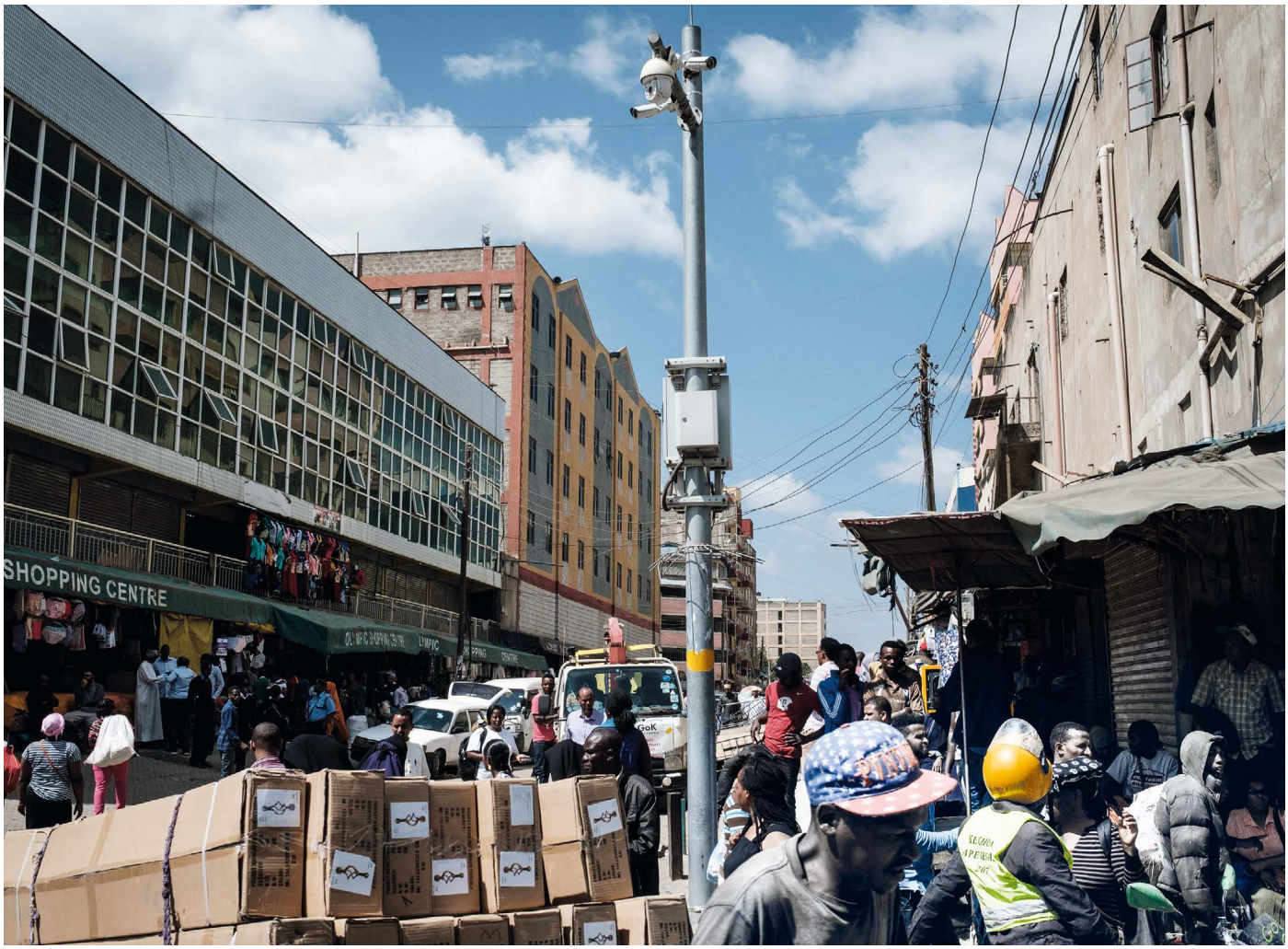
Comment



YASUYOSHI CHIBA/AFP VIA GETTY

Authorities in Nairobi have installed digital surveillance cameras as part of Kenya's smart-city initiatives.

Africa: regulate surveillance technologies and personal data

Bulelani Jili

CCTV cameras and spyware are proliferating in the continent without checks and balances. Governments must legislate locally to prevent civil-rights abuses.

Outside Kenya's Jomo Kenyatta International Airport in Nairobi, I ask a taxi driver to take me downtown.

Noting my American accent, he asks me what I'm doing there. "Researching Kenya's smart-city initiatives," I reply. Nairobi is changing fast, he says, pointing out digital cameras that have appeared on street corners, shopping centres and office blocks.

I ask him if he worries about the cameras. After a pause, he replies: "Corruption is a problem, but they are here for security."

Although this is true, the story of the spread of surveillance technologies through Africa is more complex, as it is elsewhere.

For more than a decade, African governments have installed thousands of closed-circuit television (CCTV) cameras and surveillance devices across cities, along with artificial-intelligence (AI) systems for facial recognition and other

uses. Such technologies are often part of state-led initiatives to reduce crime rates and strengthen national security against terrorism. For instance, in Uganda in 2019, Kampala's police force procured digital cameras and facial-recognition technology worth US$126 million to help it address a rise in homicides and kidnappings (see go.nature.com/3nx2tfk).

However, digital surveillance tools also raise privacy concerns. Citizens, academics and activists in Kampala contend that these tools, if linked to malicious spyware and malware programs, could be used to track and target citizens. In August 2019, an investigation by *The Wall Street Journal* found that Ugandan intelligence officials had used spyware to penetrate encrypted communications from the political opposition leader Bobi Wine[1].

Around half of African countries have laws on data protection[2]. But these are often outdated and lack clear enforcement mechanisms and strategies for secure handling of biometric data, including face, fingerprint and voice records. Inspections, safeguards and other standards for monitoring goods and services that use information and communications technology (ICT) are necessary to address cybersecurity and privacy risks.

The African Union has begun efforts to create a continent-wide legislative framework on this topic. As of March this year, only 13 of the 55 member states have ratified its 2014 Convention on Cyber Security and Personal Data Protection; 15 countries must do so before it can take effect[3]. Whereas nations grappling with food insecurity, conflict and inequality might not view cybersecurity as a priority, some, such as Ghana, are keen to address this vulnerability so that they can expand their information societies.

The risks of using surveillance technologies in places with inadequate laws are great, however, particularly in a region with established problems at the intersections of inequality, crime, governance, race, corruption and policing. Without robust checks and balances, I contend, such tools could encourage political repression, particularly in countries with a history of human-rights violations.

Here, I outline the spread of surveillance technologies in Africa and highlight problems. I focus on Kenya and Ethiopia, because these nations have pursued distinct digitization strategies for development purposes. I call on African governments to adopt the latest data-protection policies. Researchers also need to improve their understanding of how local and global factors play into each other, and how local contexts determine practical and political outcomes.

Smarter cities

ICT systems have been deployed in Africa since the 2000s, largely on the back of billion-dollar investments to expand Internet and mobile-phone networks. Governments see their widening use as a means to deliver better health care, employment, security and education, as well as improve economic development. For example, Ethiopia's WoredaNet project aims to improve digital connections and communication between local, regional and federal governments to boost public-sector services. Companies are attracted to the continent by the high demand for digital infrastructure; it also has fewer barriers to entry and less regulation than do the United States or Europe.

"A clear plan needs to be developed that emphasizes secure data infrastructures."

In particular, Chinese state and private technology investments have grown in African ICT markets. Loans from Chinese state banks hold appeal because they come with relatively few conditions. For example, the largest telecommunications agreement in the continent's history was signed in 2006 between the Ethiopian Telecommunication Corporation and Chinese telecoms giant ZTE. Backed by the China Development Bank, ZTE offered a loan of $1.5 billion to install thousands of kilometres of fibre-optic cable to connect Ethiopia's 13 largest cities. Another Chinese company, Huawei, partnered with ZTE in 2011, jointly winning a separate tender bolstered by $1.6 billion in loans from the Export–Import Bank of China (EXIM)[4].

The Kenyan government also contracted Huawei and ZTE to install fibre-optic cables with financing from EXIM. Sagem, a French company, worked with the two Chinese firms to create Kenya's first National Optic Fibre Backbone Infrastructure, which brought high-speed connectivity to Nairobi in 2009 (ref. 5).

Surveillance technologies were bolted on to broader smart-city initiatives in Kenya and elsewhere on the continent. These ICT systems include fibre-optic cables, digital cameras and biometric devices, which are connected and used with AI products to gather information about energy, water and traffic to improve public services. For example, Kenya's Konza City – Africa's first planned smart city – was launched in 2008 on the site of a former cattle range 60 kilometres outside Nairobi. The project has experienced delays, but aims to host the Konza National Data Centre, a smart ICT network, public-safety projects and intelligent transport.

Initiatives for safe cities rely on biometric and surveillance data to support responses to critical incidents and to enable predictive policing (the use of algorithms and past crime data to focus police activity on areas predicted to be most likely to suffer crimes). Nairobi launched the first such initiative in Africa in 2014. Around 1,800 high-definition cameras and 200 traffic surveillance devices have been installed along roads and across the city. The network feeds into a national police command centre that supports more than 9,000 police officers and 195 police stations[6].

The impact of surveillance technologies on crime rates is hard to assess, however. Statistics and claims from companies, the police, cities and governments officials often differ, along with motivations for reporting them. Scholars also find it difficult to gain access to these data.

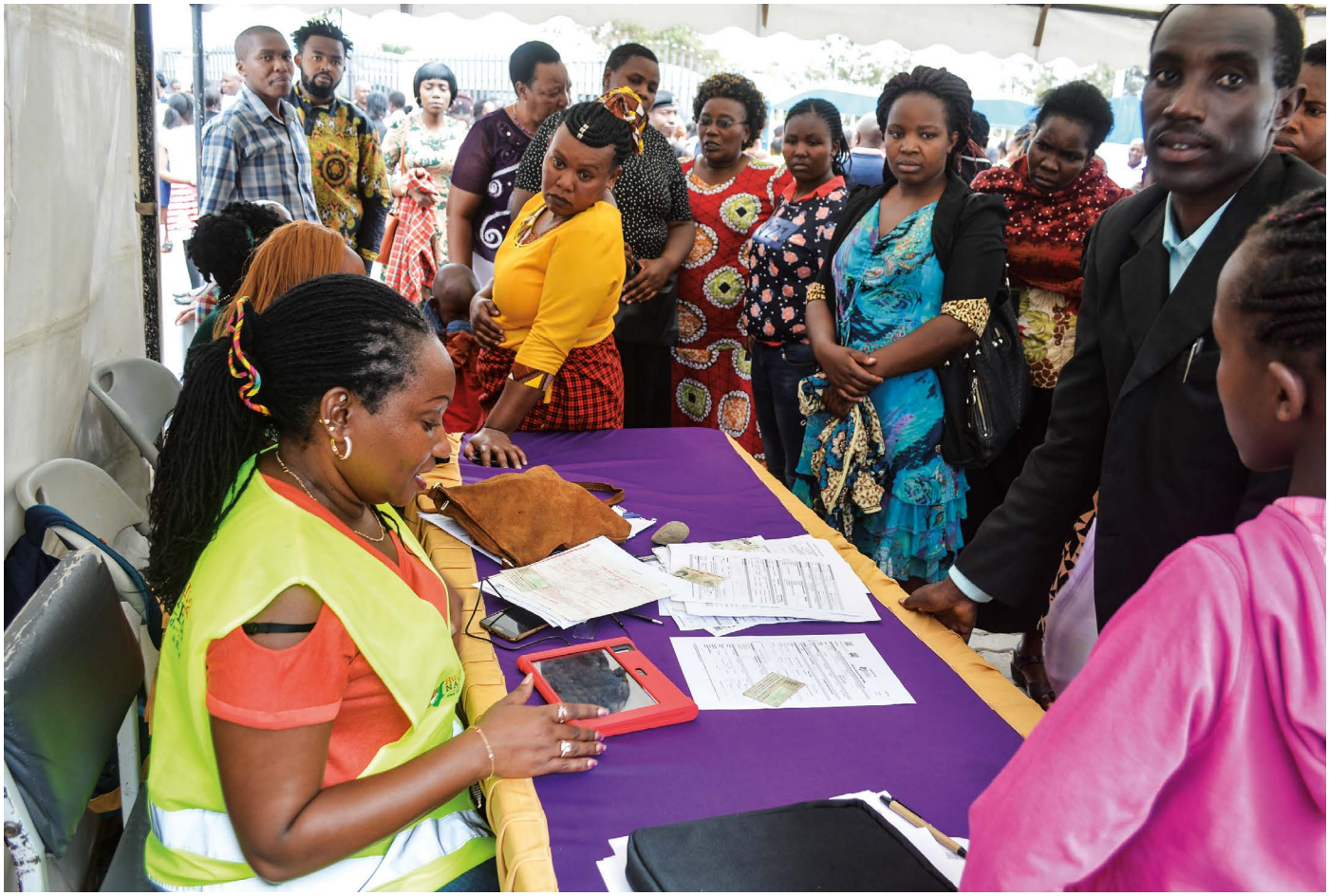
Personal data boon

Electronic government initiatives have widened the range of personal data collected. In 2011, the Kenyan government hired a French firm, Imprimerie Nationale, to establish a biometric data system for national identity cards. Kenya justified this mass registration of its citizens as a way to recover taxes and strengthen national security and policing, especially after the Islamist militant attack on Nairobi's Westgate shopping mall in 2013. Development of the system stalled, however, owing to disagreements between banks and telecoms firms over which data to collect.

In 2019, the government announced an even more ambitious scheme: the National Integrated Identity Management System (NIIMS), also known as *Huduma Namba* (Swahili for 'service number'). This national database contains information on all Kenyan citizens and foreign residents. The Huduma Card consolidates an individual's passport, driver's licence, social-security card, national identification and national insurance card into one credential. It would become paramount for accessing public services and benefits, including voting.

With the fingerprints and facial photographs of almost 40 million Kenyans collected, this, too, has stalled. In January 2020, Kenya's High Court ruled that the initiative should be halted because there was no legislation in place to guarantee the security and safety of biometric data, and because it contains no steps to ensure the system does not deprive groups of essential services. The court ordered the Kenyan government to conduct a data-protection impact assessment. The government has appealed that decision, calling for a more explicit outline of what a robust regulatory framework would look like.

Kenya has had a Data Protection Act since 2019, which aims to manage and protect data once they are acquired, processed and stored[7]. The country's constitution sees privacy as a fundamental right. As it stands, there are no clear regulations as to how Kenya's biometric databases or facial-recognition technologies will be used, or how the data will be vetted.



JAMES WAKIBIA/SOPA IMAGES/LIGHTROCKET VIA GETTY

People in Nakuru, Kenya, wait to be registered for the country's identity-management database, called *Huduma Namba*.

There are no means to audit the algorithms that empower facial-recognition technology. In November 2020, the government appointed a Data Protection Commissioner as a regulatory office to realize the ambitions of the Data Protection Act. But because the role falls under the ICT ministry, the public might lack trust in its capacity to hold the government accountable.

Accordingly, a clear plan needs to be developed that emphasizes secure data infrastructures that include data grading, auditing, access control and privacy protection; this must then be deployed and regularly updated.

Hybrid systems

Adding to this challenging landscape, the surveillance networks being established in Africa are hybrids – they are complex and diversely sourced. They involve many countries and international and domestic companies. For example, the facial-recognition technologies used at most of Kenya's borders are powered by SenseTime, which is based in Hong Kong. Yet those at Moi International Airport in Mombasa are supplied by NEC, based in Japan.

Vumacam, a South African company, is building nationwide CCTV networks in that country. With about 5,000 cameras in Johannesburg, it has partnered with the Chinese firm Hikvision and the Swedish company Axis Communications to supply the hardware; Milestone, a Danish company, has provided the software[8].

CloudWalk Technology, an AI start-up firm in Guangzhou, China, is helping the Zimbabwean government to build a facial-recognition surveillance system. By gaining access to the population's biometric data, the company aims to train its algorithm to become better at identifying people of African descent. Such improvements are needed – extensive research shows a clear bias in automated facial-analysis algorithms and data sets in regard to race and gender (see, for example, ref. 9). Yet concerns remain over state accountability. Public safeguards are needed against potential misuse of these data by the government. Scholars need to consider the competitive advantage the company gains by doing such work in Zimbabwe. More broadly, researchers need to assess whether African markets are operating as a kind of laboratory for improving the quality of surveillance technologies.

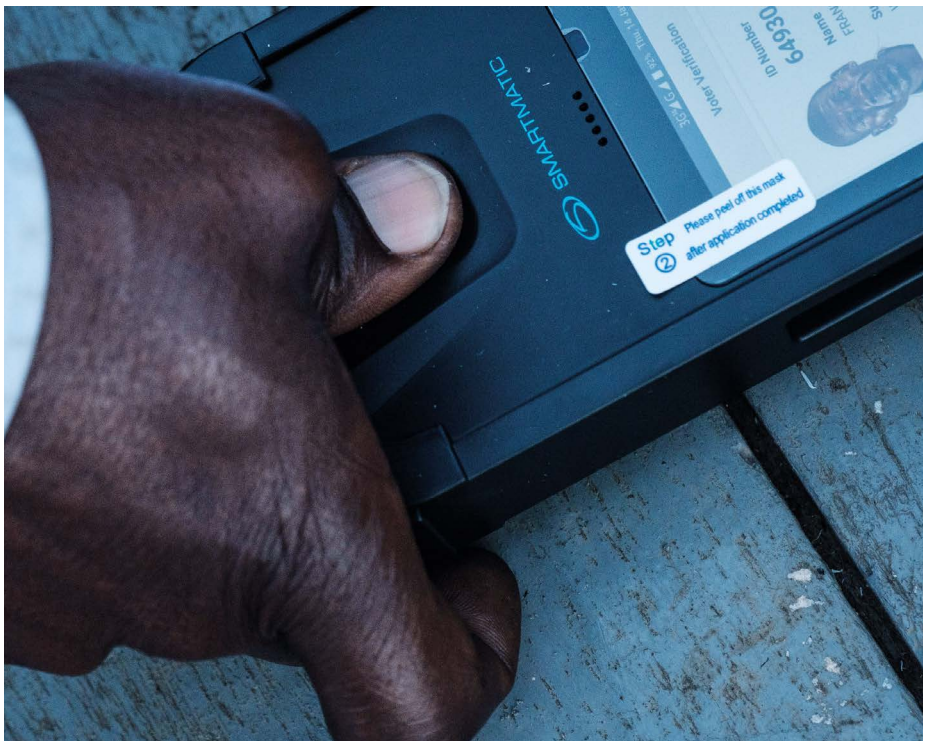
Spyware adds another dimension. The Citizen Lab, a research centre at the University of Toronto, Canada, that studies digital threats to civil society, has highlighted Ethiopia's aptitude for patching together digital infrastructure and surveillance technology (see go.nature.com/3awpsgn). The state has bought systems of the kind that can access files on targeted laptops, log keystrokes and passwords, and turn on webcams and microphones by stealth. Many commercial operators supply such tools, including UK- and Germany-based Gamma International; Cyberbit, an Israel-based cybersecurity enterprise; and Hacking Team, a supplier of remote control systems in Milan, Italy.

The fact that countries possess spyware does not mean they will necessarily surveil invasively. But the means are now widely available, and there's little legal oversight.

Loopholes persist. For example, according to documents provided by US whistle-blower Edward Snowden, the US National Security Agency has cooperated with the Ethiopian government to establish a clandestine surveillance outpost in Ethiopia. This is in part because Ethiopia was considered a suitable location for surveilling Somalia, Sudan and Yemen (see go.nature.com/3pjzxav). Kenya has shared intercepted telecommunications with the United States to track terror suspects[10].

Local contexts

Such complexities and obscurations make it hard for researchers to study the spread of surveillance technology in Africa.



In Uganda, voters in elections confirm their identities using a biometric thumbprint reader.

YASUYOSHI CHIBA/AFP VIA GETTY

African authorities, and the many other states, companies and banks they partner with, often limit access to documents and statistical data to preserve their interests. There's also little awareness or understanding among decision-makers and the public of the growing risks, and thus little pressure to address them. In my view, it is not enough to simply discredit the technologies. Instead, critics should acknowledge the risks involved and the need for the collection, deployment and storage of data to be regulated.

Accordingly, researchers need to understand how resources and relations are leveraged to establish surveillance infrastructure and practices. How do these ambitions further public interests? What kind of political, social and legal environments are these tools embedded in? How exactly are cameras, algorithms and biometrics being used? Given the diversity of African governments, answers might be needed for individual countries or cities.

In my opinion, researchers should also widen their scholarly gaze beyond arguments that the Chinese government is driving the proliferation of AI surveillance technology, and thereby the rise of digital authoritarianism in Africa. China's active push needs examining. But local agency and context must also be acknowledged; after all, these systems are being installed at the request of African governments[11]. As Kenya and Ethiopia show, many corporate entities and states are complicit in these emerging development initiatives and cybersecurity threats. Researchers need to ask how local and geopolitical factors play into each other, and how they influence practical political outcomes.

They should also question the supposed link between digital surveillance technologies and crime reduction or sustained economic growth. Currently, there's no robust evidence to support this. Smart-city initiatives need to be viewed as complex assemblages — social, economic, political and technical — that are also entangled in local contexts. Technology alone cannot resolve deep structural problems.

Next steps

On the national level, until governments improve regulation, state officials and researchers should take the following steps.

First, carry out impact assessments on the consequences of these technologies, as Kenya's High Court has proposed. Identify risks and offer mitigating measures to ameliorate concerns.

"For robust data protections to be enforceable, African states need the technical capacities to execute them."

Second, skilled and experienced personnel are needed to staff data commissioner offices. For robust data protections to be enforceable, African states need the technical capacities to execute them. Emphasis must be placed on building cybersecurity capacity among all stakeholders and at all levels. This is a daunting task, but identifying current risks is a good starting point.

Third, develop strategy around cooperation and co-regulation between the state and private enterprises to establish good practices. Public–private partnership is a model that engages industry, government, civil society and academia in the promotion and enhancement of cybersecurity. Such collaborations will also help with capacity-building by leveraging resources.

Fourth, local legislators and digital-rights advocacy groups should set up intergovernmental advisory panels to lay out recommendations for strategies and best practices surrounding governance and surveillance technology. A shared approach will engender trust.

At the regional level, more nations should join and ratify the African Union Convention on Cyber Security and Personal Data Protection. Member states should assess themselves against the requirements of the convention to establish their vulnerabilities and the reforms needed to improve cybersecurity.

To advance legal safeguards and maintain best practices, what's needed are advisory panels, training and conferences, along with the collaboration of digital advocacy groups, policymakers, security professionals and ordinary citizens. Such collective action will accelerate the learning curve, devise policy solutions that are relevant to varied African contexts and ensure a balance between freedom and the demands of digital development.

The author

Bulelani Jili is a Meta Research PhD fellow at Harvard University, Cambridge, Massachusetts; and a visiting fellow at Yale Law School,New Haven, Connecticut, USA.
e-mail: bulelanijili@g.harvard.edu

1. Parkinson J., Bariyo, N. & Chin, J. *The Wall Street Journal* (15 August 2019).
2. Collaboration on International ICT Policy in East and Southern Africa. *Mapping and Analysis of Privacy Laws in Africa* (CIPESA, 2021).
3. African Union. *African Union Convention on Cyber Security and Personal Data Protection* (AU, 2014).
4. Thakur, M. *Building on Progress? Chinese Engagement in Ethiopia*. South African Institute of International Affairs Occasional Paper No. 38 (SAIIA, 2009).
5. Republic of Kenya Ministry of Information, Communications and Technology. *National Broadband Strategy 2018–2023 Interim Report* (Government of Kenya, 2018).
6. Feldstein, S. *Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Strategic Aims in Africa* (U.S.-China Economic and Security Review Commission, 2020).
7. Republic of Kenya. *The Data Protection Act, 2019.* Kenya Gazette Suppl. 181 (Acts No. 24) (Government of Kenya, 2019).
8. Hao, K. & Swart, H. *MIT Technol. Rev.* (19 April 2022).
9. Kleinberg, J., Ludwig, J., Mullainathan, S. & Sunstein, C. R. *J. Leg. Anal.* **10**, 113–174 (2018).
10. Al-Bulushi, S. *Secur. Dialogue* **52** (Suppl.), 115–123 (2021).
11. Jili, B. *Chinese Surveillance Tools in Africa. Research Brief No. 8/2019* (China, Law and Development Project, 2020).

The author declares no competing interests.