WIN-WIN OR WIN LOSE? AN EXAMINATION OF CHINA'S SUPPLY OF MASS SURVEILLANCE TECHNOLOGIES IN EXCHANGE FOR AFRICAN'S FACIAL IDS

https://doi.org/10.29053/pslr.v16i1.4506

*by Sumaya Nur Hussein**

Abstract

The use of Facial Recognition Technologies (FRT) has become increasingly prevalent. While these technologies have been applauded for their many benefits, their use have been criticised for problems relating to accuracy. More particularly, FRT technologies have demonstrated low accuracy when identifying people of colour. This has led to the call for diversification of data, which has been intensified by major corporations and nations competing to lead in Artificial Intelligence development (the AI race). In an attempt to diversify its data sets, China, as a significant player in the AI race, has entered into an agreement with Zimbabwe. The agreement is meant to benefit both parties mutually as a 'win-win' agreement, which entails the collection of African facial IDs in exchange for high-end mass surveillance technologies. This article questions whether this agreement can genuinely be a win-win. To demonstrate this, the article will discuss and analyse China's viewpoint on this 'win-win' in light of the AI race and take a closer look at how this agreement places China one step ahead of others in the race to lead facial recognition technologies. As such, the article examines that which is hidden in China's win-win perspective by delving deeper into the biometric data and the underlying principles of its Regulation to determine whether the collection of Facial IDs is in line with these principles. Finally, I attempt to redefine the meaning of what is truly a 'win-win' in this context.

*LLB, Strathmore University. ORCID iD: 0000-0003-4509-0989.

1 Introduction

Facial recognition technology (FRT) has quickly entered the public domain. With various advantages over previous biometric surveillance techniques, such as the ability to survey at a distance, FRT has entered the worldwide market as the purported be-all and end-all of twenty-first-century surveillance technology.[1] Its success has been fuelled by advances in machine learning, dramatic declines in hardware and processing prices, and an ever-increasing desire for surveillance and security in both the public and private sectors. Facial recognition is unquestionably the most commonly used artificial intelligence ('AI') technology in China, used in a wide range of sectors for several purposes, ranging from identification to boosting efficiency.[2] Recognising the efficiency gains that facial recognition may generate in the public and private sectors, the Chinese government has prioritised the study, development, implementation, and commercialisation of this technology.[3] As a result, facial recognition affects practically every area of a person's life in China — for example, facial recognition was widely employed in suppressing the COVID-19 outbreak by validating identity without person-to-person interaction.[4]

China is presently the world's second-biggest economy,[5] with forecasts to overtake the United States as the world's largest economy by 2030. China unveiled its 'One Road and Belt Initiative' (BRI) in 2013, consisting of a land and a sea route connecting China to the rest of the world.[6] This project has piqued the interest of many experts, who regard it as a new geopolitical strategy for China to expand not just its economic cooperation but also its influence

1 S Curtis 'Inflection points: Facial recognition technology in the United States and China' (2020) 1 *The Asia Society Northern California Team* at 1.

2 L Dudley 'China's ubiquitous facial recognition tech sparks privacy backlash' *The Diplomat* 7 March 2020 https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/#:~:text=One%20of%20the%20most%20public,facial%20recognition%20scan%20for%20admission (accessed 27 March 2020). According to World Economic Forum 'A framework for responsible limits on facial recognition use case: Flow management' 2020 at 4, 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.'

3 Y Luo & R Guo 'Facial recognition in China: Current status, comparative approach and the road ahead' (2021) 25(2) *University of Pennsylvania Journal of Law and Social Change* at 155.

4 Luo & Guo (n 3) 155.

5 J Woetzel et al 'China and the world: Inside the dynamics of a changing relationship' 2019 at 1.

6 Ž Koboević et al 'The maritime silk road and China's belt and road initiative' (2018) 65(2) *Naše More* at 113-114.

throughout the world.[7] China's BRI is majorly motivated by the concept of 'win-win,' which is based on traditional Chinese cultural ideals of 'peace and collaboration' and adheres to the concepts of peaceful coexistence and mutual gain.[8] It's also strongly tied to and promotes the notion of peaceful development, with cooperation and mutual gain as the foundations of win-win solutions.[9]

As China gains power in global markets as a significant contributor to the FRT industry, there are rising concerns about the extensive use of this technology.[10] According to numerous media reports, FRT, as employed in the commercial sector, is prone to problems such as a lack of transparency and cybersecurity risks such as data leaking.[11] Concerns have also been raised from a legislative perspective; a report from a multi-agency task force recently published an article exposing significant privacy vulnerabilities identified in a review of mobile applications that use face recognition in China. Forcing users to disclose facial information, a lack of clear guidelines for information collection, and the difficulty for data subjects to withdraw consent to the collection and use of facial information have all been noted as issues.[12] Civil-society advocates have questioned the fundamental reasons advanced by the companies and governments that develop and promote these technologies, noting the actual harms caused by their use. Increasingly, research shows that these systems perform poorly when employed in real-world contexts, even when the system fulfils the industry's restricted assessment standards that are used to back up promises of accuracy. Even systems with great accuracy rates have unevenly spread errors. They perform worse in certain categories, with exceptionally high failure rates for Black women, gender minorities, young and old individuals, disabled people, and manual labourers. This is mainly because the data sets used to train these kinds of technology are mostly Caucasians.[13] Research has shown that FRTs trained in China

7 Associated Press 'Belt and road's real aims? Expanding China's global influence and military presence, US study says' *South China Morning Post* 18 April 2018 https://www.scmp.com/news/china/diplomacy-defence/article/2142266/belt-and-roads-aim-promote-chinese-interests-and (accessed 29 March 2022).

8 C Xulong 'Win-win cooperation: Formation, development and characteristics' China Institute of International Studies 17 November 2017 https://www.ciis.org.cn/english/ESEARCHPROJECTS/Articles/202007/t20200715_3604.html (accessed 29 March 2022).

9 As above.

10 Luo & Guo (n 3) 155; China Youth Daily, '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* 7 January 2020 http://www.xinhuanet.com/2020-01/07/c_1125428533.htm and https://perma.cc/T63F-BEQA (accessed 29 March 2022).

11 Luo & Guo (n 3) 162.

12 As above.

13 A Donkor 'The race to build facial recognition tech for Africa is being led by this award-winning engineer' *Quartz Africa* 17 September 2020 https://qz.com/africa/1905079/facial-recognition-tech-in-africa-boosted-by-ghana-ai-startup/ (accessed 25 July 2021).

have more accurately identified Asian faces than those developed in the West.[14] This is attributed to the fact that the data sets — in this case, photos of Asian faces — have been available to China, which was subsequently used to train its FRT AI.[15] This means that for China to improve the accuracy of their FRT AI's in recognising people of colour, they need to diversify the data sets that they use to train them.

In 2018, CloudWalk, a Chinese start-up through BRI, signed a strategic partnership deal with the Zimbabwean government. China has described this agreement as a win-win as both parties will benefit mutually. The agreement is that Cloudwalk will give high-end mass surveillance technologies in exchange for the Facial IDs[16] of Zimbabweans, which will be crucial in training these technologies' algorithms to further improve their accuracy. Even though this arrangement has raised concerns in the media for being a form of digital colonialism and risking the privacy rights of Zimbabweans, there has yet to be any academic analysis.

This article will examine whether the collection of facial IDs of Africans in exchange for high-end mass surveillance technologies can genuinely be considered a 'win-win'. To demonstrate this, the second part of the article will discuss and analyse China's viewpoint on this 'win-win'. In this part, the AI race, which is crucial in this context, is explained to demonstrate how major corporations and states are in a race to lead AI developments, and closer attention is given to how this agreement places China one step ahead of others in the race to lead facial recognition technologies. The third part looks at the other side of the coin, which is what China's win-win viewpoint leaves out. Here, the article delves deeper into the biometric data and the underlying principles of its Regulation. The facial IDs of Africans are the commodity of exchange in this agreement, which means that to ensure that it is a gain for Africans (Zimbabweans), it is then crucial to determine whether principles of biometric data regulation, especially with regards to consent, have been observed. This research looks at Zimbabwe as a case study. The fourth section looks at the way forward by redefining what a genuine win-win is, and the final part concludes the article.

14 R Noorden 'The ethical questions that haunt facial recognition research' *Nature* 18 November 2020 https://www.nature.com/articles/d41586-020-03187-3 (accessed 1 August 2021).

15 As above.

16 Face ID or Facial Recognition is a type of biometric authentication that identifies users based on the structure, contours, and heat patterns present in their faces.

2 China's View of Win-Win

2.1 The AI Race

Sundar Pichai, CEO of Google,[17] believes that Artificial Intelligence (AI) is 'arguably the most important thing humanity has ever worked on that is deeper than electricity or fire'. In recent years, there has been a surge of interest in AI, and as a result, it has become more integrated into business and daily life processes, and AI-powered tasks are transforming enterprises, markets, and industries. Regarding AI's ability to impact the economy and society, experts and observers equate this trend to a new industrial revolution. AI has the potential to change not simply how we think about productivity or our relationship with the environment, but also aspects of national power. Artificial intelligence is projected to be one of the most disruptive emerging technologies.[18] Just as previous industrial revolutions boosted the power and influence of governments that exploited technology more broadly, AI has the same potential to change the game on a global scale.

Global leadership in several areas of fundamental and applied artificial intelligence research has emerged as a strategic aim for both major corporations and nation-states.[19] As for significant corporations, the past few years have seen increased competition between industry research groups for talented researchers and start-ups.[20] Different states have also established their own AI strategic aims.

China, for example, announced its 'Next Generation AI Development Plan' in 2017 to become a world leader in the field by 'expanding on China's first-mover advantage in AI development'.[21]

17 C Parker 'Artificial intelligence could be our saviour, according to the CEO of Google' World Economic Forum 24 January 2018 https://www.weforum.org/agenda/2018/01/google-ceo-ai-will-be-bigger-than-electricity-or-fire (accessed 26 March 2022).

18 AJW Gevel & C Noussair 'The nexus between artificial intelligence and economics' (2013) *Springer Heidelberg* at 39.

19 S Cave & S ÓhÉigeartaigh 'An AI race for strategic advantage: Rhetoric and risks' 2018 at 1.

20 KA Stiftung, 'Comparison of national strategies to promote artificial intelligence: Part 1' 2019 at 14-15 & 21.

21 G Webster et al 'Full translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)' New America 1 August 2017 https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/ (accessed 27 March 2022).

The European AI plan, launched in 2018, outlines the EU's ambition to 'lead the way in creating and using AI for good and all'.[22] Furthermore, the American AI policy, announced in early 2019 via executive order, wants to accelerate the nation's leadership in AI.[23] This terminology can also be seen in the AI strategies of other countries, such as Canada and Japan.[24] Africa is no exception, as the African Commission's Resolution 473 recognises the need to create conditions for harnessing the benefits of AI.[25] To summarise, while each strategy emphasises its specific assets, all countries want to be first, and claim to be first, in at least one component of the race.

Winning the 'race to AI' appears to be motivated not just by the need to secure a competitive position on the global market, but also as an almost existential imperative, whereby — in addition to the conventional concerns about national security[26] — economic security is invoked. Indeed, not only do the tremendous gains that potentially result from the deployment of AI[27] appear to bolster the race

22 European Commission 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the regions: Artificial Intelligence for Europe' 2018 at 2.

23 The US national AI strategy is found in Vought R 'Guidance for regulation of artificial intelligence applications (draft memorandum)' US White House 2019 at 2 https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf (accessed 28 March 2022).

24 See for example the focus on 'leadership' in Canada's AI strategy in CIFAR 'Pan-Canadian AI strategy' 2022 https://cifar.ca/ai/ (accessed 30 March 2022) or in Japan's national strategy in Strategic Council for AI Technology 'Artificial Intelligence Technology Strategy: Report of Strategic Council for AI Technology' 2017 https://www.nedo.go.jp/content/100865202.pdf (accessed 30 March 2022).

25 African Commission on Human and Peoples' Rights '473 Resolution on the need to undertake a Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa' ACHPR/Res. 473 (EXT.OS/ XXXI) 2021.

26 Notably, the 'race to AI' is often also raised in the context of a so-called 'arms race' to AI, the military sector being one of the application fields where AI is both booming and of strategic importance for countries. See in this regard, T Rabesandratana 'Europe moves to compete in global AI arms race' (2018) 360(6388) *Science* at 474; See also AA Hunter et al 'Artificial Intelligence and national security: The importance of the AI ecosystem' (2018) *Centre for Strategic and International Studies* at 3.

27 See for instance, PwC 'Sizing the price: What's the real value of AI for your business and how can you capitalise' 2017 at 8. 'See also' Deloitte 'Artificial Intelligence innovation report' 2018 at 2-8. J Bughin et al 'Notes from the AI frontier: Modeling the impact of AI on the world economy' McKinsey Global Institute 4 September 2018 at 1-2 https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy (accessed 31 March 2022).

rhetoric, but so does the high cost of non-adoption,[28] as no country wants to 'miss the [AI] train'.[29]

2.2 One step ahead for China's facial recognition technologies

The race to dominate AI technologies does not exclude surveillance. Facial recognition systems are a subfield of AI technology that can identify people from photos and videos by analysing their facial traits.[30] Deep learning, a type of AI that processes information by sending inputs through numerous stacked layers of simulated neurons, is now used to fuel facial recognition systems.[31] These neural networks are trained on thousands, if not millions, of datasets that the system is likely to meet, allowing the model to 'learn' how to accurately identify patterns in data.[32]

For years now, the use of FRTs have faced challenges with accuracy. An increasing body of research reveals disparities in error rates across demographic categories, with female, black, and 18-30-year-old individuals having the consistently lowest accuracy. An intersectional method was used to evaluate three gender classification algorithms, including those produced by IBM and Microsoft, in the seminal 2018 'Gender Shades' research. Darker-skinned females, darker-skinned men, lighter-skinned females, and lighter-skinned males were divided into four groups. All three algorithms fared poorly on darker-skinned females, with error rates of up to 34% greater than on lighter-skinned males. The National Institute of Standards and Technology (NIST) validated these findings, discovering that facial recognition systems across 189 algorithms are the least accurate for women of colour. These intriguing findings elicited quick replies, starting an ongoing debate over equity in face recognition. IBM and Microsoft announced plans to reduce bias in

28 In High-Level Expert Group on AI 'Policy and Investment Recommendations on AI' 26 June 2019 at 43 https://www.europarl.europa.eu/italy/resource/static/files/import/intelligenza_artificiale_30_aprile/ai-hleg_policy-and-investment-recommendations.pdf (accessed 27 March 2022) the European Commission's High-Level Expert Group on AI noted: 'If no action is taken the EU28 will suffer a deterioration of its innovation capital, which would result in a loss of €400 billion in cumulative added value to GDP by 2030'. See also Bughin 'Notes from the AI frontier: Tackling Europe's gap in digital and AI' 2019 at 6-1;. L Probst 'Harnessing the economic benefits of artificial intelligence' 2017 at 6-7;. V Mahidhar & T Davenport 'Why companies that wait to adopt AI may never catch up' Business Review 6 December 2018 https://hbr.org/2018/12/why-companies-that-wait-to-adopt-ai-may-never-catch-up (accessed 1 April 2022).

29 European Commission (n 22) 4.

30 W Crumpler 'How accurate are facial recognition systems — and why it does it matter?' Center for Strategic & International Studies 14 April 2020 https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter (accessed 31 March 2022).

31 As above.

32 As above.

testing by changing testing groups and improving data gathering on key demographics.

In light of the AI race, when it comes to FRTs, especially those that use facial recognition, the superior technologies are those that can identify people with accuracy, or accurately verify identities regardless of race. There have been attempts to diversify the datasets used to train facial recognition algorithms to improve the accuracy of these technologies. As a result, superior facial recognition technologies will be the most accurate and have the slightest margin for error, and states are competing to achieve this goal.

To diversify data sets, major corporations and nations have been accused of illegal collection of biometric data, especially that of people of colour. A case in point is that Google offered US$5 gift cards to its contractors in exchange for completing a demographic survey and consenting to play 'a selfie game'.[33] The contractors failed to mention that while individuals were playing, the phone was recording photographs of them, which would eventually be used to train a facial recognition algorithm. In California, four *Black Lives Matters* activists sued Clearview AI Company, which had illegally collected and stockpiled the facial IDs of 3 billion people, mostly Black people.[34]

China is keen to build the world's best AI, and Chinese corporations are looking to Africa to speed up the diversity training of their algorithms. By implementing the technique in a mainly African population, we will be able to more accurately detect other ethnicities, potentially putting the Chinese company ahead of US and European developers. For example, CloudWalk employs 3D light facial processing, which reads dark-skinned faces better than other facial recognition technologies. CloudWalk will be able to train its algorithms on data collected from Zimbabweans based on this agreement. The gathered data is intended to assist China in developing one of the world's most inclusive and racially diverse facial recognition databases.

2.3 The 'win-win' notion

China's view that exchanging facial IDs for high-end mass surveillance technologies is a win-win situation originates from the concept of 'win-win' cooperation. It is based on traditional Chinese cultural ideals of 'peace and collaboration' and adheres to the concepts of

33 K Jeremy 'Why did Google Pay black people $5 to harvest their faces?: Eye on A.I' *Fortune* 8 October 2019 https://fortune.com/2019/10/08/why-did-google-offer-black-people-5-to-harvest-their-faces-eye-on-a-i/ (accessed 1 April 2022).

34 'Facial recognition company sued by California activist' *AP News* 10 March 2021 https://apnews.com/article/san-francisco-law-enforcement-agencies-lawsuits-california-biometrics-0f7642d1f9222d8a3047f7062c91c0e7 (accessed by 1 April 2022).

peaceful coexistence and mutual gain.[35] It is also strongly tied to and promotes the notion of peaceful development with cooperation and mutual gain as the foundations of win-win solutions.[36]

China's 'win' is having access to a large pool of diverse data sets to train their algorithms, which will enable them to produce accurate facial recognition technologies, potentially putting the Chinese companies ahead of US and European developers. This is a tremendous economic benefit as these technologies are becoming employed in public safety applications such as surveillance systems, tracking offenders, and identifying fugitives.[37] It has also been used to combat human trafficking, track down kidnappers, and reuniting families with long-lost children.[38] Facial recognition is becoming a more common choice in payment and courier services in business and finance, as it maximises security and reduces fraud.[39] In the transportation industry, facial recognition has been used in airports and train stations to save passengers time at check-in, assist passengers in paying their fares, and identify unlicensed drivers and jaywalkers.[40]

Africa's gain is having access to high-end mass surveillance technologies. Carnegie's 2019 report on *The Global Expansion of AI Surveillance* deduced that Africa is lagging in expanding AI

35 Xulong 'Win-win cooperation: Formation, development and characteristics', China Institute of International Studies 17 November 2017 https://www.ciis.org.cn/english/ESEARCHPROJECTS/Articles/202007/t20200715_3604.html (accessed 29 March 2022).

36 As above.

37 Y Zeng et al 'Responsible facial recognition and beyond' Chinese Academy of Sciences, 2019 at 2; L Moon 'China's facial recognition cameras apprehend third fugitive Jacky Cheung concertgoer in two months' *South China Morning Post* 22 May 2018 https://www.scmp.com/news/china/society/article/2147245/chinas-facial-recognition-cameras-apprehend-third-fugitive-jacky (accessed 30 March 2022); K Lo 'In China, these facial-recognition glasses are helping police to catch criminals' *South China Morning Post* 7 February 2018 https://www.scmp.com/news/china/society/article/2132395/chinese-police-scan-suspects-using-facial-recognition-glasses (accessed 30 March 2022).

38 F Jenner 'Face search is the new facial recognition tool used to fight human trafficking' *Techli* 10 July 2018 https://techli.com/facesearch-is-the-new-facial-recognition-tool-used-to-fight-human-trafficking/54617/ (accessed 30 March 2022); Z Yan 'Police using AI to trace long-missing children' *China Daily* 4 June 2019 http://www.chinadaily.com.cn:9000/a/201906/04/WS5cf5c8a8a31051914270/index.html (accessed 30 March 2022); A Cuthbertson 'Indian police trace 3,000 missing children in just four days using facial recognition technology' *Independent* 24 April 2018 https://www.independent.co.uk/tech/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html (accessed 30 March 2022).

39 A Lee 'Alipay rolls out world's first 'Smile to Pay' facial recognition system at KFC outlet in Hangzhou' *South China Morning Post* 1 September 2017 https://www.scmp.com/tech/start-ups/article/2109321/alipay-rolls-out-worlds-first-smile-pay-facial-recognition-system-kfc (accessed 30 March 2022); Xinhua 'Facial recognition comes to express delivery in Chinese cities' *ChinaDaily* 12 April 2019 http://www.chinadaily.com.cn/a/201904/12/WS5cb07c72a3104842260b5f0a.html (accessed 30 March 2022); M Roux 'Why facial recognition is important for banking services' SightCorp 19 March 2019 https://sightcorp.com/blog/why-facial-recognition-is-important-for-banking-services/ (accessed 30 March 2022).

surveillance technologies, with less than one-quarter of its countries investing in AI monitoring. This is mainly attributed to technological underdevelopment.[41] Moreover, the report also acknowledges that these figures are sure to climb in the coming years as there is an increase in Chinese enterprises entering the African Market to supply these technologies. This can be seen as mutually advantageous for African countries as they reap the benefits of high-end technologies.

3 What China's viewpoint leaves out

3.1 The regulation of biometric data as a yardstick

To truly understand whether this kind of agreement mutually benefits both parties, this part of the article discusses the value of biometric data. Depending on the situation, the definition of biometric data may differ.[42] However, in a broader sense, biometrics refers to 'unique and measurable human biological and behavioural features that can be utilised for identification, or automated techniques of recognising an individual based on those qualities'.[43] While regulatory definitions vary, popular 'biometric identifiers' include retina or iris scans, fingerprints, voice prints, and scans of hand or face IDs, which is the focus of this article.[44] The inherent characteristics of biometric data necessitate protection and Regulation of this type of data since the features that uniquely identify a person are part of a person's body, and their collection and use interfere with a human's autonomy and dignity.[45]

40 S Liao 'Facial recognition scans are expanding to Delta flights in Atlanta International Airport' *The Verge* 20 September 2018 https://www.theverge.com/2018/9/20/17884476/facial-recognition-scan-delta-flight-atlanta-international-airport (accessed 27 March 2022); S Liao 'A Chinese subway is experimenting with facial recognition to pay for fares' *The Verge* 13 March 2019 https://www.theverge.com/2019/3/13/18263923/chinese-subway-facial-recognition-fares-pay-ai (accessed 31 March 2022); Xinhua 'Facial recognition identifies unlicensed drivers in Shanghai' *ChinaDaily* 6 December 2017 http://global.chinadaily.com.cn/a/201712/06/WS5a279db4a3107865316d4d6c.html (accessed 31 March 2022); L Tao 'Jaywalkers under surveillance in Shenzhen soon to be punished via text messages' *South China Morning Post* 27 March 2018 https://www.scmp.com/tech/china-tech/article/2138960/jaywalkers-under-surveillance-shenzhen-soon-be-punished-text (accessed 31 March 2022).

41 S Kemp 'Digital 2019: Internet trends in Q3 2019' Datare Portal 19 July 2019 https://datareportal.com/reports/digital-2019-internet-trends-in-q3 (accessed 28 March 2022).

42 F Nguyen 'The standard for biometric data protection' (2018) 7(1) *Journal of Law & Cyber Warfare* at 63.

43 Nguyen (n 42) 63.

44 As above.

45 C Wendehorst & Y Duller 'Biometric recognition and behavioural detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces' (2021) *European Parliamen*t at 9.

Biometric systems have primarily been governed by data-protection legislation. Biometric data is often recognised as a susceptible category of personal data and is governed by regulations on its collection, keeping, and dissemination.[46] There are underlying principles that are present in most data protection and privacy. These principles include purpose limitation, proportionality and minimisation, fairness and transparency, accountability, and consent.[47]

The most relevant principle concerning the collection of biometric data is that an individual's data should only be gathered and used with their consent. When consent is used as the basis for the collection, open disclosure to the individual of the nature of their data gathered and the intended uses of such data is required for consent to be meaningful. For example, the EU's Article 19 of the GDPR provides that when processing unique category data like biometric data, an individual's 'explicit' consent is acquired.[48] In Australia, one of the 'Privacy Principles' of the federal Privacy Act 1988 (as modified) is that personal information about an individual gathered for one reason may not be used or disclosed to another without the individual's consent.[49] Where no consent is necessary nor obtained, transparency can, at the very least, provide clear and understandable answers to ensure public trust and avoid misunderstandings. Individuals can be advised about which information is public and which is kept private. For instance, unlike the GDPR, the California Consumer Privacy Act of 2018 does not need consent prior to gathering personal information in most situations. Consumers must, however, be informed 'as to the categories of personal information to be collected and the objectives for which the categories of personal information shall be used' at the time of information collection.[50]

One of the driving forces behind worldwide agreement on the core principles of data protection has been the security of personal data transported across national borders. For example, one of the principles established in the OECD Privacy Framework governing transborder flows of personal data is that a data controller 'remains accountable for personal data under its control regardless of where the data is located'.[51] Many governments, however, ban the

46 A Kak 'The state of play and open questions for the future' in A Kak (ed) *Regulating biometrics: Global approaches and urgent questions* (2020) at 16-17.
47 World Bank Group 'Data protection and privacy laws' The World Bank 15 July 2018 https://id4d.worldbank.org/guide/data-protection-and-privacy-laws (accessed 29 March 2022).
48 General Data Protection Regulation (EU) 2016/679, hereafter 'the GDPR'.
49 See The Privacy Act 119 of 1988 Schedule 1.
50 California Consumer Privacy Act Senate Bill 1121 of 2018 sec 1798.100(b).
51 Organization for Economic Cooperation and Development: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 art 17.

extraterritorial transfer of personal data due to uncertainties about data protection laws in foreign countries. Such transfers may be approved in specific circumstances or when a third country's data protection regulations are appropriate. For example, in some cases, the EU's GDPR restricts transfers of personal data outside the European Economic Area.[52] In accordance with article 45, such transfers are permitted if the European Commission rules that the receiving country 'provides an acceptable degree of protection'. Such a move necessitates a thorough examination of the country's data protection structure, including personal data protections and oversight and recourse mechanisms.

3.2 The Zimbabwean case: win-lose

This section will illustrate that the agreement to collect the facial IDs of Zimbabweans to be used to train facial recognition algorithms in China in exchange for high-end mass surveillance technologies is a loss for Zimbabwe. Following the discussion on the underlying principles that govern biometric data, this collection violates both the principle of consent and that of cross-border data transfer.

On 3 December 2021, Zimbabwe gazetted the much-anticipated Data Protection Act, which attempts to regulate a technology-driven business environment and to protect data subjects in cyberspace by assuring the authorised use of technology.[53] Regarding consent when collecting biometric data, section 12(1) of Zimbabwe's Data Protection Act prohibits the processing of biometric data unless the data subject has granted a written agreement to the processing.[54] The requirement of consent is further elaborated in section 5.1 of the same Act as any specific, unequivocal, freely given, informed expression of will by which the data subject or their legal representative, judicial or legally appointed representative authorises the processing of their data.[55] Additionally, where the processed information is sensitive or involves genetic, biometric, or health data, section 11 of the Act states that the data subject must be informed of their right to withdraw consent at any time, without reason, and without cost.[56] Most people in Zimbabwe are not fully aware that their facial IDs are being collected, meaning, their consent was not sought.[57]

52 The GDPR (n 48), art 45.
53 See Data Protection Act 5 of 2021 ('the Act').
54 The Act (n 53), sec 12.
55 The Act (n 53), sec 5.1.
56 The Act (n 53), sec 11.
57 WH Gravett 'Digital colonisers: China and artificial intelligence in Africa' (2020) 62(2) *Global Politics and Strategy* at 164.

While the potential argument that the government of Zimbabwe can give consent on behalf of its citizens could arise, this still does not meet the threshold since the Zimbabwean Parliament has to approve international agreements entered into by the Zimbabwean President or with his authority.[58] As a result, there appears to be no intra- and inter-governmental checks and balances to establish or regulate any relevant rights Zimbabweans may have to such data and who is accountable for securing it.[59] Such an act can be exploitative and tokenising of the humans contributing to the improvement of the system for which their data is used if it is not done with the active consent of those affected and in the spirit of mutual benefit. When asked how she felt about the agreement, Natasha Msonza, the co-founder of the Digital Society of Zimbabwe, said 'it feels like CloudWalk is looking for guinea pigs,' adding that she does not 'believe that the Zimbabwe government gave this proposition much thought before volunteering its citizens to be subjected to racial facial recognition experiments'.[60]

Regarding cross-border transfer, Part VII of the Act provides that transferring personal information to a third party in a foreign country by a data controller is prohibited unless an adequate level of protection is ensured in the country of the recipient and the data is transferred solely to allow tasks covered by the data controller's competence to be carried out.[61] What constitutes an adequate level of protection per section 28(2) is determined by the circumstances of a data transfer operation or set of operations, including the nature of the data and the purpose and duration of the proposed processing operation, among other factors.[62] The recipient country, in this case, is China, where Cloudwalk is situated and has a record of disregarding data protection and privacy principles. In China, cases keep rising regarding the challenges of using FRTs in the commercial sector with major risks being transparency and cybersecurity.[63] Legal concerns arising from these technologies are no exception as a task force comprised of multiple agencies recently published an article highlighting significant privacy flaws discovered in a review of FRT-enabled mobile apps in China. These include the requirement for users to provide facial information, the lack of clear rules for information gathering, and the difficulty in withdrawing consent for the collection and use of facial information.[64]

58 'Constitution of the Republic of Zimbabwe, 2013' (as set out in sec 1 of the Constitution of Zimbabwe Amendment Act 20 of 2013) sec 327(3).
59 Gravett (n 57) 164.
60 A Hawkins 'Beijing's big brother tech needs african faces' *Foreign Policy* 24 July 2018 https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/ (accessed 30 July 2021).
61 n 53, Part VII.
62 n 53, sec 28(2).
63 Luo & Guo (n 3) 162.
64 As above.

4 Redefining a win-win situation

This section explores ways in which this type of agreement can be mutual — a win-win situation. The first option explored is the 'ban option' and the second is the data protection route.

As it concerns the ban option, this involves countries that have opted to ban the use of facial recognition technologies until there is adequate protection of biometric data. Wojciech Wiewiorowski, the European Data Protection Supervisor, remarked at the Biometrics Institute's 2020 Congress that he supports the idea of a moratorium on the deployment of biometrics in public areas in the EU to allow for an informed and democratic debate.[65] Other countries are pressing for a moratorium or even outright bans. For example, the Australian Human Rights Commissioner has advocated for a moratorium until adequate legislation is enacted.[66] Similarly, in 2019, California became the first state in the United States to prohibit the use of FRT by law enforcement organisations.[67] In 2020, the city of Portland banned FRT not only for all governmental departments, including local police, but also for private businesses, such as hotels and restaurants.[68] Even in China, there has been some backlash towards the use of facial recognition, especially concerning who has access to this data. Most individuals feel like they are constantly being watched.[69] In the 2019 case of Guo Bing, a professor at Hangzhou's Zhejiang University filed a lawsuit against a nearby wildlife park when it tried to subject him to additional, required facial scans months after he purchased a yearlong permit. This was the first case of its kind and indicated the discomfort many citizens feel with the mass surveillance they have been subjected to.[70] Following this case, Hangzhou, the eastern Chinese city, home to the Chinese tech giant Alibaba, has issued a draft rule prohibiting property managers from

65 W Wiewiórowski 'The state of biometrics: Update from the European data protection supervisor' Centre for Strategic & International Studies, 2020 at 4.

66 J Bajkowski 'Human Rights Commission wants moratorium on expanding facial recognition' *IT News* 17 December 2019 https://www.itnews.com.au/news/human-rights-commission-wants-moratorium-on-expanding-facial-recognition-535684 (accessed 2 April 2022).

67 G Kostka et al 'Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom and the United States' (2021) 30(6) *Public Understanding of Science* at 672; T Greene 'California bans law enforcement from using facial recognition software for the next 3 years' *TNW* 10 October 2019 https://thenextweb.com/news/california-bans-law-enforcement-from-using-facial-recognition-software-for-the-next-3-years (accessed 2 April 2022).

68 Kostka et al (n 67) 672.

69 Human Rights Watch, 'China's global threat to human rights' 25 March 2014 https://www.hrw.org/world-report/2020/country-chapters/global (accessed 1 September 2021).

70 A Kerry, 'China facial recognition: Law professor sues wildlife park,' *BBC News* 8 November 2019, https://www.bbc.com/news/world-asia-china-50324342 (accessed 8 November 2015).

installing facial recognition cameras in residential compounds without first obtaining consent from local inhabitants.[71] The proposed legislation follows a first-of-its-kind lawsuit over facial recognition technology in Hangzhou. At a national level, African countries can opt to ban the adoption of mass surveillance technologies from China until there are policies protecting their citizens' data. This may be considered an extreme option as such a decision will disregard some of the benefits of surveillance in developing countries, such as security and border control.

The second option is the data protection Route. This option entails states providing data protection laws that regulate biometric data. According to David Kaye, UN Special Rapporteur on the Promotion and Protection of the Right to Free Expression, these technologies operate in a 'free for all' environment, spreading 'technology that is causing immediate and regular harm to individuals and organisations that are essential to democratic life'.[72] He advocates for creating worldwide norms and publicly owned procedures to regulate domestic and foreign usage of private monitoring technology.[73] When it comes to facial recognition technologies, one of the most significant concerns is the protection of an individual's privacy and, more precisely, people's consent when it comes to collecting and using their facial IDs. When it comes to issues arising from the use of facial IDs, the GDPR has already provided the EU with tight regulations for the protection of personal data.

The European Commission also intends to establish severe limitations on facial recognition technology to provide EU residents specific control over how their data is used. For Africa, at a continental level, the AU's Convention on Cyber Security and Personal Data Protection seeks to tighten existing information and communication technology legislation in its member countries.[74] Personal data processing is only considered valid under the convention if the subject has given his or her consent.[75] States are required to prevent data collection and processing of racial, ethnic, or geographical origin.[76] Notably, an AU member state cannot transfer personal data to a non-member state unless the latter state

71 CGTN 'Facial recognition in the spotlight: Hangzhou targets' 2 November 2020 https://news.cgtn.com/news/2020-11-02/Hangzhou-targets-partial-ban-of-facial-recognition-technology-V5vZD8UaGc/index.html.

72 United Nations 'Moratorium call on surveillance technology to end 'free-for-all' abuses: UN Expert' United Nations News 25 June 2019 https://news.un.org/en/story/2019/06/1041231 (accessed 31 August 2021).

73 As above.

74 See African Union Convention on cyber security and personal data protection 2014, hereafter 'AU Convention' Preamble.

75 AU Convention (n 74) chap II sec 3 art 13(1).

76 AU Convention (n 74) chap II sec 3 art 14(1).

guarantees the privacy, freedoms, and fundamental rights of the individual or persons whose data is transferred.[77] Individuals also have the right to be notified before their data is shared with third parties for the first time and to object to such disclosure expressly.[78] The convention has fourteen signatories and has only been ratified by eight countries.[79] The ratification of this convention by more African countries can strengthen the Act to promote more nuanced data protection.

Concerning national regulations of biometric data, as of 2022, 33 out of the 54 African countries have passed specific rules and regulations to protect personal data, and this number is steadily increasing. Many of these countries' laws have been motivated by the EU GDPR, which has set an example for many.[80] Current trends show that many African countries have passed comprehensive data privacy legislation and established fully functional data protection authorities. This is in reaction to the growing need for states to protect people's data by giving individuals data rights, implementing rules on how businesses and governments use data, and establishing authorities to enforce these laws. Some of these emerging tendencies are discussed below.[81] This is a positive trajectory with prospects of strengthening data protection laws, especially concerning biometric data.

5 Conclusion

The article examined whether China's view that exchanging African Facial IDs for high-end mass surveillance technology is a win-win situation. At the surface level, the notion that this agreement is mutually beneficial to both China and Africa has not only been perpetuated by China, but Africa has also bought into this idea. However, a closer examination of what the agreement means for each party reveals that it is, in fact, a 'win-lose' agreement. To demonstrate this, the article had three objectives. The first objective was to discuss China's view of 'win-win', and the findings are that this agreement is a win for China as access to African Facial IDs will contribute to diversifying their data sets. As a result, this will lead to

77 AU Convention (n 74) chapter II sec 3 art 14(6)(a) & 14(6)(b).
78 AU Convention (n 74) chapter II sec 3 art 18.
79 African Union 'List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection' 2020.
80 Privacy International Organisation '2020 is a crucial year to fight for data protection in Africa' 3 March 2020 https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa (accessed 1 August 2021).
81 B Daigle 'Data protection laws in Africa: A pan-African survey and noted trends' *Journal of International Commerce and Economics* 2021 at 2-3 https://www.usitc.gov/journals (accessed 3 April 2022); T Hadebe 'Trends' Data Protection Africa 31 March 2020 https://dataprotection.africa/trends/ (accessed 3 April 2022).

the production of FRTs that are more accurate and inclusive, which puts China one step ahead in the AI race.

As for the second objective, the article analysed what is obscured by China's viewpoint. Facial IDs, which qualifies as biometric data, are sensitive data regulated by biometric data principles. The findings in this section show that the collection of facial IDs goes against the principles of biometric data, such as consent, and this makes Africans (in this case, Zimbabweans) vulnerable to data violation practices. The third objective was to redefine a genuine 'win-win' for both China and Zimbabwe, and the article recommends two paths. The first is a ban option of FRT until there are laws to protect biometric data, and the second option looks to the data protection route. Since the global rise and adoption of data protection laws, African countries have also welcomed the incorporation of these laws. Data protection laws seem to be the most promising solution to levelling the playing field and ensure a *truly* win-win situation.