

Facial recognition law in China

Zhaohui Su,¹ Ali Cheshmehzangi,^{2,3} Dean McDonnell,⁴ Barry L Bentley,⁵
Claudimar Pereira da Veiga,⁶ Yu-Tao Xiang^{7,8,9}

¹School of Public Health, Southeast University, Nanjing, China. ²Department of Architecture and Built Environment, University of Nottingham - Ningbo China, Zhejiang, China. ³Network for Education and Research on Peace and Sustainability, Hiroshima University, Hiroshima, Japan. ⁴Department of Humanities, Institute of Technology Carlow, Carlow, Ireland. ⁵Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, UK. ⁶School of Management—PPGOLD, UFPR, Curitiba, PR, Brazil. ⁷Department of Public Health and Medicinal Administration, University of Macau, Taipa, China. ⁸Institute of Translational Medicine, University of Macau, China. ⁹Centre for Cognitive and Brain Sciences, University of Macau, China

Abstract

Although the prevalence of facial recognition-based COVID-19 surveillance tools and techniques, China does not have a facial recognition law to protect its residents' facial data. Oftentimes, neither the public nor the government knows where people's facial images are stored, how they have been used, who might use or misuse them, and to what extent. This reality is alarming, particularly factoring in the wide range of unintended consequences already caused by good-intentioned measures and mandates amid the pandemic. Biometric data are matters of personal rights and national security. In light of worrisome technologies such as deep-fake pornography, the protection of biometric data is also central to the protection of the dignity of the citizens and the government, if not the industry as well. This paper discusses the urgent need for the Chinese government to establish rigorous and timely facial recognition laws to protect the public's privacy, security, and dignity amid COVID-19 and beyond.

Brief report

Amid the pandemic, ranging from thermal facial recognition to masked face recognition, the utilisation of facial recognition technologies has been prevalent across societies.¹ In scale, scope and speed, China has been a global leader in the adoption and application of facial recognition, along with other artificial intelligence (AI) technologies, for COVID-19 control and prevention.² In Chinese cities big and small, it is even common for small businesses like local restaurants

to install facial recognition-based cameras to administer COVID-19 surveillance tasks such as temperature checks. However, while it is applaudable for individuals and organisations to stay vigilant about pandemic safety measures with the aid of advanced technologies, it is equally, if not more, important to understand how personal data,³ especially those biometric in nature, are being processed and protected. At the moment, little is known about how facial images of residents in China are stored and used, who might use or misuse them, and to what extent.⁴

It is possible that China is not only a global leader in the use of AI technologies, it might also be ahead of the curve in the misuse of face recognition tools and the abuse of people's biometric data. At the moment, China has yet to have a facial recognition law. Though the Data Security Law, Personal Information Protection Law and other existing legal apparatus are promising signs of better data protection,⁵ most of these legal frameworks are either too vague or too broad. Take the Personal Information Protection Law for instance. Though the law underscores the importance of protecting personal data,⁶ it offers no concrete guidance on data protection practices, such as how and where to store sensitive facial data, whether and which encryption should be used, and who should be the data-auditors, rule-makers or law-enforcers. In other words, neither the government, the public, nor perhaps even the restaurant owners, might know who has access to the customers' data, even though facial images have been collected at the local restaurant level since the onset of the pandemic. Also factor in the prevalence of facial recognition technologies installed in China,⁷ possibly in the name of COVID-19 prevention and under the pretence of government permission, it is clear that timely rules, regulations and laws that could guide responsible and accountable use and application of facial recognition technologies are urgently needed.

Considering the toll the pandemic has already exerted on society, especially the unintended consequences caused by good-intended measures or mandates,⁸ the Chinese government should ensure that measures that aim to help, such as thermal facial recognition technologies for detecting potential COVID-19 infections, do not

result in additional unintended consequences. Biometric data are matters of personal rights and national security.⁹ Furthermore, in light of the surge of worrisome AI applications such as deepfake pornography (map the faces of celebrities and private citizens, including teenagers and children, on to explicit sexual material to create hyper-realistic pornographic videos without these individuals' consent),¹⁰ the protection of biometric data is also integral to the dignity of the citizens and the government, if not the industry as well.

It is also pivotal that the government establish a rigorous system of facial recognition rules, regulations and laws that could eliminate potential bad actors within. There is a vast number of public service officials who work across levels of the government, with varying access clearance, weak points and ulterior motives and that might compromise⁹ the government's own ability to protect its residents and itself from high-stake data breach or compromise. Essentially, without the presence of rigorous systematic intervention and supervision, it might be a matter of when, rather than if, crises originated in the lack of biometric data protection occur. As the world is still fighting COVID-19 and its resultant crises, it is of utmost urgency that the Chinese government establish facial recognition laws to protect its residents, as well as the healthy development of the industry. When it comes to advanced technologies, great power truly comes great responsibility—China should not only be the world's forerunner in AI, but also lead the global accountability, responsibility and solidarity in the protection of the privacy, safety and dignity of the public in the context of facial recognition technologies and beyond.

References

1. Biometric Technology Today. New biometric products flood out to tackle Covid-19. *Biometric Technology Today* 2020;2020(5):1–2.
2. Jiang Y. To halt COVID-19, Chinese border City turns to facial recognition, 2021. Sixth tone. Available: <https://www.sixthtone.com/news/1007957/to-halt-covid-19%2C-chinese-border-city-turns-to-facial-recognition> [Accessed 05 Dec 2021].
3. Bengio Y, Janda R, Yu YW, et al. The need for privacy with public digital contact tracing during the COVID-19 pandemic. *Lancet Digit Health* 2020;2(7):e342–4.
4. Roberts H, Cowls J, Morley J, et al. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI Soc* 2021;36(1):59–77.
5. Aho B, Duffield R. Beyond surveillance capitalism: privacy, regulation and big data in Europe and China. *Econ Soc* 2020;49(2):187–212.
6. DigiChina. Knowledge base: personal information protection law, 2021. Stanford University. Available: <https://www.wired.com/story/china-personal-data-law-pipl/> [Accessed 05 Dec 2021].
7. Zhang P. Privacy in China: the growth of facial recognition technology in the private sector raises concerns about security and identity, 2021. SCMP. Available: <https://www.scmp.com/lifestyle/article/3111428/privacy-china-growth-facial-recognition-technology-private-sector-raises> [Accessed 05 Dec 2021].
8. Su Z, McDonnell D, Roth S, et al. Mental health solutions for domestic violence victims amid COVID-19: a review of the literature. *Global Health* 2021;17(1):67.
9. Su Z, McDonnell D, Bentley BL, et al. Addressing Biodisaster X threats with artificial intelligence and 6G technologies: literature review and critical insights. *J Med Internet Res* 2021;23(5):e26109.
10. Mika W. The emergence of deepfake technology: a review. *Technology Innovation Management Review* 2019;9(11) <https://timreview.ca/article/1282>

Acknowledgements

The authors wish to express their gratitude the editors and reviewers for their constructive input and insightful feedback.

Contributors

ZS conceived the work, reviewed the literature, drafted, and edited the manuscript. AC, DMD, BLB, CPdV, and YTX reviewed the literature and edited the manuscript. All authors approved the manuscript for submission.

Funding

The authors have not declared a specific grant for this research from any funding agency in the public, commercial or not-for-profit sectors.

Competing interests

None declared.

Patient consent for publication

Not applicable.

Provenance and peer review

Not commissioned; externally peer reviewed.

ORCID iDs

Zhaohui Su <http://orcid.org/0000-0003-2005-9504>

Barry L Bentley <http://orcid.org/0000-0002-4360-5902>