idea of prioritizing surveillance technologies over classroom upgrades. None, however, expressed a broad-based critique of facial recognition technologies per se.

In fact, the university already had a history of using facial recognition software, which was not only unopposed, but even broadly popular. Starting in 2019, facial recognition systems were installed at the main entrances, dormitories, and libraries for facilitated access and campus security. These measures were received quite positively by students, some of whom were relieved that forgetting their access cards in their dorm rooms was no longer a cause of concern. Pedestrian traffic flows were notably improved. University campuses across China had implemented similar measures, with no apparent problems. The new proposal at China Pharmaceutical University was, however, unique in also installing cameras in some classrooms for use in monitoring student behavior, and this was the specific issue that drove student and online dissatisfaction.[29] (See Figure 2.)

Knowledge Creation Circle (Weibo ID Name)

#University testing out classroom facial recognition# I feel that after the entrance of facial recognition into classroom learning…to be honest, it is a bit terrifying. There is no need to take attendance, every action, even if you accidentally doze off, is unobstructed [to the cameras], so going to school becomes more stressful than going to work. AI tech such as facial recognition + data analysis treats people like "machines," and it is very hard to control. The problem is that people are not machines. **Liked 37,506 times**

Top responses on Weibo to news reports on the rollout of facial recognition in classrooms

1. Of course it should be cancelled; it's too much of a violation of human rights! **Liked 2,750 times**

2. When I was in high school, I was very confused why the school didn't spend a few thousand RMB to install air conditioners for students, but instead chose to install 360-degree surveillance cameras that cost thirty-thousand each…with sixty students in a crowded classroom, during the summer the fans didn't work, and it was so hot that we were drenched in sweat. **Liked 3,070 times**

3. "Raising Pigs" made more digital and scientific. **Liked 2,531 times**

Figure 2. (Top) A post on Weibo regarding use of facial recognition technology at China Pharmaceutical University, in Jiangsu province. (Bottom) Top responses on Weibo to news reports about the uses of facial recognition technology in classrooms.

China Pharmaceutical University's use of facial recognition both in the classroom and outside it touches on a number of key themes at the forefront of discussions in the country today. It reveals a general acceptance and support for measures that are understood to improve security and facilitate convenience. At the same time, it reveals a degree of suspicion of uses that go beyond these functions. The use of cameras in classrooms potentially introduced the monitoring of students' individual behaviors, touching a nerve across the student body that continues to be debated online today. Yet, supporters have responded too, defending the use of facial recognition in classrooms as an opportunity to track students' learning. Ongoing discussion of the proper limits of facial recognition technology thus continues, allowing for diverse voices to express their opinions within a fairly tight set of parameters.

Even though freedom of speech is not explicitly mentioned in the Chinese press, much less by the courts, it is not unreasonable to think that it might have had some bearing on community opinion in an academic setting. There is no doubt that its deployment in the classroom could have the effect of changing what professors teach and students are willing to say. Indeed, one of the popular comments on this post did touch on the very sensitive notion of "human rights," implying that the students' rights to privacy were being violated by the deployment of the technology. The fact that the comment was not deleted by state censors further suggests a willingness to countenance some particularly harsh critiques within the specific context of an educational setting, where state control is already firm and where investment in the status quo more generally runs high.

Lest we give the impression that the collection of student facial data has been unique to China, there have been several instances of the harvesting of big data at American universities as well. As in China, universities—with large numbers of students who reappear again and again in camera shots—are tempting locations to mine facial data and experiment with new technologies. In 2016, Duke University released more than two million video frames of footage of students walking on the university campus. Scientists at Stanford University and the University of Washington have engaged in acts of data mining off-campus and published the information without explicit consent. Though much of this data was deleted in 2019 following national media attention, academic papers have continued to cite data gleaned from the image collections.[30] A real issue remains in the fact that it is not always possible to know when facial recognition is being used, since taking selective samplings of data from the images of generic security cameras is also technically feasible. In 2020, students at the University of Miami accused the school's administration of using facial recognition to identify student protesters in standard footage—a charge that the administration has denied.[31]

We might also point out that there are differences between the United States and China in terms of who has voiced dissatisfaction thus far. In the case of China Pharmaceutical University, concern came from online netizens and some of the students themselves. In the American context, where higher education is split between public and private institutions, pushback hitherto has largely come from journalists, activists, and academics who are concerned about the general uses and extensions of this technology. As of today, the University of Southern California, a private institution, is one of the only institutes of higher education in the country that has openly admitted to the institutional use of facial recognition technology within their campus security

systems. Upon its launch in 2020, the system sparked some heated campus discussion.[32] For most American students not enrolled at USC, the issue may not yet seem overly pressing. But if students confront enhanced uses of facial recognition on their campuses in the future, there may well be more pushback.

Case Study Three: Metro Security

In 2019, the Beijing Municipal Government announced plans to roll out facial recognition technology at security entrance checks in metro stations throughout the city, pitched as a way to increase user convenience by reducing lines at security checkpoints. The new protocol would use facial recognition to identify known passengers and divide them into groups based on their social credit rating needing different levels of security checks. The proposal was publicly opposed by Lao Dongyan □□□, professor of law at Tsinghua University, who called for a more formal legal framework for the implementation of facial recognition technology and the collection of personal data by both the government and private enterprises. In a widely circulated essay, Lao framed her argument in the following terms:

> Facial recognition involves the collection of biological data that is important for individuals, and relevant organizations or institutions must prove the legality of this practice before collection.…If the arbitrary adoption of internal standards to divide passengers into three, six, or nine classes and apply different security-check measures accordingly is implemented, we have reason to suspect that such a measure violates the principles of equity in the Constitution; it also violates the fundamental right to personal freedom for citizens.[33]
>
> [illegible]……[illegible]
> [illegible]

Professor Lao opposed facial recognition technology within a broader critique of the seemingly endless increase in public security investments and crime prevention measures. Nonetheless, as of March 2021, the system is being rolled out across Beijing as part of a public trial to cut down on wait-times at security checkpoints. Apparently, the government believes that increased convenience for individuals will be the best way to promote the measure.[34]

It should be pointed out that there is widespread misunderstanding of China's "social credit system" in the Western press. There exists no uniform credit score or nationwide integrated credit system. Instead, a variety of private point-based metrics

and local government systems exist across the country. The government's goal is to eventually link up successful private pilot programs within a national system that would ideally function as a kind of dual police record and credit score.[35] As conceived in the specific context of the Beijing metro, commuters with clean records would apply for a trial pass online and submit their facial recognition information. The plan would simply allow a fast track in metro security lines for people who have no history of bringing illegal items onto trains. Since most riders fall into this category, any "good social credit" record would essentially serve to keep its holder off of a blacklist of riders with a history of problems, who might be pulled aside for heightened checks. The result is that, although framed as a way to reward good social credit, the facial recognition system would actually function more to punish those with bad social credit.

Following her essay about the Beijing metro system, Professor Lao entered the public spotlight again a year later when she circulated posts from the group chat of her residential community, speaking up against the property management company's decision to roll out facial recognition technology in the access control system for entrances into residential buildings. In discussions with the local community, Professor Lao invoked the Personal Information Security Standards. This act ultimately led the managers to provide residents the choice to opt into the facial recognition system. Her protest with the property managers was disseminated online through social media and even publicized in some popular media outlets.[36] (See Figure 3.)

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

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

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

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

Figure 3. Top responses on Weibo to news reports about Professor Lao Dongyan's protest against uses of facial recognition technology in her residential community.

Lao's standing as a professor of law at Tsinghua University—routinely ranked as China's best institution of higher education—provided her with a distinct platform to publish and circulate her dissatisfaction with facial recognition. Out of all the cases presented here, Professor Lao's is in some ways the most unusual, since she directly attacked the use of facial recognition by a municipal government. We understand her circumstance as unique, in that she is a powerful person at a prominent public institution of higher education who framed her critique of a local system as supporting the state by referring to the Constitution and existing law. At the same time, her critique on the metro system had no evident impact in terms of actual policy. This result further confirms both the extent to which the state remains firm on its own uses of facial recognition and the degree to which her essay was deemed unthreatening.

Although Professor Lao was ultimately unsuccessful in contesting the plan for the metro system undertaken by the state, she did manage to change her residential community's "private" use of the technology on a much smaller scale. For this success, a modest number of Weibo users celebrated her efforts.[37] But we must stress that the use of facial recognition in gated residential complexes is arguably one of the most widespread and broadly popular commercial uses of the technology in China today. In the end, the legitimacy of public uses was again affirmed, and the private uses were

not forbidden—only restricted so as to require a degree of buy-in and acceptance from individuals.

Case Study Four: A Televised Exposé

The “315 Evening Party” is a television event sponsored by China Central Television and the Chinese government that takes place annually on March 15, the date designated by the NGO Consumers International as World Consumer Rights Day. The “315” tradition was started in 1991 to draw attention to business practices that harm consumers’ interests. During the 2021 event, the leading issue was the nonconsensual collection of facial information by businesses at retail locations. More than twenty domestic and international brands operating in China, including Kohler, Max Mara, and a BMW-certified car dealership, were found to have surreptitiously installed facial recognition cameras and collected their customers’ data in retail stores across China. Kohler, the American plumbing products company, was the first to be named and shamed during the Evening Party. Anonymous reporters in China had learned from one of its sales directors that facial recognition cameras were used to help the company track individual customer’s visiting history at different retail stores.[38]

The CCTV exposé emphasized the restrictions laid out in the noncompulsory Personal Information Security Standards, categorizing facial data as “personal sensitive information,” collection of which requires the subject’s consent in advance.[39] As we have previously seen, many commercial enterprises in China currently employ facial recognition without acquiring such consent, in violation of the guidelines. The Evening Party thus served as an opportunity for the government to register popular dissatisfaction with the continued practice alongside support for the policy against it. The particular regulation cited had been updated in October of 2020, and the televised event publicized it as a leadup to the likely adoption of more specific and binding facial recognition laws in 2021. More broadly, the event may be understood as an official signal that private enterprises should be prepared to incorporate heightened data protection and user agreements into their use of facial recognition, as is already mandated or recommended by official state guidelines. (See Figure 4.)

Top responses on Weibo to news reports on the 315 exposés of businesses that collected customers' facial data illegally

1. This kind of technology, can't we use it on solving the trafficking of women and children? **Liked 19,512 times**

2. Being taken advantage of by big data is becoming a present reality. **Liked 7,082 times**

3. Don't forget your helmet if you go out! **Liked 5,326 times**

Figure 4. Top responses on Weibo to news reports about the 315 exposés of businesses that illegally collected customers' facial data.

Out of all the cases profiled in this study, this particular incident received the most online attention, with 19,512 "likes" for the top Weibo comment: "This kind of technology—can't we use it for solving the trafficking of women and children?" This comment is worth considering for a moment. It perfectly captures how public suspicion of the private, commercial applications of facial recognition technology coincides with and even seems to contribute to support for state "security" uses. As previously mentioned, the "315 Evening Party" is a state-sponsored televised event, and the public shaming of high-profile commercial enterprises drew a large and energetic audience. While a single comment cannot be taken as conclusive proof of broad trends, we might consider the possibility that the state plays a role in shaping the terms of debate through a carefully curated and sustained dialogue with popular opinion. The state appears to direct attention to private, commercial abuses of the technology while legitimatizing its own relatively unchecked use of it. This feedback loop ultimately works to support state action by aligning it with popular opinion against private bad actors who do not follow appropriate procedures.

That said, it is worth pointing out that Facebook, IBM, Google, Microsoft, Amazon, and FaceFirst have all been sued in US courts for their collection and analyses of facial data.[40] Many of these companies are actively fighting these lawsuits, and there is little evidence as of yet that the financial burden of this litigation has significantly changed their behavior, though it might in the future with additional regulation. It may well be that political motives galvanized the organizers of the "315 Evening Party" to call out a number of prominent foreign firms operating in the country. That does not mean the accusations against these companies were false; in all likelihood, they were accurate.

Suing IBM in the United States and running a television story on BMW in China may in fact have a similar function, namely, publicly shaming companies with the aim to draw a wider audience's attention to privacy issues and change corporate behavior.

Conclusions

It must be emphasized that these four cases do not represent a full view of the Chinese public's views of facial recognition technologies. Like the quantitative use of small-batch anonymous surveys, our qualitative approach merely seeks to provide a snapshot of a complex and ever-changing landscape. Methodological challenges remain, due especially to limitations in the public record. We have no indication of the particular experience of Uyghurs with facial recognition technology, for instance, and we have relied largely on internet users for a country where approximately three hundred million or more people still lack regular access — though that number is rapidly decreasing.[41] To be clear, even a post "liked" nearly forty thousand times represents a small drop in the bucket for a country of 1.4 billion citizens. Furthermore, the situation is constantly changing. Anecdotally, several colleagues working in Chinese academia and industry have suggested to us that public support for the use of facial recognition for a range of uses may have increased in the wake of the Covid-19 pandemic.

We must stress too that all four cases profiled above occurred in urban settings, and over 80 percent of the respondents to one of aforementioned surveys were college graduates. More research is needed into class divides. For instance, while facial recognition technologies have been deployed in Chinese factories to replace access cards and document work hours, there has been little discussion over how the rollout of facial recognition technologies in factories may infringe on workers' rights.[42] These four case studies should be understood as only an incomplete window into public perceptions, reactions, and debates concerning facial recognition technology in the country today.

Tentatively, we suggest that the central government may be monitoring the adoption of facial recognition technology in the commercial sector as a way to gauge the public's reception of these technologies wholesale. Even though the bounds of what exactly constitutes "public" space is debated and negotiated case-by-case, there is a clear regulatory difference in the country between security uses of facial recognition technology by the state—which are largely not debated in online forums—and commercial uses by enterprises such as Alibaba or housing complexes, which are. That said, this divide is sometimes hard to discern, as seen in the past year, when

government agencies outsourced the development of public service health code apps that involved facial data collection to the major technology firms Tencent and Alibaba.[43] There are further regulatory differences between large "private" enterprises that are required to forge close ties to the state apparatus and smaller private enterprises, like a wildlife park or a car dealership, which operate locally. And, in the spaces between, the relationship between some organizations, like a housing management company, and the local branches of state authority are not always entirely clear.

Without interrogating the actual divide between "private and party" in China, we simply contend that the public perception of a difference between the two is important for understanding the arena of play. While discussion of the state's use of facial recognition is both generally limited and broadly accepting, there is active debate regarding perceived private sector use of the technology, and it is in this direction that the state attempts to direct public concern and energy. As such, public dissatisfaction with a safari park's use of facial data may not translate over to a police bureau's use of similar data. Through the widespread adoption of facial recognition technologies in the commercial sector, the central government has likely learned much about what works and what doesn't in the eyes of the public. It may be that many people who embrace facial recognition technology in some contexts would prefer increased governmental oversight over its commercial uses, particularly when it occurs without individuals' knowledge or consent. It seems too that when citizens push back against a specific commercial enterprise's use of facial recognition, the enterprise is usually required to provide an opt-in or -out option in a user agreement. The state may indeed be preparing to make such agreements standard practice, a position promoted in the "315 Evening Party" and suggested by the statements in the 2021 draft Personal Information Protection Law. How practical or meaningful those user consent agreements will be in practice is another question.

It is striking to note—even in our narrow subset of cases—the role of the legal community, and particularly professors of law, in voicing concerns over facial recognition technologies. Professors Guo Bing and Lao Dongyan have been some of the more prominent figures in voicing concerns over facial data collection, protection, and storage in China over the past three years. Yet their concerns have been targeted toward very specific applications of the technology, rather than the general use of the technology itself. Such tactics may reflect the politics of the possible in China today. University legal academics naturally possess more knowledge of the country's laws and legal system than the average citizen, and thus are able to protest certain

deployments of the technology through citing relevant laws, framing themselves as on the side of the state and providing them with a degree of political cover. But with increased oversight of university academics during Xi Jinping's tenure, scholars of law may have to be more careful than ever not to overstep discursive boundaries acceptable to the party.

Indeed, the central government under Xi's direction has not shied away from measures that highlight the legal system and continue a long trend toward the routinization of legal proceedings, and it seems likely that facial recognition technology will soon be taken more formally into account.[44] Law maintains a high level of sociopolitical prestige in China, and it is not quite accurate to say that the law simply exists as a top-down tool of control—though it is used in that way as well. It is remarkable that most of the opponents of specific applications of facial recognition technologies mentioned here invoked existing national laws or regulatory standards to make their points. But given the decades-long history of the development of facial recognition technologies in China, the relative lack of firm and clear regulations governing private applications of the technology through 2020 is striking. This lacuna is likely intentional. Facial recognition represents a rapidly shifting landscape—both technologically and in the court of public opinion—and the state is shaping new laws as it learns more.

In some ways, the situation in China is not dissimilar to those in Europe and North America. Comprehensive legal regulations for the acquisition and use of facial data remain very much a work in progress across these regions. The unannounced collection of facial data by researchers has occurred in both China and the West, and private companies have been named and shamed for their uses of the technology in violation of personal privacy across the board. The fact that proposed and enacted laws in China and elsewhere are now seeking to ensure that consent is obtained before mining facial data is further indication that in China, Europe, and the United States, collection without consent is likely already taking place. While the scope of debate may differ among the countries, the overarching regulatory problems these countries are facing are similar in part because they are all responding to the same rapidly evolving situation on the ground.

The invocation of law by both the Chinese state and popular commentators is important for another reason. While we often conceive of the law as a tool to codify existing ethical norms, law can also be employed to box out uneasy ethical questions from the scope of discussion. The successful cases presented against facial recognition technology presented here generally did not appeal to the morality or immorality of

the technology, but rather to precise claims rooted in the Chinese state's own codes and regulations. That said, among the general public, some online comments did touch on broader ethical dimensions, such as human rights, and it remains to be seen whether the state's "strategy" in selectively allowing limited debate could backfire or ignite a stronger demand for civil liberties over time.[45]

We conclude with two broad takeaways. On the one hand, we should not see the Chinese state's uses of facial recognition technologies in public security and the private uses of these technologies in the commercial realm as in ideological conflict or even practical contradiction: by allowing limited debate on private abuses, the Chinese state in fact solidifies its own position as a guarantor of law while claiming to further the safety and convenience of the public. On the other hand, because the state presents itself as the consummate ethical actor to the domestic public, the primary space open for discussion lies in fields and applications that have yet to be firmly regulated by it. This dynamic poses an intriguing question: as the state assumes more explicit control over the private companies involved in the collection and preservation of biometric data, where will public concerns be directed if and when future problems arise?

Discussion Questions

- How might different governments shape public debate about the ethical implications of emerging technologies? What political incentives are at play in China and elsewhere?
- Are there foundational ethical principles in using facial recognition technology that hold constant across different regime types?
- Who should be the social actors and political authorities to make the distinction between beneficial and harmful uses of facial recognition technology?
- If you were to design new applications of facial recognition technologies, how might you take into account both legal regulations and ethical considerations? How do you think those considerations are in tension in both the United States and China?
- How can social media be used in research on the public reception of technology? What would Twitter, TikTok, or Facebook posts tell us about the American public's concerns about technology? How might they also lead us astray?
- Under any circumstances, could you accept cameras in a classroom? What would they be? Could you accept facial recognition on a university campus if it was offered to increase your security?

- If you knew your university campus employed facial recognition, would that influence your decision to join a protest on campus against the university administration?
- Which companies today own your facial data? Can you even answer that question? If you do know, could you ask for it back? How would you go about doing that?
- What groups of people in American society have been at the forefront of identifying risks of facial recognition technology? Are they employed in government? Do they work for technology companies? Do they write for media outlets? Prior to taking this class, did you hear of such risks?

Acknowledgements

This case study originated through an MIT 2020–2021 Undergraduate Research Opportunities Project (UROP) examining litigation in the PRC through the online database, "China Judgements Online." We would like to thank David Kaiser, Emma Teng, David Goldston, David Clark, Yasheng Huang, Jeremy Daum, Nathan Hill, Zeyi Yang, Yuan Yang, Wenfei Zhou, Neal Xu, Henry Xu, and Tianyu Fang for their generous feedback on this case study. All errors are our own.

Bibliography

Allen, Kerry. "China Facial Recognition: Law Professor Sues Wildlife Park." *BBC News*, November 8, 2019.

Anonymous. "China Using Facial Recognition to ID Scalpers at Hospitals." *Associated Press*, February 24, 2019.

Anonymous. "Shuju anquanfa, geren xinxi baohufa wei 2021 nian quanguo renda shenyi zhongdian" □□□□□□□□□□□□□□2021□□□□□□□□□. *Renmin youdian bao* □□□□□, January 1, 2021.

Anonymous. "'Renlian shibie diyi an' zhongshen panjue: Shanchu mianbu tezheng xinxi wai zengpan dongwuyuan shenchu zhiwen shibie xinxi" "□□□□□□□"□□□□□□□□□□□□□□□□□□□□□□□□□□□□. *Yangguang wang* □□□, April 10, 2021.

Anonymous. "Tengxun qiantou qicao shouge 'fangyi chuxing ma' tuanti biaozhun, wei yiqing fangkong he fugong fuchan zhuli" □□□□□□□□"□□□□□"□□□□□□□□□□□□□□□□□□. *Xinhua News*, March 6, 2020.

Borak, Masha. "Chinese People Are Concerned about Use of Facial Recognition, Survey Shows." *South China Morning Post*, January 26, 2021.

Chan, Tara Francis. “China is Monitoring Employees’ Brain Waves and Emotions.” *Insider*, April 30, 2018.

Chen, Shu-ching Jean. “SenseTime: The Faces Behind China's Artificial Intelligence Unicorn.” *Forbes*, March 13, 2018.

George, Damian, Kento Reutimann, and Aurelia Tamò-Larrieux. “GDPR Bypass by Design? Transient Processing of Data under the GDPR.” *International Data Privacy Law* 9 (2019): 285–298.

Georgetown Journal of International Affairs (Editorial Staff). “Dr. James Millward on the Uyghur Crisis in Xinjiang.” *Georgetown Journal of International Affairs*, September 19, 2019.

Global Times (Editorial Staff). “China and US Should Lift Mutual Travel Restrictions in August or September: Chief Epidemiologist.” *Global Times*, March 2, 2021.

Guojia shichang jiandu guanli zongju □□□□□□□□□□ and Guojia biaozhunhua guanli weiyuanhui □□□□□□□□□□. *Xinxi anquan jishu geren xinxi anquan guifan* □□□□□□ □□□□□□□□ □, October 1, 2020.

Hangzhoushi Fuyang renmin fayuan □□□□□□□□□. “Guo Bing yu Hangzhou yesheng dongwu shijie youxian gongsi fuwu hetong jiufen yishen minshi panjueshu” □□□□□□□□□□ □□□□□□□□□□□□□□□□□□□. *China Judgments Online* (*Zhongguo caipan wenshu wang*) □□□□□ □□, 2019.

Hu Jing □□. “Du ni qianbian reng bu yanjuan -- Ji Su Guangda jiaoshou de renlian shibie yanjiu shiye” □□□□□□□□--□□□□□□□□□□□□□□□□. *Kexue Zhongguoren* □□□□□, 16 (2011): 72–73.

Huang, Yasheng. “China’s Use of Big Data Might Actually Make It Less Big Brother-ish.” *MIT Technology Review*, August 22, 2018.

Knight, Will. “MIT Cuts Ties with a Chinese AI Firm Amid Human Rights Concerns.” *Wired*, April 21, 2020.

Kobie, Nicole. “The Complicated Truth about China’s Social Credit System.” *Wired*, July 6, 2018.

Lao Dongyan □□□. “Ditie shiyong renlian shibie de falü yinyou” □□□□□□□□□□□□□. *Caixin* □ □, October 31, 2019.

Li, Xin. “Chinese Hospital Introduces Facial Recognition for Bill Pay.” *Xinhua News*, September 21, 2018.

Liao Jin □□. “Jiaoyubu kejisi: Xiaoyuan tuiguang renlian shibie jishu ying jinshen, jiang xianzhi he guanli” □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□. *Pengpai* □□, September 5, 2019.

Lin, Xifen, and Wei Shen. “Reforms to China's Pretrial Detention System: The Role of The Procuratorate.” *International Journal of Law, Crime and Justice* 44 (2016): 183–211.

Lippert, Katherine. “Amid Coronavirus, USC is Requiring Facial Recognition Scans of Students Living on Campus, but the Technology Sparks Controversy.” *USC Annenberg Media*, May 15, 2020.

Liu, Caiyu, and Yeping Yin. “Honest Passengers First! Beijing Subway Trial of Credit-Based Fast Entry System.” *Global Times*, March 10, 2021.

Liu Yuxiu □□□. “Faxue jiaoshou de yici weiquan: Renlian shibie de fengxian chaochu ni suo xiang” □□□□□□□□□□□□□□□□□□□□□□□□□□. *Pengpai* □□, October 21, 2020.

Lu, Chaochao, and Tang, Xiao’ou. “Surpassing Human-Level Face Verification Performance on LFW with GaussianFace.” *Proceedings of the 29th AAAI Conference on Artificial Intelligence (AAAI-15)*, December 20, 2014.

Lu, Shen. “China Could Soon Have Stronger Privacy Laws Than the U.S.” *Protocol*, May 8, 2021.

Marr, Bernard. “Meet the World's Most Valuable AI Startup: China’s SenseTime.” *Forbes*, June 17, 2019.

McBride, Sarah. “Chinese AI Project Is Under Review at MIT after U.S. Blacklists Company.” *Bloomberg News*, October 8, 2019.

Rauenzahn, Brianna, Jamison Chung, and Aaron Kaufman. “Facing Bias in Facial Recognition Technology.” *Regulatory Review*, March 20, 2021.

Perkowitz, Sidney. “The Bias in the Machine: Facial Recognition Technology and Racial Disparities.” *MIT Case Studies in Social and Ethical Responsibilities of Computing*, February 5, 2021.

Sandler, Rachel. “Students Accuse the University of Miami of Using Facial Recognition to Identify Student Protestors. The University Denies It.” *Forbes*, October 15, 2020.

Taigman, Yaniv, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf. "DeepFace: Closing the Gap to Human-Level Performance in Face Verification." *Conference on Computer Vision and Pattern Recognition (CVPR)*, June 24, 2014.

Van Noorden, Richard. "The Ethical Questions that Haunt Facial-Recognition Research." *Nature* (News Feature), November 19, 2020.

Wang Chunrui □□□. "Chao bacheng shoufangzhe fandui gonggong xiaofei changsuo shiyong renlian shibie" □□□□□□□□□□□□□□□□□□□□. *Xinjingbao* □□□, January 26, 2021.

Yang, Yuan, and Nian Liu. "China Survey Shows High Concern over Facial Recognition Abuse." *Financial Times*. December 5, 2019.

Yang, Zeyi. "China Sours on Facial Recognition Tech." *Protocol*, March 18, 2021.

Zhang Sheng □□. "AI jin xiaoyuan, bianjie zai nali?" AI□□□□□□□□□? *Pengpai* □□, October 24, 2019.

Zhang, Taisu, and Tom Ginsberg. "China's Turn Toward Law." *Virginia Journal of International Law* 59 (2019): 306–389.

Zhang, Zhouxiang. "Who Has the Power to Collect My Face Information?" *China Daily*, November 5, 2019.

Zhongguo hulian wangluo xinxi zhongixn □□□□□□□□□□. "Di 47 ci 'Zhongguo hulian wangluo fazhan zhuangkuang tongji baogao'" □47□□□□□□□□□□□□□□□□□, February 3, 2021.

Footnotes

1. For the Chinese article on the subject, see Wang Chunrui, "Chao bacheng shoufangzhe fandui gonggong xiaofei changsuo shiyong renlian shibie" □□□□□□□□□□□□ □□□□□□□□, *Xinjingbao* □□□ (January 26, 2021). For an English-language article, see Masha Borak, "Chinese People Are Concerned about Use of Facial Recognition, Survey Shows," *South China Morning Post* (January 26, 2021). ↩
2. Yuan Yang and Nian Liu, "China Survey Shows High Concern over Facial Recognition Abuse," *Financial Times* (December 5, 2019). ↩
3. Anon., "China Using Facial Recognition to ID Scalpers at Hospitals," *Associated Press* (February 24, 2019); Xin Li, "Chinese Hospital Introduces Facial Recognition for Bill Pay," *Xinhua News* (September 21, 2018). ↩

4. Shen Lu, "China Could Soon Have Stronger Privacy Laws Than the U.S.," *Protocol* (May 8, 2021). ↩
5. Xifen Lin and Wei Shen, "Reforms to China's Pretrial Detention System: The Role of The Procuratorate," *International Journal of Law, Crime and Justice* 44 (2016): 183–211. ↩
6. *Global Times* (Editorial Staff), "China and US Should Lift Mutual Travel Restrictions in August or September: Chief Epidemiologist," *Global Times* (March 2, 2021). ↩
7. Shu-ching Jean Chen, "SenseTime: The Faces Behind China's Artificial Intelligence Unicorn," *Forbes* (March 13, 2018). ↩
8. Hu Jing □□, "Du ni qianbian reng bu yanjuan -- Ji Su Guangda jiaoshou de renlian shibie yanjiu shiye" □□□□□□□□--□□□□□□□□□□□□□□□, *Kexue Zhongguoren* □□□□□, 16 (2011): 72–73. ↩
9. Facial recognition is an umbrella term to refer to several categories of technology. Face verification validates that two facial images show the same person. Face identification ascribes an identity from a stored registry to a facial image. Face clustering analyzes a batch of facial images and breaks them into discrete categories. See Yaniv Taigman *et al.*, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," *Conference on Computer Vision and Pattern Recognition (CVPR)*, June 24, 2014. ↩
10. Chaochao Lu and Tang, Xiao'ou, "Surpassing Human-Level Face Verification Performance on LFW with GaussianFace," *Proceedings of the 29th AAAI Conference on Artificial Intelligence (AAAI-15)*, December 20, 2014. ↩
11. Bernard Marr, "Meet the World's Most Valuable AI Startup: China's SenseTime," *Forbes* (June 17, 2019). ↩
12. *Georgetown Journal of International Affairs* (Editorial Staff), "Dr. James Millward on the Uyghur Crisis in Xinjiang," *Georgetown Journal of International Affairs* (September 19, 2019). ↩
13. Anon., "Shuju anquanfa, geren xinxi baohufa wei 2021 nian quanguo renda shenyi zhongdian" □□□□□□□□□□□□□□2021□□□□□□□□□. *Renmin youdian bao* □□□□□ (January 1, 2021); Zeyi Yang, "China Sours on Facial Recognition Tech," *Protocol* (March 18, 2021). ↩

14. Quoted from Yang, "China Sours on Facial Recognition Tech." ↩
15. Quoted from Lu, "China Could Soon Have Stronger Privacy Laws Than the U.S." ↩
16. The first draft of the PIPL was published in October 2020 and the second draft was released at the end of April 2021. The second release adds three articles and revises the language of several provisions for clarity. One important difference is that the second draft specifies the oversight procedures for biometric data-storage and processing by large technology companies. The second release also specified the Cyberspace Administration's responsibilities in formulating laws for personal information protection in light of emerging technologies such as facial recognition. ↩
17. Richard Van Noorden, "The Ethical Questions that Haunt Facial-Recognition Research," *Nature* (News Feature, November 19, 2020). ↩
18. Sarah McBride, "Chinese AI Project Is Under Review at MIT after U.S. Blacklists Company," *Bloomberg News* (October 8, 2019); Will Knight, "MIT Cuts Ties with a Chinese AI Firm Amid Human Rights Concerns," *Wired* (April 21, 2020). ↩
19. Damian George *et al.*, "GDPR Bypass by Design? Transient Processing of Data under the GDPR," *International Data Privacy Law* 9 (2019): 285–298; Van Noorden, "The Ethical Questions that Haunt Facial-Recognition Research." ↩
20. Brianna Rauenzahn *et al.*, "Facing Bias in Facial Recognition Technology," *Regulatory Review* (March 20, 2021); see also Sidney Perkowitz, "The Bias in the Machine: Facial Recognition Technology and Racial Disparities," *MIT Case Studies in Social and Ethical Responsibilities of Computing* (February 5, 2021). ↩
21. Kerry Allen, "China Facial Recognition: Law Professor Sues Wildlife Park," *BBC News* (November 8, 2019). ↩
22. Anon., "'Renlian shibie diyi an' zhongshen panjue: Shanchu mianbu tezheng xinxi wai zengpan dongwuyuan shenchu zhiwen shibie xinxi" "□□□□□□□"□□□□□□□□□□□□□□□□□□□□□□□□□□□□. *Yangguang wang* □□□ (April 10, 2021). ↩
23. Zhouxiang Zhang, "Who Has the Power to Collect My Face Information?" *China Daily* (November 5, 2019). ↩
24. Hangzhoushi Fuyang renmin fayuan □□□□□□□□□. "Guo Bing yu Hangzhou yesheng dongwu shijie youxian gongsi fuwu hetong jiufen yishen minshi panjueshu" □

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□. *China Judgments Online* (*Zhongguo caipan wenshu wang*) □□□□□□□, 2019. ↩

25. Eighty-five percent of the respondents responded that they hope to see proper contracts before facial recognition technology is used. See Wang, "Chao bacheng shoufangzhe fandui gonggong xiaofei changsuo shiyong renlian shibie." ↩

26. For the original post in Chinese, see: http://weibo.com/1642088277/JuNiVl4LQ ↩

27. See for instance the following sentence: "The school stated: the school has previously consulted with the public security department and the legal affairs department. Since the classroom is a public place, there is no 'invasion of privacy'" □□□ '□□□□' □□□. Quoted from Zhang Sheng □□, "AI jin xiaoyuan, bianjie zai nali?" AI□□□□□□□□□? *Pengpai* □□ (October 24, 2019). ↩

28. Liao Jin □□. "Jiaoyubu kejisi: Xiaoyuan tuiguang renlian shibie jishu ying jinshen, jiang xianzhi he guanli" □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□. *Pengpai* □□ (September 5, 2019). ↩

29. For the original post in Chinese, see: https://m.weibo.cn/detail/4412128381237844. ↩

30. Van Noorden, "The Ethical Questions that Haunt Facial-Recognition Research." ↩

31. Rachel Sandler, "Students Accuse the University of Miami of Using Facial Recognition to Identify Student Protestors. The University Denies It," *Forbes* (October 15, 2020). ↩

32. Katherine Lippert, "Amid Coronavirus, USC is Requiring Facial Recognition Scans of Students Living on Campus, but the Technology Sparks Controversy," *USC Annenberg Media* (May 15, 2020). ↩

33. Quoted from Lao Dongyan □□□, "Ditie shiyong renlian shibie de falü yinyou" □□□□□□□□□□□□□. *Caixin* □□ (October 31, 2019). ↩

34. Caiyu Liu and Yeping Yin, "Honest Passengers First! Beijing Subway Trial of Credit-Based Fast Entry System," *Global Times* (March 10, 2021). ↩

35. Nicole Kobie, "The Complicated Truth about China's Social Credit System," *Wired* (July 6, 2018). ↩

36. Liu Yuxiu □□□, "Faxue jiaoshou de yici weiquan: Renlian shibie de fengxian chaochu ni suo xiang" □□□□□□□□□□□□□□□□□□□□□□□□. *Pengpai* □□ (October 21, 2020). ↩

37. For the original post in Chinese, see: https://m.weibo.cn/status/4607699805538650. ↩

38. For the original post in Chinese, see: http://weibo.com/2258727970/K6l450C0g. ↩

39. Guojia shichang jiandu guanli zongju □□□□□□□□□□ and Guojia biaozhunhua guanli weiyuanhui □□□□□□□□□□. *Xinxi anquan jishu geren xinxi anquan guifan* □□□□□□ □□□□□□ □□ (October 1, 2020). ↩

40. Van Noorden, "The Ethical Questions that Haunt Facial-Recognition Research." ↩

41. Zhongguo hulian wangluo xinxi zhongixn □□□□□□□□□□. "Di 47 ci 'Zhongguo hulian wangluo fazhan zhuangkuang tongji baogao'" □47□□□□□□□□□□□□□□□□□□ (February 3, 2021). ↩

42. Tara Francis Chan, "China is Monitoring Employees' Brain Waves and Emotions," *Insider* (April 30, 2018). ↩

43. In March 2021, Tencent collaborated with Shenzhen's municipal government to develop guidelines for private technology companies issuing health codes. See Anon., "Tengxun qiantou qicao shouge 'fangyi chuxing ma' tuanti biaozhun, wei yiqing fangkong he fugong fuchan zhuli" □□□□□□□□"□□□□□"□□□□□□□□□□□□□□□□□□. *Xinhua News* (March 6, 2020). ↩

44. Taisu Zhang and Tom Ginsberg, "China's Turn Toward Law," *Virginia Journal of International Law* 59 (2019): 306–389, on 307. ↩

45. Yasheng Huang, "China's Use of Big Data Might Actually Make It Less Big Brother-ish," *MIT Technology Review* (August 22, 2018). ↩