Digital Coloniser? China and Artificial Intelligence in Africa

Willem H. Gravett

Abstract

By using African countries as laboratories to improve its AI-based technologies, China is also reinforcing African governments' illiberal and authoritarian tendencies.

China is aggressively pursuing artificial-intelligence (AI) capabilities, and spending billions on related research.[1] China uses these technologies domestically for surveillance and social control, spying on its citizens, learning about their private and public actions, and regulating their behaviour.[2] In Xinjiang, for example, authorities conduct mass collection of biometric data, including voice samples and DNA, and use AI-enabled facial-recognition technology to identify, classify and track Uighur Muslims.[3]

In 2015, Beijing launched its 'Made in China 2025' plan with an eye to dominating cutting-edge technology industries.[4] An integral part of China's strategy is to become the world's premier artificial-intelligence innovator by 2030, surpassing its rivals technologically, and to build a core domestic AI industry with gross output exceeding $150 billion.[5] The Chinese Communist Party envisions that AI will play a crucial role in maintaining social stability, not only in such areas as education, healthcare and environmental protection, but also in state security, where applications include internet censorship and analysing surveillance-camera footage to trace people's movements.[6] Kai-Fu Lee, one of China's best-known high-tech venture capitalists, has argued that China has an advantage in developing AI because its leaders are 'less fussed by "legal intricacies" and "moral consensus"'. According to him, the Chinese 'are not passive spectators in the story of A.I. – we are the authors of it' such that 'the values underpinning our vision of an A.I. future could become self-fulfilling prophecies'.[7]

Significantly for Africa, China hopes to become a world leader in AI in part by using developing countries as laboratories to improve its surveillance technologies. In March 2018, the Chinese AI start-up company CloudWalk Technology, based in Guangzhou, signed an agreement with the government of Zimbabwe to deploy facial-recognition technology there. Beijing touted the agreement as an example of 'win–win' diplomacy – Chinese AI companies would have the opportunity to train their algorithms on African faces to diversify their datasets and improve the accuracy of their products, and the Zimbabwean government would have access to cutting-edge technology to monitor its population.[8]

PricewaterhouseCoopers has estimated that AI technology could increase global GDP by $15.7 trillion – a full 14% – of which $1.2trn would be added for Africa.[9] AI could help solve some of Africa's most intractable development problems.[10] In particular, it could help farmers adapt to climate change, assist in predicting the outbreak of diseases and natural disasters, facilitate the protection of wildlife from poachers and help make congested urban centres more liveable. African nations have accordingly begun turning to AI for solutions.[11]

With this potential power, however, come possible abuses and unintended consequences.[12] In particular, the current use of Chinese technology exports to the continent, especially facial-

recognition technology, raises grave human-rights concerns. Repressive governments in Africa could use centralised biometric databases to target political opponents and to reinforce discrimination against specific segments of the population.

Vectors of China's influence

Chinese technological penetration in Africa raises the spectre of digital neocolonialism – that is, China's application of economic and political pressures to control and strategically influence African governments. Although China's presence in Africa has been growing steadily for 20 years, it started escalating drastically in 2013 following Chinese President Xi Jinping's unveiling of the Belt and Road Initiative (BRI), a trillion-dollar international-development strategy to extend Beijing's influence in host countries through bilateral loans and infrastructure projects.[13] Most African countries have enthusiastically embraced the BRI.[14] China has emerged as the largest source of financing for infrastructure projects in Africa, and evidence of its influence is on wide display on the continent.[15]

China is also sponsoring training and education for the next generation of African leaders, bureaucrats, students and entrepreneurs, hosting tens of thousands of African university students annually, while the Chinese government offers thousands of scholarships to African students every year.[16] The Hanban (Chinese Language Council) has also founded 59 Confucius Institutes in Africa to spread Chinese language and culture.[17]

The BRI emphasises information technology.[18] And in Africa, China is unrivalled on the technological front.[19] Much of the continent has come to rely on Chinese companies for their telecommunications and digital services.[20] China Telecom plans to lay a 150,000-kilometre fibre-optic network covering 48 African nations.[21] Transsion Holdings, a Shenzhen-based company, has overtaken Samsung to become the leading smartphone provider in Africa.[22] Huawei, the Chinese telecommunications giant, has built 70% of the 4G networks and most of the 2G and 3G networks on the continent, vastly outpacing its European rivals.[23] The Kenyan government has appointed Huawei as principal adviser on its 'master plan' for information and communication technologies.[24] ZTE Corporation, the Chinese telecommunications conglomerate, provides the Ethiopian government with infrastructure to enable it to monitor communications by opposition activists and journalists.[25] Another Chinese company, H3C, won the contract to build a new telecommunications network for the Nigerian international airport in Abuja.[26] Hikvision has established an office in Johannesburg and, through a local video-surveillance provider, rolled out 15,000 cameras throughout the metropolitan area in 2019.[27]

Chinese companies play a clear role in Beijing's aspirations for global telecommunications dominance. Although some of these firms are ostensibly private enterprises motivated by market forces, all of them remain answerable to the government.[28] Hikvision, the world's leading manufacturer of surveillance-camera equipment, has strong ties to the Chinese government. The company disclosed in its 2018 annual report that the Chinese government was a controlling shareholder, and the company's chairman was appointed to the National People's Congress in 2018.[29] Similarly, a company owned by the Chinese government is the controlling shareholder in ZTE.[30] Huawei's founder is Ren Zhengfei, a former officer in the 'military technology division' of the People's Liberation Army.[31] Powerful ties between Huawei's management and the Chinese security and intelligence apparatus have continued.[32] The company reportedly receives billions of dollars in government subsidies.[33]

The Chinese Communist Party has systematically placed 'party cells' led by senior executives in technology companies to enhance its access to and control over these companies.[34] Moreover, a national-security law enacted in 2015 mandates that companies acquiesce to 'third-party' (read: government) access to their networks, source codes and encryption keys.[35] The significant inroads that especially Huawei has made in Africa – despite American warnings about corresponding cyber-security vulnerabilities – is evidence that for African governments and businesses, the imperative of greater internet access trumps all other considerations.[36]

Many African nations, further attracted by easy loans and investments, have become almost entirely dependent on China for their technology and services, and susceptible to pressure to subscribe to the Chinese notion of 'internet sovereignty'.[37] The danger is that this Chinese model of sprawling censorship and automated surveillance systems will lead to a dramatic reduction in digital freedom across the continent and imperil emerging democracy.[38] Ostensibly to help governments identify threats to 'public order', China appears to be promoting digital authoritarianism as a way for African governments to control their citizens through technology.[39] For example, the technology provided by ZTE over the past 20 years has been integral to the Ethiopian government's efforts to monitor private citizens and organisations, especially those who are critical of the government.[40] Huawei is the leading vendor of advanced surveillance systems worldwide by an enormous margin, and it is aggressively seeking new markets in sub-Saharan Africa. It is setting up advanced 'safe city' platforms, offering facial recognition and intelligent video-surveillance systems to repressive governments, and providing advanced analytic capabilities.[41] A recent *Wall Street Journal* investigative report found that Huawei technicians in both Uganda and Zambia had assisted government officials in spying on political opponents.[42]

Through seminars and official visits, the Chinese government is actively advising media elites and government officials in countries participating in the BRI to follow its lead on internet sovereignty. According to Freedom House, 'increased activity by Chinese companies and officials in Africa preceded the passage of restrictive cybercrime and media laws in Uganda and Tanzania' (whose largest trading partner is China), as well as in Nigeria, during 2018.[43] The governments of Cameroon, Chad and Togo have also ordered internet shutdowns and blocked websites and socialmedia platforms ahead of critical political moments, such as elections and protests.[44] The *Financial Times* reported that at least five governments in Africa – Chad, Democratic Republic of the Congo, Eritrea, Ethiopia and Mauritania – had shut down the internet in the first half of 2019, and that in June of that year the Sudanese government did so 'as soldiers from a government paramilitary force went on a killing spree in the capital Khartoum … preventing protesters from documenting the violence on social media'.[45] Benin, Tanzania, Uganda and Zambia have also started stifling freedom of expression through the imposition of social-media or 'blogger' taxes, 'leaving millions of Africans struggling to cover the costs of getting online'.[46]

The Chinese government's dominance over internet connectivity on the continent affords it significant leverage over African governments.[47] China could foster African nations' dependence on and financial obligation to China, echoing their relationships with their erstwhile colonisers. This could lead to China's inordinate political control over African governments and populations. The AI technology and data-mining techniques that China is providing constitute an especially acute temptation to such states, and could increase China's leverage.

Facial-recognition technology in China

China has become the fastest-growing user of facial-recognition technology.[48] This technology has proven to be a potent tool for maintaining control over Chinese society.[49]

Facial-recognition cameras are much more intrusive and discriminating than ordinary closed-circuit television (CCTV), which has been a mainstay of police forces for 25 years.[50] The technology, first developed and used in the West, is powered by AI algorithms. It analyses a person's distinctive facial features in minute detail, distinguishing them from thousands or even millions of potential matches. The algorithms can also assess in real time the number and density of people in a given frame, individuals' gender, their height, the characteristics of their clothing and even their gait. Facial-recognition cameras are often mobile and concealable. Thus, they can scan distinctive facial features in order to create detailed biometric maps or databases of individuals when they are walking down the street without their knowledge, let alone their consent. In effect, facial-recognition technology enables a government to remotely secure a GPS ankle monitor on any person.[51]

China's path to online censorship and digital surveillance started in the early 2000s with projects such as Golden Shield and continued thereafter with programmes like Skynet. In 2015, the Chinese Ministry of Public Security launched a project to establish the world's most powerful facial-recognition system, which will be able to identify any one of China's 1.393bn citizens within three seconds and with 90% accuracy. The system will be connected to surveillance-camera networks and will use cloud facilities to connect to data-storage and -processing centres across the country. Isvision, a security company based in Shanghai, is developing the system. It has set up similar systems for law-enforcement authorities in Xinjiang and Tibet.[52] In early 2018, Chinese police also deployed facial-recognition glasses. The Beijing-based company LLVision Technology sells basic versions of this technology to countries in Africa and Europe. Such glasses can be used to identify criminals, such as drug dealers and thieves, but also to hunt down human-rights activists and dissidents.[53]

China, of course, is not the only country experimenting with facial-recognition technology. The United States, which already had approximately 62 million CCTV security cameras installed as of 2016, has higher per capita penetration than China.[54] The FBI's Next Generation Identification System uses facial recognition to compare images from crime scenes with a national database of mug shots. But China's ambition sets it apart. Western law-enforcement agencies generally use facial recognition to identify criminal suspects – not to track social activists or dissidents, or to monitor entire ethnic groups. According to Maya Wang of Human Rights Watch, what distinguishes China is 'a complete lack of effective privacy protections, combined with a system that is explicitly designed to target individuals seen as "politically threatening"'.[55]

China's development of what Richard Fontaine and Kara Frederick call the 'autocrat's new tool kit' will have a profound impact on the rights and liberties of its citizens.[56] Indeed, the Uighurs have already felt that impact acutely.[57] The Chinese government has been waging a well-documented mass-surveillance and internment campaign against them in the fractious, far-western region of Xinjiang, where approximately one million people have been detained in 're-education' camps.[58] In Xinjiang, facial-recognition cameras have become ubiquitous at roadblocks, gas stations, airports, railways and bus stations, residential and university compounds, and entrances to Muslim neighbourhoods and mosques.[59] More than 2,500 cameras have also been installed in Ulan Bator, the capital of Mongolia.[60] The Chinese

government is using biometric data, including facial recognition, iris scans and mass DNA collection, to track Uighurs and other minorities on an unprecedented scale.[61] Technology maps the target population's activities street by street and phone by phone. In the cities of Hotan and Kashgar there are poles bearing as many as ten video cameras at intervals of 100–200 metres along every street. As well as watching pedestrians, these cameras can read car number plates and correlate them with the faces of drivers. The cameras are equipped to work continuously, night and day.[62]

Thus, Xinjiang has become, in the words of Freedom House's Sarah Cook, 'a laboratory for testing big-data, facial recognition and smartphone-scanner technologies that can eventually be deployed across China and beyond'.[63] Several Chinese AI companies, including CloudWalk, Hikvision and SenseTime, have emerged on the cutting edge of this effort. Their work entails complicity in the oppression of Xinjiang's Uighur Muslim population and other groups.[64] Seen in a broader context, this is perhaps unsurprising. The Chinese state argues, and most of the Chinese population believes, that invasive surveillance practices have a specific and relatively narrow purpose – namely, to combat what Beijing calls the 'three evils' – terrorism, separatism and religious extremism – and that they are showing positive results. From this perspective, developing the world's leading AI algorithms is primarily a political and security endeavour rather than a commercial one. The Chinese companies' management, of course, sees their involvement in government monitoring and detention activities in Xinjiang as affording them a competitive edge in the international market, because access to large amounts of data is essential to developing and refining AI algorithms. Data on and images of ethnic Chinese and Turkic Uighurs could enable developers to correct common race-related errors – some stemming from biases inherent in Western training – in facial-recognition software and gain market share in other parts of the world.[65]

Authorities in Xinjiang have repeatedly stated that their goal is to achieve both 'ethnic unity' and 'social stability'.[66] The facial-recognition technology, which is integrated into China's rapidly expanding networks of surveillance cameras, looks exclusively for Uighurs based on their physical appearance, and maintains records of their movements for search and review. According to the *New York Times*, this is 'the first known example of a government intentionally using [AI] for racial profiling', and may usher in 'a new era of automated racism'.[67] It is facial recognition in aid of racial recognition.

In 2018, a respected US academic journal published a study entitled 'Facial Feature Discovery for Ethnicity Recognition', authored by one Australian and four Chinese scholars. The study determined that an effective way to automatically predict the ethnicities of minorities in China was for facial-recognition systems to focus on specific, T-shaped regions of their faces.[68] The researchers based this conclusion on more than 7,000 photographs that they took of Uighur, Tibetan and Korean students at Dalian Minzu University in northeastern China. The study sparked concern given that widespread use of pre-emptive racial profiling to guide detentions and arrests could violate the presumption of innocence and other human rights.[69]

A new generation of abundantly financed Chinese start-up companies are catering to Beijing's demand for emerging technologies, such as AI. Most now sell analytic software that enables police to automatically distinguish Uighurs from others. Hikvision, in particular, has explicitly marketed its technology as a tool for racial and ethnic profiling.[70] Similar tools could incorporate biases based on the skin colour and other aspects of ethnicity of other groups elsewhere in the world. Clare Garvie of Georgetown University School of Law's

Center on Privacy and Technology comments: 'If you make a technology that can classify people by ethnicity, someone will use it to repress that ethnicity.'[71]

In May 2019, David Kaye, the United Nations Special Rapporteur on freedom of expression and opinion, concluded that the problem of pervasive technological surveillance was serious enough to warrant not merely tighter regulation of surveillance exports and restrictions on their use, but also an immediate moratorium on the global sale and transfer of the tools of the private surveillance industry, until rigorous human-rights safeguards were put in place to regulate such practices.[72]

Some Chinese companies, such as YITU, CloudWalk and Hikvision, focus explicitly on exporting sophisticated surveillance technology to Africa. The Chinese authorities' ongoing persecution of Uighur Muslims suggests that these technologies, despite the limitations of sensors in rural areas, will allow African governments to track many of their citizens.[73] On a continent with a troubled history of genocide, ethnic violence and apartheid, this is an alarming prospect.

Chinese facial-recognition technology in Africa

China is projected to dominate the $7bn global market for facial-recognition devices, with a 44.59% market share by 2023 and CloudWalk leading all providers.[74] China also wants to use developing countries as laboratories for improving its own surveillance technologies.[75]

In April 2018, CloudWalk launched China's first AI project in Africa when it signed a strategic-cooperation agreement with the government of Zimbabwe to build a mass national facial-recognition database and monitoring system in Zimbabwe's cities and public-transport system, including smart financial systems (to integrate finance with technology), and airport, railway and bus-station security.[76] Under this arrangement, the Zimbabwean government will apparently provide biometric data on thousands of Zimbabweans to China, which will enable it to build a more comprehensive facial-recognition database reflecting greater ethnic diversity to train CloudWalk's AI programmes.[77]

Gaining access to a population with a racial mixture far different from that of China will give CloudWalk a crucial competitive edge. Well-documented difficulties in accurately recognising faces with darker skin tones have plagued commercial facial-recognition systems developed in the West and China. The Massachusetts Institute of Technology's (MIT) Media Lab tested the accuracy of the equipment of three major facial-recognition software providers – Microsoft and IBM, both American companies, and Megvii, a Chinese one. According to the MIT study, the error rate for identifying the gender of a person from photographs of lighter-skinned men was less than 1%, for darker-skinned women as high as 35%.[78] This is because the accuracy of AI depends on the data from which it learns, and facial-recognition AI has learned predominantly from Caucasian-male faces.[79] In this connection, it is worth noting that the Black Lives Matter protests that began in the United States prompted Amazon to impose a one-year moratorium on police use of its facial-recognition software, known as Rekognition, in part because it was inaccurate.[80]

The biometric records of Zimbabwean citizens are therefore crucial both for enhancing the Chinese government's own 'tech-infused policing capacity' and for making CloudWalk's products more effective and commercially attractive.[81] CloudWalk – and ultimately all Chinese AI technology – will benefit tremendously from this opportunity to rapidly improve

its systems.[82] As with many of the agreements that China enters into in Africa, the facial-recognition technology was part of a comprehensive package under the wide-ranging BRI sweetened with soft loans, infrastructure development and technological assistance. That said, the Zimbabwean parties did not resist accepting the AI-related terms.[83] In essence, Zimbabwe is getting access to technology it would never be able to afford on the open market by using its own citizens' data as currency. Thus, this first foray of Chinese AI technology into Africa is occurring free of the ethical and legal questions that are raised in more developed markets.[84]

It is clear that CloudWalk intends to use Zimbabwe as a large research laboratory.[85] Amy Hawkins of *The Economist* has observed, other than possibly increased security and surveillance measures, the people of Zimbabwe will not see any return on the research that their personal data has facilitated. 'Acceleration is the whole point because the global AI race is ultimately a race to set standards', she writes.

> The Chinese government defines its ambitions as becoming the country that is 'setting the pace.' As racial upsets in facial recognition have shown, the standards in this field are still to play for. But with unprecedented access to a more diverse range of data, Chinese companies are edging ever closer to this goal – spreading their model of authoritarianism along the way.[86]

Hawkins may be exaggerating China's imperialism on this score. But the fact remains that legal loopholes have made it possible for Harare to share the data of thousands of Zimbabweans with CloudWalk, possibly compromising their personal privacy and safety.[87] Kuda Hove, a programme officer for the Media Institute of Southern Africa, which promotes freedom of expression in Zimbabwe, notes that

> people did not consent to the use of their biometric data in this way. Unfortunately, people do not have any way of holding the government accountable as there are no laws in place or any regulatory body tasked with the protection of people's privacy or data … Zimbabwe's 2002 Access to Information and Protection of Privacy Act doesn't cover biometric data or cross-border flows of data … The government has rarely ever acted in the people's interests.[88]

It goes almost without saying that the CloudWalk–Harare deal does not allow individual citizens to opt out of biometric-data collection. Thus, there appear to be no intra-and intergovernmental checks and balances establishing or regulating any relevant rights Zimbabweans may have to such data and who is responsible for protecting it.

China's mining of Zimbabweans' data also revives painful memories of the European powers' exploitation of Africa for its human and natural resources during the colonial era. Journalist and cognitive scientist Abeba Birhane writes:

> These firms take it for granted that such 'data' … automatically belongs to them. The discourse around 'data mining' and 'data rich continent' shows the extent to which the individual behind each data point is non-existent … [and] is symptomatic of how little attention is given to privacy concerns. The discourse of 'mining' people for data is reminiscent of the colonizer attitude that declares humans as raw material free for the taking.[89]

Especially given Africa's record of weak institutions, corruption and authoritarianism, government officials, civil-society leaders and technology entrepreneurs in Africa should be sensitive to the ways in which the collection, analysis and storage of Africans' biometric data might be dehumanising.[90]

Of course, CloudWalk's AI technology does provide an attractive means for the Zimbabwe government – which has a bleak record on human rights – to manage its own surveillance programme, helping the government identify, track and monitor its people.[91] And the deal will enable Zimbabwe to replicate parts of the very surveillance infrastructure that has limited individual freedoms so severely in China. Indeed, live facial recognition has the potential to fundamentally change the relationship between people and the police, and even alter the very meaning of public space.[92] When Zimbabwean citizens walk past a facial-recognition camera, they will effectively be standing in a police line-up with other pedestrians alongside those suspected of crimes. Although the professed purpose of the technology is to combat crime in Zimbabwean cities, it could also be used to stifle opposition.[93] Zimbabwean journalist Garikai Dzoma believes that 'the benefits of using the database and technology to fight crime are far outweighed by the dangers the system poses to individual freedoms'.[94] For example, facial-recognition cameras could identify every individual who attends a protest.[95] They could automatically flag behaviour deemed suspicious, or people who look or act in a certain way.

This is not dystopian alarmism. It is precisely how the Chinese government is already using the technology. Freedom House ranks China at 14/100 and Zimbabwe at 30/100 in lack of internet freedom. It is unlikely that Zimbabwe will become freer – in the sense of more liberal – as a result of its collaboration with China on surveillance technology, even if the effort results in a reduction of crime. It's more probable that the Zimbabwean government intends to use this technology to attempt to monitor and control the population.

The Zimbabwean government has long curtailed freedom of expression by various means. In 2015, then-president Robert Mugabe accepted a gift of cyber-surveillance software from Iran, including international mobile subscriber identity (IMSI) catchers, which enable eavesdropping on telephone conversations.[96] Zimbabwe has also previously looked to China as a model for managing several aspects of society, including social media and communications. In 2016, Mugabe heralded China as an example of social-media regulation that he hoped Zimbabwe could emulate.[97] Zimbabwe's 2017 Cybercrime and Cybersecurity Bill criminalised communicating falsehoods online – the same legal pretext China has employed to stifle dissent.[98] The technology provided by the CloudWalk deal will leave government opponents in Zimbabwe with even fewer places to hide. Zimbabwe's post-Mugabe government seems even more determined to establish dominion over all aspects of its digital and public spaces.[99] In January 2019, after days of protests over a 100% increase in fuel prices, security forces launched a crackdown in which 12 people were killed and 600 were arrested. The government also ordered its first countrywide internet shutdown.[100]

Potential legal redress

Appropriately applied, the African Union Convention on Cyber Security and Personal Data Protection could minimise the type of exploitative data mining on the African continent threatened by the CloudWalk–Harare deal. Unfortunately, fewer than 20% of African nations have signed it, and Zimbabwe is not one of them.[101] But future abuses may produce national and international pressure on non-signatories to relent.

The convention mandates that the establishment of a regulatory framework on cyber security and personal data protection respect the rights of citizens, guaranteed under the fundamental texts of domestic law and protected by international human-rights conventions and treaties, particularly the African Charter on Human and Peoples' Rights. The convention also calls for the establishment of an appropriate normative framework consistent with the African legal, cultural, economic and social environment.

Under the convention, the processing of personal data is considered legitimate only when the subject has given his or her consent.[102] States are compelled to prohibit any data collection and processing revealing racial, ethnic or regional origin.[103] Significantly, an AU member state cannot transfer personal data to a non-member state, unless the latter state ensures the protection of the privacy, freedoms and fundamental rights of the person or persons whose data is transferred.[104] Additionally, individuals have the right to be informed before their personal data is disclosed for the first time to third parties, and to expressly object to such disclosure.[105]

In late 2019, the African Commission on Human and Peoples' Rights promulgated the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa.[106] The declaration directly addresses the protection of personal information and communication surveillance in the context of the right to privacy. While the declaration is not a mandatory legal document, it is strongly precatory, and establishes the preferred legal framework for the protection of personal information that requires states to adopt laws regulating the processing of personal information.[107]

According to Principle 40, individuals have a right to privacy, including the right to protect personal information against access by third parties through digital technologies.[108] Principle 42 calls on states to ensure that individuals consent to the processing of their personal information; that the processing of personal information is 'in accordance with the purpose for which it was collected … and not excessive'; that the processing is transparent; and that the information is kept confidential and secure at all times.[109] In addition, every person has the right to control his or her own personal information.[110]

If Zimbabwe were to ratify the convention and respect the declaration, domestic Zimbabwean legislation would prohibit the government from gathering Zimbabweans' biometric data wholesale, allow individual citizens to opt out of the process and prohibit outright the transfer of citizens' biometric data to Chinese entities.

* * *

Many Africans worry that they will be left behind in the global AI race and the corresponding economic transformation. But the danger also looms that those in the developing world will become mere passive consumers – and potential victims – of AI systems developed elsewhere for different people, cultures and situations.[111] As China strives to become an AI powerhouse and the dominant force in AI technology on the African continent, the moral, ethical and cultural concerns raised by what Freedom House's Adrian Shahbaz has called China's 'techno-dystopian expansionism' deserve greater attention.[112] During a recent debate on AI ethics and norms, Chinese scholar Zhang Wei expressed China's chillingly doctrinaire approach to AI ethics: 'Chinese values means that China will value the security of the collective over the rights of the individual when it comes to AI.'[113] Facial-recognition technology has unprecedented potential for the large-scale invasion of privacy and erosion of

individual rights. Sifting data to look for pickpockets, robbers and terrorists can easily morph into ferreting out and repressing political dissidents. Democratic governments should resist the temptation to undermine human rights in the name of safety and security, and refrain from sacrificing individual rights at the altar of innovation.[114]

African nations should take a step back and collectively consider to what extent they actually need or want widespread facial-recognition technology, what sensible measures of regulation or legislation might look like, and how to ensure that national law-enforcement and security agencies do not abuse the technology.[115] Africans themselves – in particular, entrepreneurs active in the AI field – should consider how AI can benefit local communities and not blindly import Chinese AI systems premised on authoritarian control, or, for that matter, Western AI systems spurred by excessive enthusiasm for technological advances or profit. They will have to distinguish between using new technologies legitimately for traditional law-enforcement, counter-terrorism and military purposes, and using them illegitimately to solidify single-party social control and curtail basic human rights.[116]

Lawmakers, civil-society leaders and technologists should press for appropriate safeguards to deal with the practical human-rights challenges arising from major AI-related programmes.[117] Unlike China, Zimbabwe and some other African countries have constitutions and laws that protect individual rights, including privacy and freedom of expression. Furthermore, Africans can call upon an international human-rights frame-work to address violations, and have access to a fairly robust regional human-rights system that could be mobilised to constrain potentially repressive Chinese technology.

Notes on contributors

Willem H. Gravett teaches law at the University of Pretoria.

Notes

1 See Arthur Gwagwa and Lisa Garbe, ‘Exporting Repression? China’s Artificial Intelligence Push into Africa’, Council on Foreign Relations, 17 December 2018, https://www.cfr.org/blog/exporting-repression-chinasartificial-intelligence-push-africa.

2 See Michael Cook, ‘Exporting Enslavement: China’s Illiberal Artificial Intelligence’, Mercatornet, 15 August 2018, http://mercatornet.com/exporting-enslavement-chinasilliberal-artificial-intelligence/23473/.

3 See Gwagwa and Garbe, ‘Exporting Repression?’.

4 See Amy Hawkins, ‘Beijing’s Big Brother Tech Needs African Faces’, *Foreign Policy*, 24 July 2018, https://foreignpolicy.com/2018/07/24/beijingsbig-brother-tech-needs-african-faces/.

5 See Jeffrey Ding, ‘Deciphering China’s AI Dream: The Context, Components, Capabilities, and Consequences of China’s Strategy to Lead the World in AI’, Future of Humanity Institute, University of Oxford, March 2018, p. 7, https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf; Hawkins, ‘Beijing’s Big Brother Tech Needs African Faces’; Christina Larson, ‘China’s Massive Investment in Artificial Intelligence Has an Insidious Downside’, *Science*, 8 February 2018, https://www-sciencemag-org.uplib.idm.oclc.org/news/2018/02/china-s-massive-investment-artificialintelligence-has-insidious-downside; and Paul Mozur, ‘Beijing Wants AI to Be Made in

China by 2030', *New York Times*, 20 July 2017, https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html.

6 See Xiao Qiang, 'The Road to Digital Unfreedom: President Xi's Surveillance State', *Journal of Democracy,* vol. 30, no. 1, January 2019, pp. 25–39.

7 Quoted in 'For Artificial Intelligence to Thrive, It Must Explain Itself', *The Economist*, 15 February 2018, https://www.economist.com/science-and-technology/2018/02/15/for-artificial-intelligence-to-thrive-itmust-explain-itself.

8 See Gwagwa and Garbe, 'Exporting Repression?'.

9 Kwasi Gyamfi Asiedu, 'Google Is Throwing Its Weight Behind Artificial Intelligence for Africa', *Quartz Africa,* 14 June 2018, https://qz.com/africa/1305211/google-is-making-abig-bet-on-artificial-intelligence-inafrica-with-its-first-research-center/. Of course, AI and other advanced technologies also have a downside for Africa. Many commentators, including Asiedu, have bemoaned a 'premature deindustrialization' to denote the industrial and factory employment that AI will put an end to – jobs that there were not enough of to begin with.

10 See Lindsey Andersen, 'Artificial Intelligence in International Development: Avoiding Ethical Pitfalls', *Journal of Public and International Affairs,* 20 May 2019, https://jpia.princeton.edu/news/artificial-intelligence-internationaldevelopment-avoiding-ethical-pitfalls.

11 See Andersen, 'Artificial Intelligence in International Development'; Asiedu, 'Google Is Throwing Its Weight Behind Artificial Intelligence'; and Eshan Gul, 'Is Artificial Intelligence the Frontier Solution to Global South's Wicked Development Challenges?', *Towards Data Science*, 5 July 2019, https://towardsdatascience.com/isartificial-intelligence-the-frontier-solution-to-global-souths-wicked-development-challenges-4206221a3c78.

12 See Andersen, 'Artificial Intelligence in International Development'. AI is not like a howitzer – most of the technology is dual-use, meaning it can be used for both good and evil ends. See Cook, 'Exporting Enslavement'.

13 Antoaneta Roussi, 'China Charts a Path Into European Science', *Nature*, 8 May 2019, p. 326, https://www-nature-com.uplib.idm.oclc.org/immersive/d41586-019-01126-5/index.html.

14 Thus far, 39 African countries and the African Union Commission have entered into BRI cooperation agreements, with others expected to follow suit. Antoaneta Roussi, 'China's Bridge to Africa', *Nature*, vol. 569, 16 May 2019, p. 325.

15 China funds one in five infrastructure projects on the continent. See Bates Gill, Chin-hao Huang and J. Stephen Morrison, 'Assessing China's Growing Influence in Africa', *China Security*, vol. 3, no. 3, Summer 2007, p. 9; and Barry Sautman and Yang Hairong, 'Friends and Interests: China's Distinctive Links with Africa', *African Studies Review*, vol. 50, no. 3, December 2007, p. 80.

16 See Gill, Huang and Morrison, 'Assessing China's Growing Influence in Africa', p. 6. For example, China hosted almost 62,000 African university and post-graduate students in 2016, and the Chinese government offered 8,470 scholarships to African students in 2015. Roussi, 'China's Bridge to Africa', p. 326.

17 Joshua Eisenman and Joshua Kurlantzick, 'China's Africa Strategy', *Current History*, vol. 105, no. 691, May 2006, p. 221.

18 See Michael Abramowitz and Michael Chertoff, 'The Global Threat of China's Digital Authoritarianism', *Washington Post*, 1 November 2018, 170 | Willem H. Gravett https://www.washingtonpost.com/opinions/the-global-threat-of-chinasdigital-authoritarianism/2018/11/01/46d6d99c-dd40-11e8-b3f0-62607289efee_story.html; and Adrian Shahbaz, 'Freedom on the Net 2018: The Rise of Digital Authoritarianism', Freedom House, October 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2018.

19 See Roussi, 'China's Bridge to Africa', p. 326.

20 See Hawkins, 'Beijing's Big Brother Tech Needs African Faces'.

21 David Ignatius, 'China Has a Plan to Rule the World', *Washington Post*, 29 November 2017, https://www.washingtonpost.com/opinions/china-has-a-plan-to-rule-theworld/2017/11/28/214299aa-d472-11e7-a986-d0a9770d9a3e_story.html.

22 See Lynsea Chutel, 'China Is Exporting Facial Recognition Software to Africa, Expanding Its Vast Database', *Quartz Africa*, 25 May 2018, https://qz.com/africa/1287675/china-is-exporting-facial-recognitionto-africa-ensuring-ai-dominancethrough-diversity/; and Hawkins, 'Beijing's Big Brother Tech Needs African Faces'.

23 Amy MacKinnon, 'For Africa, Chinese-built Internet Is Better than No Internet at All', *Foreign Policy*, 19 March 2019, https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-isbetter-than-no-internet-at-all/.

24 See Abramowitz and Chertoff 'The Global Threat of China's Digital Authoritarianism'.

25 Hawkins, 'Beijing's Big Brother Tech Needs African Faces'.

26 Shahbaz, 'Freedom on the Net 2018'.

27 See Hawkins, 'Beijing's Big Brother Tech Needs African Faces'; and Heidi Swart, 'Video Surveillance and Cybersecurity (Part Two): Chinese Cyber Espionage Is a Real Threat', *Daily Maverick*, 26 June 2019, https://www.dailymaverick.co.za/article/2019-06-26-video-surveillanceand-cybersecurity-part-two-chinesecyber-espionage-is-a-real-threat/.

28 See Shahbaz, 'Freedom on the Net 2018'.

29 Charles Rollet, 'In China's Far West, Companies Cash In on Surveillance Program that Targets Muslims', *Foreign Policy*, 13 June 2018, https://foreignpolicy.com/2018/06/13/in-chinas-far-west-companiescash-in-on-surveillance-programthat-targets-muslims/. In a leaked confidential investors prospectus, the company candidly acknowledged that '[our controlling shareholder] … is subject to the control of the People's Republic of China government … [and] will continue to be in a position to exert significant influence over our business'. Swart, 'Video Surveillance and Cybersecurity'.

30 *Ibid*.

31 It has been reported that Zhengfei may have been a 'high-ranking Chinese spymaster and indeed may still be'. Max Chafkin and Joshua Brustein, 'Why America Is So Scared of China's Largest Tech Company', *Bloomberg Businessweek*, 23 March 2018, https://www.bloomberg.com/news/features/2018-03-22/why-america-is-so-scared-of-china-sbiggest-tech-company.

32 ‘Sun Yafang, for example, chairwoman of Huawei from 1999 to 2018, was Digital Coloniser? China and Artificial Intelligence in Africa | 171 once employed in China’s ministry of state security.’ Steven Feldstein, ‘The Global Expansion of AI Surveillance’, Carnegie Endowment for International Peace, September 2019, p. 15, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

33 *Ibid*., p. 15.

34 According to Zhang Lin, ‘China’s large privately-owned firms are becoming more like state-owned enterprises, as many in recent years have implanted in their businesses cells of the Communist Party, the Communist Youth League and even discipline inspection committees.’ Zhang Lin, ‘Chinese Communist Party Needs to Curtail Its Presence in Private Business’, *South China Morning Post*, 25 November 2018, https://www.scmp.com/economy/china-economy/article/2174811/chinese-communist-party-needscurtail-its-presence-private.

35 Feldstein, ‘The Global Expansion of AI Surveillance’, p. 15.

36 See MacKinnon, ‘For Africa, Chinesebuilt Internet Is Better Than No Internet at All’.

37 See Scott N. Romaniuk and Tobias Burgers, ‘How China’s AI Technology Exports Are Seeding Surveillance Societies Globally’, *Diplomat*, 18 October 2018, https://thediplomat.com/2018/10/how-chinas-aitechnology-exports-are-seedingsurveillance-societies-globally/.

38 See Samuel Woodhams, ‘How China Exports Repression to Africa’, *Diplomat*, 23 February 2019, https://thediplomat.com/2019/02/how-chinaexports-repression-to-africa/.

39 See Abramowitz and Chertoff, ‘The Global Threat of China’s Digital Authoritarianism’.

40 See Romaniuk and Burgers, ‘How China’s AI Technology Exports Are Seeding Surveillance Societies Globally’.

41 Feldstein, ‘The Global Expansion of AI Surveillance’, p. 15.

42 Joe Parkinson, Nicholas Bariyo and Josh Chin, ‘Huawei Technicians Helped African Governments Spy on Political Opponents’, *Wall Street Journal*, 14 August 2019, https://www.wsj.com/articles/huawei-technicianshelped-african-governments-spy-onpolitical-opponents-11565793017.

43 Shahbaz, ‘Freedom on the Net 2018’. See also Duniah Tegegn, ‘African Union’s Revised Declaration on Principles of Access to Information and Freedom of Expression’, 13 December 2019, Amnesty International USA, https://medium.com/@amnestyusa/african-unions-revised-declaration-onprinciples-of-access-to-informationand-freedom-of-2d7d636dddb2; and Woodhams, ‘How China Exports Repression to Africa’.

44 ‘Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association’, UN General Assembly, Human Rights Council, 17 May 2019, p. 13, https://undocs.org/A/HRC/41/41.

45 David Pilling, ‘The Fight to Control Africa’s Digital Revolution’, *Financial Times*, 20 June 2019, https://www.ft.com/content/24b8b7b2-9272-11e9-aea1-2b1d33ac3271.

46 Only in Benin did protests result in a quick abandonment of the tax plan. 'Taxing Social 172 | Willem H. Gravett Media in Africa', Internet Health Report 2019, April 2019, https://internethealthreport.org/2019/taxing-social-media-in-africa/.

47 Writes Amy MacKinnon: 'There is leverage that comes with being the low-cost solution provider to a country whose political leadership, might, in part, derive their popular support from being able to offer connectivity to their population.' MacKinnon, 'For Africa, Chinese-built Internet Is Better Than No Internet at All'.

48 Qiang, 'The Road to Digital Unfreedom', p. 56.

49 See Simon Denyer, 'The All-seeing "Sharp Eyes" of China's Security State', *Washington Post*, 8 January 2018, https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharpend-of-a-drive-for-total-surveillance/.

50 See Feldstein, 'The Global Expansion of AI Surveillance', p. 18.

51 *Ibid*., p. 10.

52 Stephen Chen, 'China to Build Giant Facial Recognition Database to Identify any Citizen Within Three Seconds', *South China Morning Post*, 12 October 2017, https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognitiondatabase-identify-any.

53 See Richard Fontaine and Kara Frederick, 'The Autocrat's New Tool Kit: The Next Generation of Repressive Technology Will Make Past Efforts to Spread Propaganda and Quash Dissent Look Primitive', *Wall Street Journal*, 15 March 2019, https://www.wsj.com/articles/the-autocratsnew-tool-kit-11552662637?.

54 Denyer, 'The All-seeing "Sharp Eyes" of China's Security State'.

55 Quoted in *ibid*.

56 Fontaine and Frederick, 'The Autocrat's New Tool Kit'.

57 See Alina Polyakova and Chris Meserole, 'Exporting Digital Authoritarianism: The Russian and Chinese Models', Brookings Institution, August 2019, https://www.brookings.edu/research/exporting-digital-authoritarianism/.

58 See Charles Rollet, 'Western Academia Helps Build China's Automated Racism', *Coda*, 6 August 2019, https://codastory.com/authoritarian-tech/westernacademia-china-automated-racism/.

59 Denyer, 'The All-seeing "Sharp Eyes" of China's Security State'.

60 'Mongolia Installs 2,530 Surveillance Cameras in Capital', Xinhuanet, 18 June 2019, http://www.xinhuanet.com/english/2018-06/19/c_137264873.htm.

61 Rollet, 'Western Academia Helps Build China's Automated Racism'.

62 'China Has Turned Xinjiang Into a Police State Like No Other', *The Economist*, 31 May 2018, https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang-into-apolice-state-like-no-other.

63 Sarah Cook, ‘China’s Cyber Superpower Strategy: Implementation, Internet Freedom Implications, and U.S. Responses’, Freedom House, 28 September 2018, https://freedomhouse.org/article/chinas-cyber-superpower-strategyimplementation-internet-freedomimplications-and-us. Because the region is somewhat outside of the public eye, there can also be more experimentation in Xinjiang. See Digital Coloniser? China and Artificial Intelligence in Africa | 173 Megha Rajagopalan, ‘This Is What a 21st-century Police State Really Looks Like’, BuzzFeed News, 17 October 2017, https://www.buzzfeednews.com/article/meghara/the-police-stateof-the-future-is-already-here.

64 In its marketing materials, CloudWalk touted its surveillance systems’ ability to recognise ‘sensitive groups of people’. Paul Mozur, ‘One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority’, *New York Times,* 14 April 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificialintelligence-racial-profiling.html.

65 See Cook, ‘China’s Cyber Superpower Strategy’.

66 Rajagopalan, ‘This Is What a 21st-century Police State Really Looks Like’.

67 Mozur, ‘One Month, 500,000 Face Scans’.

68 See Cunrui Wang et al., ‘Facial Feature Discovery for Ethnicity Recognition’, *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery,* vol. 9, no. 11, January–February 2019.

69 See Rollet, ‘Western Academia Helps Build China’s Automated Racism’. There is substantial and well-founded scepticism about these capabilities. Promoters of some particularly controversial apps claim they can gauge intelligence or sexual orientation, even emotion. This seems highly questionable. Not all ethnicities have clearly distinct markers; some are largely cultural constructs.

70 See Charles Rollet, ‘In China’s Far West, Companies Cash In on Surveillance Program that Targets Muslims’, *Foreign Policy*, 13 June 2018, https://foreignpolicy.com/2018/06/13/in-chinas-far-west-companies-cashin-on-surveillance-program-thattargets-muslims/. The company has since removed the video making this claim. See Charles Rollet, ‘Hikvision Markets Uyghur Ethnicity Analytics, Now Covers Up’, IPVM, 11 November 2019, https://ipvm.com/reports/hikvision-uyghur.

71 Quoted in Mozur, ‘One Month, 500,000 Face Scans’.

72 ‘Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression’, UN General Assembly, Human Rights Council, 28 May 2019, p. 3, https://undocs.org/A/HRC/41/35. Specifically with regard to facial-recognition technology, the Special Rapporteur tellingly concluded: ‘Facial recognition technology seeks to capture and detect the facial characteristics of a person, potentially profiling individuals based on their ethnicity, race, national origin, gender and other characteristics, which are often the basis for unlawful discrimination … Perhaps no other environment demonstrates the comprehensive intrusiveness of these technologies better than China. Credible reporting suggests that the Government of China, using a combination of facial recognition technology and surveillance cameras throughout the country, looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review. Much of the technology deployed by the Government appears to be produced domestically, by both Stateowned and private enterprises’ (p. 5). 174 | Willem H. Gravett

73 See Abramowitz and Chertoff, ‘The Global Threat of China’s Digital Authoritarianism’.

74 This is a dramatic increase of the country's market share of 29.29% in 2017. See Chris Burt, 'Global Market for Facial Recognition Devices to Surpass $7 Billion by 2025, Led By CloudWalk', *Biometric Update*, 14 August 2018, https://www.biometricupdate.com/201808/global-market-for-facial-recognitiondevices-to-surpass-7-billion-by-2025-led-by-cloudwalk. The 'Global Face Recognition Device Market Research Report 2018', referred to in Burt's article, can be accessed at https://genmarketinsights.com/report/global-face-recognition-device-market-research-report-2018/41637/.

75 See Hawkins, 'Beijing's Big Brother Tech Needs African Faces'.

76 See Garikai Dzoma, 'Zimbabwe Government Is Sending Our Faces to China so China's Artificial Intelligence System Can See Black Faces', *TechZim*, 8 November 2018, https://www.techzim.co.zw/2018/11/zimbabwegovernment-is-sending-our-faces-tochina-so-chinas-artificial-intelligencesystem-can-learn-to-see-black-faces/; Hawkins, 'Beijing's Big Brother Tech Needs African Faces'; Zhang Hongpei, 'Chinese Facial ID Tech to Land in Africa', *Global Times*, 17 May 2018, https://www.globaltimes.cn/content/1102797.shtml; Romaniuk and Burgers, 'How China's AI Technology Exports Are Seeding Surveillance Societies Globally'; Roussi, 'China Charts a Path Into European Science', p. 326; Adrian Shahbaz, 'Fake News, Data Collection, and the Challenge to Democracy: Freedom on the Net 2018 – The Rise of Digital Authoritarianism', Freedom House, October 2018, https://freedomhouse.org/report/freedom-net/freedomnet-2018; and Samuel Woodhams, 'How China Exports Repression to Africa', *Diplomat*, 23 February 2019, https://thediplomat.com/2019/02/howchina-exports-repression-to-africa/.

77 See especially Hongpei, 'Chinese Facial ID Tech to Land in Africa'. See also Chutel, 'China Is Exporting Facial Recognition Software to Africa, Expanding Its Vast Database'; Ryan Gallagher, 'Export Laws', Index on Censorship, 12 September 2019, https://journals-sagepub-com.uplib.idm.oclc.org/doi/10.1177/0306422019876445; and Hanibal Goitom, 'Regulation of Artificial Intelligence: Sub-Saharan Africa', Library of Congress, January 2019, https://www.loc.gov/law/help/artificial-intelligence/africa.php.

78 See Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research Conference on Fairness, Accountability and Transparency*, vol. 81, 2018, pp. 6–12, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

79 See Hawkins, 'Beijing's Big Brother Tech Needs African Faces'.

80 See Kari Paul, 'Amazon to Ban Police Use of Facial Recognition Software for a Year', *Guardian*, 11 June 2020, https://www.theguardian.com/technology/2020/jun/10/amazon-rekognition-softwarepolice-black-lives-matter. See also Shita Ovide, 'A Case for Banning Digital Coloniser? China and Artificial Intelligence in Africa | 175 Facial Recognition', *New York Times*, 9 June 2020, https://www.nytimes.com/2020/06/09/technology/facialrecognition-software.html.

81 See Shahbaz, 'Fake News, Data Collection, and the Challenge to Democracy'; and Woodhams, 'How China Exports Repression to Africa'.

82 See Hawkins, 'Beijing's Big Brother Tech Needs African Faces'.commenting on the Zimbabwe agreement, Yao Zhiqiang, the chief executive officer of CloudWalk, stated: 'The difference between technologies tailored to an Asian face and those to a black one are relatively large, not only in terms of color, but also facial bones and features … The machine learning needed to expand the technology's capability would require sufficient data.' Quoted in Hongpei, 'Chinese Facial ID Tech to Land in Africa'.

83 The deal included dozens of cooperation agreements between Harare and Chinese technology and biotechnology firms. Yao Zhiqiang confirmed to China's *Global Times* that the 'Zimbabwean government did not come to Guanzhou purely for AI or facial ID technology, rather it had a comprehensive plan for such areas as infrastructure, technology and biology'. Quoted in Hongpei, 'Chinese Facial ID Tech to Land in Africa'. China has historically been a close partner of Zimbabwe, and remains the single biggest investor in the country's beleaguered economy, having sunk billions of dollars into diamond and platinum mines, new highways and electricity-generating dams. See Ray Mwareya, 'Zimbabwe Drifts Towards Online Darkness', *Coda*, 26 February 2019, https://www.codastory.com/authoritarian-tech/zimbabwe-driftstowards-online-darkness/.

84 See Chutel, 'China Is Exporting Facial Recognition Software to Africa, Expanding Its Vast Database'.

85 See Chris White, 'Chinese Companies Using Zimbabweans as Guinea Pigs to Identify Black Faces', *National Interest*, 3 December 2019, https://nationalinterest.org/blog/buzz/chinese-companies-use-zimbabweansguinea-pigs-identify-black-facesreport-101447.

86 Hawkins, 'Beijing's Big Brother Tech Needs African Faces'.

87 See Romaniuk and Burgers, 'How China's AI Technology Exports Are Seeding Surveillance Societies Globally'.

88 Quoted in Hawkins, 'Beijing's Big Brother Tech Needs African Faces'.

89 Abeba Birhane, 'The Algorithmic Colonization of Africa', *Real Life*, 18 July 2019, https://reallifemag.com/the-algorithmic-colonization-of-africa/.

90 See Gwagwa and Garbe, 'Exporting Repression?'.

91 Fontaine and Frederick comment: 'A political dissident in Harare may soon have as much to fear as a heroin smuggler in Zhengzhou.' Fontaine and Frederick, 'The Autocrat's New Tool Kit'. See also Ryan Khurana, 'The Rise of Illiberal Artificial Intelligence', *National Review*, 10 August 2018, https://www.nationalreview.com/2018/08/china-artificial-intelligence-race/; and Romaniuk and Burgers, 'How China's AI Technology Exports Are Seeding Surveillance Societies Globally'.

92 Frederike Kaltheuner, 'Facial 176 | Willem H. Gravett Recognition Cameras Will Put Us All in an Identity Parade', *Guardian*, 27 January 2020, https://www.theguardian.com/commentisfree/2020/jan/27/facial-recognition-camerastechnology-police.

93 See Woodhams, 'How China Exports Repression to Africa'.

94 Dzoma, 'Zimbabwe Government Is Sending Our Faces to China so China's Artificial Intelligence System Can See Black Faces'.

95 See Kaltheuner, 'Facial Recognition Cameras Will Put Us All in an Identity Parade'.

96 Hawkins, 'Beijing's Big Brother Tech Needs African Faces'.

97 Romaniuk and Burgers, 'How China's AI Technology Exports Are Seeding Surveillance Societies Globally'.

98 Hawkins, 'Beijing's Big Brother Tech Needs African Faces'.

99 See Mwareya, ‘Zimbabwe Drifts Towards Online Darkness’.

100 Partial internet service was restored in February 2019, but social-media apps and communications services such as Facebook, WhatsApp and Twitter remained blocked for days longer.

101 Of the 55 member states of the African Union, the signatories to the convention are: Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Mozambique, Rwanda, São Tomé and Príncipe, Sierra Leone, Togo, Tunisia and Zambia. However, only Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda and Senegal have ratified or acceded to the convention. See ‘List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cybersecurity and Personal Data Protection’, African Union, 18 June 2020, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.

102 ‘African Union Convention on Cybersecurity and Personal Data Protection’, Chapter II, Section 3, Article 13(1) of the Convention.

103 *Ibid*., Chapter II, Section 3, Article 14(1).

104 *Ibid*., Chapter II, Section 3, Article 14(6)(a). The prohibition is not applicable where, before any personal data is transferred to the third country, the data controller requests authorisation for such transfer from the national protection authority. Chapter II, Section 3, Article 14(6)(b).

105 *Ibid*., Chapter II, Section 3, Article 18.

106 The declaration was adopted by the African Commission on Human and Peoples’ Rights at its 65th ordinary session, held from 21 October to 10 November 2019 in Banjul, Gambia, and replaces its 2002 ‘Declaration of Principles on Freedom of Expression in Africa’. The declaration is a ‘soft law’ instrument that interprets Article 9 (right to receive information and free expression) of the African Charter on Human and Peoples’ Rights. For the text, see African Commission on Human and Peoples’ Rights, ‘Declaration of Principles on Freedom of Expression and Access to Information in Africa’, https://www.achpr.org/presspublic/publication?id=80.

107 See Principles 40–2 of the ‘Declaration of Principles on Freedom of Digital Coloniser? China and Artificial Intelligence in Africa | 177 Expression and Access to Information in Africa’.

108 *Ibid*., Principle 40(1) and (2).

109 *Ibid*., Principle 42(2).

110 *Ibid*., Principle 42(4).

111 See Lindsey Andersen et al., ‘Human Rights in the Age of Artificial Intelligence’, Access Now, November 2018, p. 29, https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf.

112 See Shahbaz, ‘Fake News, Data Collection, and the Challenge to Democracy’.

113 See ‘Léifēng wǎng lùn dào AI ānquán yǔ lúnlǐ: Wǒmen néng dádào diànyǐng lǐ de zhìnéng ma? Zuì kěnéng shíxiàn de AI chǎngjǐng shì shénme? Rúhé kàndài AI zìzhǔ xìng?’ [On AI safety and ethics: what is the most likely AI scenario? How to view AI autonomy?], Phoenix Network

Technology, 3 June 2019, https://web.archive.org/web/20190628115141/http:/tech.ifeng.com/a/20190603/45601943_0.shtml.

114 See Andersen et al., 'Human Rights in the Age of Artificial Intelligence', p. 31; and Kaltheuner, 'Facial Recognition Cameras Will Put Us All in an Identity Parade'.

115 See Dylan Curran, 'Facial Recognition Will Soon Be Everywhere. Are We Prepared?', *Guardian*, 27 May 2019, https://www.theguardian.com/commentisfree/2019/may/21/facialrecognition-privacy-prepared-regulation.

116 See Birhane, 'The Algorithmic Colonization of Africa'.

117 See Gwagwa and Garbe, 'Exporting Repression?'.