enact
Enhancing Africa's response to transnational organised crime

This project is funded by the European Union

Issue 17 | November 2020

RESEARCH PAPER

Who's watching who?

Biometric surveillance in Kenya and South Africa

Karen Allen and Isel van Zyl

Summary

Biometric data is used to help confirm identity, and in time may be able to predict an individual's actions. It is crucial that this data is protected against function creep and other forms of misuse. This paper maps the use of biometric technology in sub-Saharan Africa by focusing on Kenya and South Africa as case studies. While there are clear advantages (e.g. reducing data theft and fraud, and accelerating economic development through data efficiencies), potential harms are associated with the networked gathering and storage of biometric data – this includes the misuse by criminal groups for financial gain.

Key findings

- The potential for countries such as South Africa and Kenya to become surveillance states, for the moment appears to be limited by resource constraints and government capacity.
- The key drivers of biometric surveillance are governments, international organisations such as the World Bank, and the private sector (including banking and security industries).
- Sub-Saharan Africa could become the testing ground for emerging biometric technologies, with China and the US leading the way in piloting such technologies and offering them on a trial or discounted basis. This is arguably part of a geopolitical strategy to develop surveillance norms.
- Regional initiatives such as the cyber security expert group of the African Union (AU) should ensure that emerging biometric technologies and their potential benefits and harms are regularly reviewed.

- Regulating the biometrics space is an urgent priority. Data protection legislation in Kenya and South Africa aims to protect data once it is acquired, processed and stored. However, there are currently no regulations on how, for instance, centralised government biometric databases such as South Africa's proposed Automated Biometric Information System (ABIS) will be policed. The information regulator in South Africa confirms that overseeing the use of facial recognition technology, as well as other forms of biometrics, is part of its terms of reference under the Protection of Personal Information (POPI) Act 2013. However, how the legislation is to be enforced and the necessary skills developed among e.g. the police and prosecutors are ongoing issues.
- There are no regulations or minimum standards for the CCTV industry in South Africa and Kenya. There also appears to be no systems in place for auditing the algorithms used for e.g facial recognition purposes.
- Biometric technology is highly vulnerable to function creep. This could violate international principles of process limitation embodied in legislation in Kenya and South Africa. Privacy International has cited the Aadhaar centralised biometric data system in India as an example of function creep. The use of facial recognition technology to profile demonstrators during anti-racism protests in the United States (US) is another example of function creep. This has led to a number of tech providers temporarily withdrawing their products pending new regulations.
- Data surveillance and biometrics represent a paradigm shift in that the supply and use of the technology is dominated by the private sector rather than the state.

Introduction: Why is there a debate?

The discussion about potential abuses of biometric technology is especially sensitive given the highly personal nature of the data being collected and stored and the far-reaching consequences of potential data breaches.

Biometric data includes unique physiological and behavioural characteristics of individuals based on face, iris, voice, fingerprint and DNA markers.[1] These help to confirm identity, and in time, may be able to predict actions and reactions based on someone's gait and facial expression.

The use of biometrics for micro marketing, or verifying voter identity during elections, or monitoring border movements, is widely discussed in public media. There is also a growing body of literature examining the biometric surveillance culture of both states and private actors:

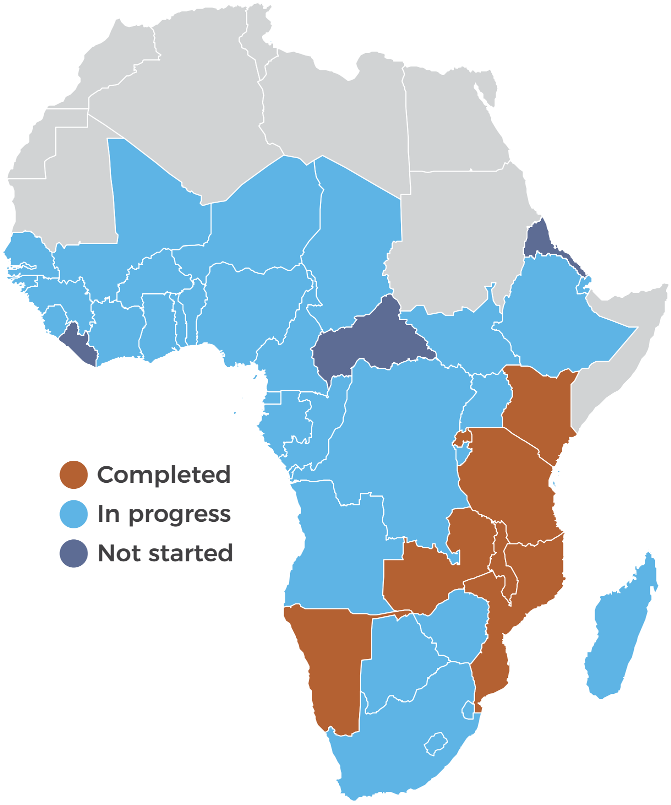
> "Many of our activities online and, increasingly, offline, generate data – geo-location data when we walk around with our mobile phone; metadata of our online communication; data on our likes and preferences; data on our movements and activities in 'smart cities' and 'smart homes' that are increasingly filled with sensors. This data is collected, stored, monitored, shared, and sold by social media services, other online platforms, data brokers, intelligence agencies, and public administration".[2]

This paper limits its scope to mapping the use of biometrics and public space surveillance through the use of closed-circuit television (CCTV) cameras and artificial intelligence (AI) assisted biometric technologies – including facial recognition technology – in Kenya and South Africa.

It also charts the development of national databases for the purposes of centralising biometric data, in order to enhance, limit or deny access to services.

Kenya and South Africa have been selected for close study as they both have energetic tech sectors, and are witnessing a rapid expansion of Internet and mobile phone use. Mobile subscriptions reached 54.5 million in Kenya in 2019 and 96.9 million in South Africa, according to the World Bank.[3]

Figure 1: **Status of analog-to-digital switchover in sub-Saharan Africa as of June 2018**



Source: GSMA Intelligence

Since other countries, including Nigeria and Ghana, are also seeing greater use of biometric technologies this study is by no means exhaustive, but it is meant to be indicative of a broader trend.[4]

Framework of this study

This paper firstly gives the context in which biometric surveillance is being introduced in Africa through a close focus on Kenya and South Africa. It highlights the debate on and tension between privacy and security in the technology space. The paper then examines the use of surveillance and verification tools by the private and public sectors, including banks, government departments and law enforcement.

It also aims to address the risks and benefits associated with biometric technologies and explore the existing legal frameworks and governance issues. It concludes by summarising various findings or observations to inform future discussions.

Emerging biometric tools are briefly located within a wider context of surveillance technologies, in order to understand some of the concerns and sensitivities raised by civil society. Fears about data privacy have been articulated in response to more traditional surveillance technologies, including mobile phone intercepts and wire-tapping.[5]

There are similar privacy concerns in the biometric field, as well as additional threats such as algorithmic bias, data theft, identity theft or denial of access, and other cybersecurity breaches. In addition, new surveillance technologies have the potential for function creep, whereby the technology is deployed for a purpose other than the originally intended one.

This paper draws on local and international experience in order to flag potential areas for future policy discussion. It highlights the paradigm shift represented by the trend where private sector operators, rather than state providers, now dominate the biometric surveillance market. This is in marked contrast to many of the more traditional forms of surveillance, where the state still has a monopoly on use.

Methodology

The research was conducted through a literature review on the status of biometric surveillance globally. It also included a review of other academic publications, industry reports, government documents and media reports. Given that biometric surveillance is still an emerging area of innovation, it has relied heavily on primary sources, in particular interviews held with academics, members of the security service and the South African Police Service (SAPS), industry experts, civil society organisations, journalists, private sector providers, regulators and representatives of government and local government.

Limitations

The research was constrained by notable absences in contributions. The Kenyan government declined to participate in this research, despite several invitations to do so via the police service and Department of Home Affairs. In South Africa repeated approaches were made to the Department of Home Affairs to discuss current and future plans for the use of biometric technology. However, senior staff indicated they were unavailable to contribute to the research or comment on some of the observations in this paper.

Biometric technology: definitions and context

Biometric technologies have evolved through the desire of governments and commercial actors such as banks to capture personal data, in order to verify and authenticate identification documents. Today biometrics includes face, voice, iris, fingerprint and DNA-based technologies. They are used in border security and government databases, among others.

In South Africa the Home Affairs National Identification System Project (HANIS), a fingerprint-based identification system, has been in place since 1996. It is due to be replaced with a centralised biometric system – the Automated Biometric Information System (ABIS) – in the next two to three years.[6]

> Today biometrics includes face, voice, iris, fingerprint and DNA-based technologies

Similarly, Kenyan airports have used facial and fingerprint technology since 2019 as part of a Japanese-funded project.[7]

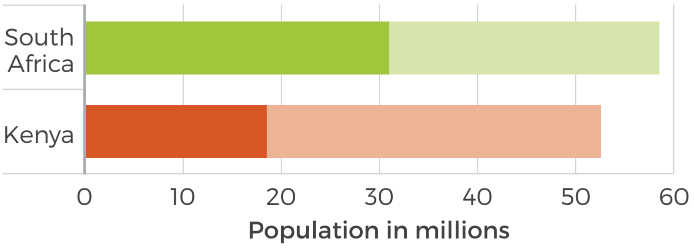
Advances in storage, software and data capturing capacity have helped to drive the spiralling demand for centralised biometric systems. This has been accelerated by the private security industry, international institutions such as the World Bank, governments and the financial services sector.

In many respects it is a response to lived experiences of high crime rates, terrorism and corruption.[8] It is also driven by the desire by governments to fulfil their human rights obligations to ensure citizens have a legal identity, consistent with UN Sustainable Development Goal (SDG) 16.9.[9]

The rapid growth of the mobile phone market has created a powerful platform on which to build biometric technologies.[10] More than half of all South Africans and a third of all Kenyans own a smartphone. On the rest of the continent the number of smartphone owners is more 'modest' but growing.[11]

As password security is rapidly overtaken by biometric identifiers, many banks in South Africa and Kenya now rely on self-verification and authentication for proof of identity.[12] This involves an individual taking a photograph of themselves on their smartphone and submitting it for initial verification and subsequent authentication, against, for instance, another form of photo ID. This is known as 'one-to-one' verification/authentication.

Figure 2: Smartphone adoption in Kenya and South Africa



Source: L Silver and C Johnson

Facial recognition relies on an image being matched against a database of other images and is often referred to as 'one to many'.

Face-based biometrics has got a lot of public attention, in part because of its perceived intrusive nature. Yet such technology is becoming a preferred method of identification, as it is considered harder to fake for technical reasons.

Vast amounts of personal data are needed to develop these technologies. In addition to centralised biometric databases, personal data may also be acquired through the use of surveillance cameras in public spaces. These can collect data without the explicit consent of the individual being filmed.

Surveillance cameras are increasingly applying AI capabilities. This allows them to 'learn' behaviours to determine what is 'normal' and what is not, without the intervention of human beings. As a result vast amounts of additional data, upon which important decisions may be based, are being generated by machines.

Yet there are factors that limit how accurately data can be acquired by surveillance cameras. The capturing of face-based data is highly sensitive to factors such as low light or harsh sunlight, camera angle and the level of movement or background activity in the frame.

Furthermore, networked surveillance cameras – which are essentially computers with cameras attached – are only as efficient as the connectivity of the network. As faster speeds and ultimately 5G technology become available, one can safely assume that the performance of such cameras will improve.

Privacy versus security

South Africa’s Constitution protects the right to privacy, as does Article 31 of the Bill of Rights enshrined in the Kenyan Constitution.[13] However, the creeping prevalence of surveillance technologies, as shown in the Artificial Intelligence Global Surveillance Index (AIGS), for example,[14] signals a shift in power dynamics from the state to the private sector.

Historically, surveillance technologies and operations such as signals intelligence (SIGINT) have been controlled by the state. Yet increasingly the private sector is occupying that space by developing the technology and servicing the surveillance equipment and software used by the state and private clients. This arguably represents a paradigm shift with implications for data security, data sovereignty and accountability.[15]

Moreover, the use of biometric surveillance technologies in crime prevention, or as a means through which individuals can access government services, underscores the delicate balance between security and privacy, or indeed privacy and convenience.

Use of biometric surveillance technologies in crime prevention underscores the balance between security and privacy

Increased health surveillance during the Covid-19 pandemic through Bluetooth-enabled smartphone technology[16] shines a spotlight on that balance and is worthy of further research.

A detailed study of the expansion of closed-circuit surveillance in Southern Africa,[17] which includes facial recognition technology, captures the speed with which camera surveillance is being rolled out, especially in highly populated urban areas.

The study also highlights China’s dominance in the market. This is the result of its competitive advantage, owing to its advanced knowledge in the field of biometrics, its established position in the information technology (IT) market and the affordability of its products.

This dominance is likely to continue, given the enthusiasm of many African governments, including South Africa and Kenya, to develop so-called Smart Cities[18] and the stated desire of Chinese companies such as Huawei to be their preferred supplier.

The rollout of cutting-edge surveillance technology is part of China’s Belt and Road Initiative. Studies suggest that, beyond supporting economic development, its aim is to promote surveillance values and greater strategic leverage vis-à-vis the West.[19]

Smart Cities are described in Huawei’s sales literature[20] as offering ‘instrumented, interconnected and intelligent services’ underpinned by digital surveillance capabilities, including facial recognition technology.

China provides much of the digital infrastructure upon which high-definition surveillance cameras depend, and that dominance is likely to continue. The City of Ekurhuleni on South Africa’s East Rand has been earmarked by Huawei for a pilot project under its ‘Safe City Solutions’ brand. The tech giant has already installed its Safe City Solutions in over 700 cities in 100 countries.[21]

In Kenya, where Huawei also has a sizable footprint, the firm has linked its technology to a 46% reduction in regional crime rates.[22]

Risks versus benefits

The balance between the risks and benefits of biometric technologies appears to be highly context specific.

Commercial entities such as banks point to the usefulness of facial authentication technologies in fraud prevention. In South Africa, where the technology is rapidly being adopted, a 20% increase in digital banking fraud was reported by the South African Banking Risk Information Centre (SABRIC) in 2018, compared to the previous year.[23]

The much-publicised data breach at the credit agency Experian in August 2020, which reportedly exposed 24 million South Africans’ personal information to potential fraud, underscores the very real threat of commercial crime.[24]

Most experts consider face-based systems more reliable than fingerprint technology because of the wider range of data points available on the human face. However, some of the harms associated with the technology include its susceptibility to being hacked (resulting in identities being stolen, altered or deleted, or a denial of service or access), algorithmic bias, and the risk of function creep.

The deployment of facial recognition ('one-to-many') technology in the United States (US) as a tool of mass surveillance by the police during recent public protests has raised awareness of these risks and benefits. This has led to a number of high-profile providers, including Amazon, IBM and Microsoft, withdrawing their facial recognition products pending legislation to safeguard their use.[25]

Some of the harms associated with the technology include its susceptibility to being hacked

Civil society organisations (CSOs) have also raised concerns about the commercial sale of personal digital data without a subject's consent. Many countries in Africa could become fertile harvesting grounds for biometric data, which is exported and monetised by private foreign actors or states. Zimbabwe is a case in point.[26]

In South Africa, the risk–reward debate is informed by its recent history. To date this has largely been dominated by the issue of SIGINT. This includes the use of phone intercepts by the security services, which has led to a number of legal challenges.

At the time of writing, there is one such challenge in the Constitutional Court that focuses on the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA). This legislation permits lawful interception of communications technology for policing and national security purposes.

At issue is the principle that the targets of interceptions should be notified after the fact.[27] Hitherto security agents have been forbidden from communicating this to targets, despite its being common practice in countries such as Germany, Japan and the US. The South African security agency's current position has been ruled unconstitutional by a high court.[28] The Constitutional Court is yet to make a judgment.

Furthermore, growing public mistrust of the state security apparatus has fuelled concerns over bulk surveillance and the collection, processing and storage of large volumes of highly sensitive personal data using biometric technologies. It raises questions as to who has access to such sensitive material and under what authority.

Mistrust in the South African state security apparatus is reinforced by the findings of a High Level Review Panel on South Africa's State Security Agency (SSA) ordered by President Cyril Ramaphosa, published in 2019.[29] It revealed an agency that was politicised and corrupt. Its doctrine had 'strayed away' from the principles of the Constitution, which include the right to free speech and the right to privacy.

It is against this backdrop, as well as technological advances in, for example, high-speed Internet (with the imminent prospect of 5G), that public debate about new surveillance tools takes place.

In Kenya a similar debate is underway, although the context is different. Kenya's experience of terrorist attacks post-2013, when the Westgate shopping mall in Nairobi[30] was besieged by Islamist militants, has led to the state acquiring sweeping legal powers.

CSOs have warned that the very real security threats have given the state a pretext to erode personal privacy and extend communications surveillance.[31]

As a result of financial crime and identity fraud, emerging biometric technologies have become ubiquitous across Africa in both the state security and civilian space.

The acquisition of some biometric data, such as one-to-one facial authentication, rests on the principle of consent. However, broader facial recognition technology embedded in CCTV cameras or in software through which digital video images can be run, does not rely on explicit consent. This technology is increasingly being deployed in public spaces and at borders.

Industry insiders in South Africa have told the ISS that the potential of facial recognition technology is often still 'overstated' by manufacturers. However, these technologies, with the help of AI, are being developed at a 'rapid rate' for a global market expected to be worth about US$70 million by 2025.[32] Africa seems to be a key strategic market.[33]

Potential harms

Data security

Biometric technology, which is increasingly networked (i.e., part of an Internet-based system), is potentially exposed to a number of cyber threats. These include the system being hacked and/or data stolen, polluted, altered or destroyed.

There are also questions about who has access to sensitive biometric data. If security agents can access such technologies on centralised databases without reference to a judge, we can expect to see more legal challenges in future.

In contrast, with communications-based technologies (e.g. mobile phones) a judge must issue a warrant under South Africa's RICA.[34] This point was emphasised by South Africa's information regulator in an interview for this paper.[35]

Consequently, the rollout of biometric technologies requires robust countermeasures to mitigate both cyberattacks and malicious use of data by security personnel, foreign state actors or commercial entities, for example. The South African information regulator said that such risks have increased 'exponentially'.[36]

While China provides the infrastructure underpinning the rollout of biometrics, questions of data treatment persist

Given South African companies' limited technical know-how in terms of biometrics, it seems inevitable (at least in the short term) that the country will rely on foreign providers for the bulk of its capability. This opens up questions of data sovereignty and to whose laws foreign players should defer when they capture or process data from outside their own territory.

The opacity of the China–South Africa security relationship raises questions about the dominance of Chinese technology companies with close ties to the Chinese government. While China provides the infrastructure that underpins the rollout of biometrics, and has secured contracts to develop the first Smart Cities in South Africa and Kenya, questions of governance and data treatment persist.

Algorithmic bias

The US' experience with biometric technologies offers important lessons on the potential for bias, especially in the sphere of facial recognition technology.

Algorithmic bias has been demonstrated in a number of tests by the National Institutes of Standards and Technology (NIST), which conducts yearly assessments of the technology.[37] Put simply, an algorithm is a set of rules that govern an action. Studies seem to indicate that this is not a level playing field.

Tests carried out in 2019 by the NIST on facial recognition technology in the US found a bias towards people of colour, particularly black women. It discovered that black women were incorrectly matched 10 times more often than white women.[38] Subsequent tests by the NIST provided 'empirical evidence' of 'demographic differentials' with respect to age, gender and race.[39]

Renee Cummings, a US criminologist and prominent advocate for ethical AI, recently told an ISS seminar[40] that algorithmic design is critically important in shaping biases. This means that whoever designs, develops and deploys the technology has a material bearing on its effectiveness and the situations and locations in which it is deployed.

If not monitored, new technologies can 'create old divisions', in particular racial ones.

Facial recognition technology depends on matching an image against a large pool of other images, which are often gathered in demographically different settings than those for which the technology is used. Tech companies are racing to enhance and expand their databases to make their products more attractive and relevant to African markets and, in effect, 'design out' biases.

Furthermore, the application of AI to biometric technology can result in social sorting. This is a process by which the act of categorising individuals is increasingly surrendered to machines. As the scholar David Loyn explains, 'Codes, usually processed by computers, sort out transactions, interactions, visits, calls, and other activities; they are the invisible doors that permit access to or exclude from participation in a multitude of events, experiences, and processes.'[41]

While such technologies may be efficient, for example in the humanitarian space, they also create the danger of individuals' being excluded on the basis of an algorithm. Human judgement is overridden.

Through social sorting, facial recognition technology has the potential to be used as a tool of social control and human rights violations. In 2019 the US imposed sanctions on various Chinese companies – including Hikvision,[42] a key player in the growing CCTV market in South Africa. This was in response to the use of the company's facial recognition technology to identify minority Uighur Muslims, who China claims pose a terrorist threat.[43]

This kind of social sorting amplifies concerns about the potential for similar human rights abuses on the African continent. An example of such abuse is using biometrics to identify members of the LGBTQI community, or other vulnerable populations, in countries that criminalise homosexuality.[44] This has been raised as a concern by human rights groups in settings such as Zimbabwe and Uganda.

Function creep

Biometric technologies are often run in parallel with other locational technologies such as CCTV surveillance, which film fixed areas, or tools such as vehicle number plate recognition. Together they can provide a considerable amount of data on a person's location, address, mobile phone details and image.

The volume of data subject to data analytics (i.e. human analysis) has been constrained thus far. However, the advent of computer analysis 'enables CCTV to be turned into so-called "dataveillance" devices (that is, devices which conduct surveillance through the collection and computerised analysis of data), which makes individuals and their movements more visible to the state.'[45]

This makes CCTV data a strong candidate for function creep, whereby it is used for a function other than that for which it was originally intended. One example is when data is sold to commercial firms for micro-marketing campaigns.

Likewise, centralised government biometric databases intended to make it easier to access various services may get a security function, giving the police and other security services unfettered access.

Legal frameworks

One of the biggest constraints to effective legal safeguards in the technology sphere is the disconnect between the pace of innovation and the legal and regulatory process. As technology that could be used for surveillance purposes comes on stream, regulations need constant updating.

With increasing private sector dominance of the tech space and more users of that technology (including government departments, security agencies, banks and private security companies), more creative measures to ensure accountability and quality control are needed.

While legislation may offer a set of broad principles, there are gaps in how emerging technologies are policed.

Controls are in place for more traditional methods of communications surveillance, through legislation outlining when interception surveillance is permitted (RICA) in South Africa and the Security Laws Amendment Act (2014) in Kenya.[46] Broadly speaking, the legislation covers the use of technology to intercept an individual's mobile phone usage or extract data from it, or for bulk surveillance of telecommunications traffic by the state security agency.

> While legislation may offer a set of broad principles, there are gaps in how emerging technologies are policed

In South Africa, RICA has recently been subject to legal challenge by the amaBhungane Centre for Investigative Journalism, which argued that sections of the act were incompatible with the Constitution.[47]

Regarding the acquisition of personal data by non-interception means, there are laws governing data collection, retention and disposal. This includes data acquired through biometric tools such as facial recognition.

In South Africa this falls under the Protection of Personal Information Act 2013 (POPIA), which only became fully enforceable in 2020, and in Kenya under the Data Protection Act 2019.[48]

However, the evolving means by which this data is acquired, i.e. hardware such as video cameras or other AI tools, are not fully covered by data protection legislation. There is thus a need for regulations to govern this space.

Private CCTV companies and service providers such as Vumacam (which gave input into this study) use Hikvision cameras to capture vehicle number plate data in crime prevention.

Although theoretically Vumacam has the capability to gather facial recognition data, and Hikvision is one of the main Chinese suppliers of facial recognition tech, it does not do this at present. Nevertheless, the company has been an active voice in the debate over biometric surveillance and was one of the few industry players that agreed to be interviewed for this paper.

Vumacam states in its terms of service that the data it captures is POPIA compliant. In addition, it only works with 'pre-vetted and approved' third party vendors and has conducted a number of tests on products (including those provided by Hikvision) to ensure they are cyber safe and not easily hacked.

Vumacam has publicly called for tighter regulation of the biometrics industry and proactively submitted proposals to government in this regard.[49] However, both the POPIA and its Kenyan counterpart set out exemptions for national security and crime fighting.

Both countries' privacy laws rest on eight internationally agreed principles.

Accountability: It is the duty of the responsible party to ensure compliance with the conditions of the legislation.

Processing limitation: Data processing must be done in accordance with the law and without infringing the privacy rights of the data subject.

The purpose for which the data is collected must be specific: This must be explicitly defined and must be for a lawful purpose. The data must be destroyed once the purpose for which it was collected is achieved. It must be destroyed or deleted once the responsible party is no longer authorised to retain the record, with limited exemptions.

Further processing limitation: To avoid function creep the further processing of personal information must be in accordance or compatible with the purpose for which it was collected.

Quality of information: A responsible party must take reasonable steps to ensure the personal information is complete, accurate and not misleading.

Openness: All documentation must be kept of all processing operations and, where possible, the subject must be made aware of the personal data being collected.

Safeguarding security: A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent the loss of, damage to or unauthorised destruction of personal information. Cyber-security measures must thus be in place for networked data. Any security breach must be brought to the attention of the regulator and the affected data subjects.

Participation of the data subject: A data subject has the right to ask a responsible party to confirm whether or not the responsible party holds personal information about the data subject and to request the record itself. That subject may also ask that the information be corrected or deleted if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully, or retained for longer than permitted.

Source: Privacy International's Briefing Document on International Principles on Data Privacy

CCTV surveillance appears to be a blind spot in many regulations. The collection, processing, storage and disposal of data are covered by data protection legislation in both Kenya and South Africa. However, there do not seem to be controls in determining where cameras should be located, reflecting sensitivities around vulnerable groups such as children, and balancing privacy and security.[50]

Accountability concerns are amplified by the ubiquity of public–private partnerships, as commercial sensitivities and often-complex private supply chains with a number of players can limit transparency.

Researchers have found that

> [t]here is no coordination between the laws that regulate surveillance; there is no mention of a CCTV code of practice even in the POPI Act; there are no legal provisions ensuring a balance is maintained between the need for CCTV camera surveillance and the right to privacy; CCTV cameras in South Africa continue to be installed without privacy assessments being done beforehand; neither public opinion nor participation is allowed in the rollout of CCTV measures, yet the purpose is to protect the public.[51]

Furthermore, the exemptions in the POPI Act on the grounds of national security and crime fighting potentially '[create] huge scope for abuses'.[52]

The UK police force, for example, recently faced a legal challenge in the court of appeal by a civil rights campaigner on the use of facial recognition technology. The court ruled in favour of the appellant, arguing that there had been insufficient impact assessments on whether the technology had inbuilt racial or gender biases.[53]

The case is likely to resonate globally, with similar challenges being likely given the realities of algorithmic bias referenced above.

In Kenya there has been much public discussion about the data commissioner – a position created under the Data Protection Act – whose role is to safeguard against abuse of data. Among the issues raised are the enforcement power of the data commission, which is not a statutory body; funding; the punitive sanctions available; jurisdiction; and dealing with data controllers and processors based outside of Kenya. This last point refers to cross-border data transfers.

One crucial question is 'how will the Data Commissioner deal with Section 51 of the Act that provides exemptions to regulation under the Act for processing of data for national security or public interest purposes?'[54] Will it, for instance, be able to offer guidance to the minister on when such exemptions may or may not be appropriate? And will the minister be compelled to listen?

Many of these debates are being replicated globally. Arguably, the introduction of a tough new data protection regime in Europe, called the General Data Protection Regulation (GDPR), is a point of reference for stakeholders worldwide on setting the parameters of data protection.[55]

CASE STUDIES: Kenya and South Africa

Kenya and South Africa have been selected as case studies to show the breadth and use of biometric technologies, to understand the key drivers and stakeholders associated with this technology, and to outline the current regulation. Each case study will first give an overview of the current landscape, after which it will highlight the key issues and examine the current state of regulation.

Kenya

Current landscape

In Kenya, voice fingerprint, iris and face-based recognition systems are being implemented to reduce fraud. As in many other settings, organisations such as the World Bank promote digital systems[56] as an important development tool to secure access to a range of services and to fulfil SDG 16.9 to 'by 2030, provide legal identity for all'.[57]

In addition, banks and other third-party entities that use the technology to verify and authenticate, for example, bank documents have access to government databases. This was confirmed by research conducted by KICTANET – which describes itself on its website as a 'multi stakeholder platform for people and institutions interested and involved in ICT Policy and regulation'.

In its 2018 report,[58] KICTANET describes Kenya's 'biometric craze', where 'it has become common to be asked for a new photo on primary documents even when there is one already on record'. The assumption is that images are being harvested for inclusion in a database that would enable the wider use of both facial verification and facial recognition technology.

On Kenya's borders, facial recognition technology is being deployed with the assistance of Hong Kong-registered company SenseTime.[59] In the central business district of Nairobi, biometric surveillance via CCTV cameras is being served by Japanese and Chinese suppliers, including Hikvision.[60]

Kenya is also witnessing the growth of biometric databases. For example, the Independent and Electoral Boundaries Commission Database holds the details of approximately 20 million voters. Similarly, the National Social Security Fund Register (NSSF), the National

Hospital Insurance Fund and the Kenya National Bureau of Statistics (NBS) are developing biometric databases.

In the health sector, biometric pilot schemes were first developed in Kenya in 2018 under the banner 'Afya Care – Wema Wa Mkenya' (healthcare is good for Kenyans) supported by the World Health Organization, the World Bank and Kenya's Ministry of Finance.[61]

Banks and other third-party entities that use the technology to verify and authenticate, have access to government databases

A major registration process was undertaken to collect digital data, to be inputted into a Universal Healthcare Coverage (UHC) card. This would enable the card holder to access public health services free of charge.

Much media attention has focused on the Kenyan government's controversial Huduma Namba system launched in 2019. The National Integrated Identity Management System (NIIMS) – the formal name of the Huduma Namba system – is described as an

> initiative … to create and manage a central master population database which will be the 'single source of truth' on a person's identity. The database will contain information of all Kenyan citizens and foreign nationals residing in Kenya and will serve as a reference point for ease of service delivery to the people of Kenya.[62]

The system aims to integrate an individual's personal documentation, including sensitive data such as birth certificate, bank details, profession, mobile phone number, photograph, ID number, cellphone details, fingerprints and DNA. It ran into legal difficulties when a High Court judgment halted the project in January 2020.

The case was brought by the Kenya National Commission on Human Rights (KNCHR), the Kenya Human Rights Commission (KHRC) and the Nubian Rights Forum. The Nubian Rights Forum argued that as a minority that struggles to be recognised by the Kenyan authorities and thus often do not have ID cards, Nubians would effectively be excluded from accessing government services. This is a form of social sorting, as described earlier.

Citing security concerns, the court ruled that although the collection of such data was permitted under the Constitution, not enough safeguards were in place to protect citizens from the potential misuse of their personal data.[63]

The court also found that it was unlawful to use DNA data in combination with other data, such as GPS co-ordinates from cell phone usage, to find out where someone lived:

> [W]e found that the provision for collection of DNA and GPS coordinates in the impugned amendments, without specific legislation detailing out the appropriate safeguards and procedures in the said collection, and the manner and extent that the right to privacy will be limited in this regard, is not justifiable.

Privacy International has taken a close interest in the case. It concluded that the judgment may have stalled the rollout of the system for the time being but the principle of an integrated ID card has not been challenged. This could have implications for the rollout of such technologies worldwide.[64]

Key issues

In terms of the Afya Care healthcare system, an independent analysis of the initiative in 2020 noted 'concerns about the use of identities and data extraction', and the safeguards in place to ensure privacy and prevent function creep.[65]

The same researchers questioned the range of interests behind the rollout, including healthcare providers, government and private sector digital platforms. They also examined the push–pull factors associated with those interests; in particular whether commercial interests are prioritised over others.

The researchers found that, for example, the registration process for the Afya Care system was contracted to private service provider PharmAccess, which also runs M-Tiba, a digital healthcare payment system for private healthcare services.

A single point of service for the Afya Care project may be more efficient, but it also raises concerns about how individual data is used. Could it be re-purposed or used as a micro-targeting tool by the suppliers of a commercial product, in this case the M-Tiba payment system?

Exclusion is another major issue. Interviews conducted by the ISS with CSOs such as KELIN (which represents the legal interests of HIV-positive individuals) highlighted the danger of vulnerable groups' being excluded from healthcare under the Afya Care system.

Globally 'there is very little data to show the cost benefit' of centralised data systems

Allan Maleche, KELIN's executive director, expressed concern about the impact on stigmatised groups, e.g. men who have sex with men, sex workers and those who are in conflict with the law:

> They face 3 layers of vulnerability. First of all their HIV, secondly stigma because of their sexual orientation, and thirdly because they are in conflict with the law and are perceived as criminals [homosexuality is illegal in Kenya despite recent legal challenges] … Our concern is who holds the data and who has access to it.[66]

Although Kenya has had a Data Protection Act since 2019, Maleche warned that there was still no Information Regulator to monitor alleged abuses. He also highlighted the lack of consultation prior to the Afya Care project's being introduced.

Similar concerns about how sensitive biometric data is to be used have been raised with the Huduma Namba system. A key concern with this centralised biometric database is the question of whose interests are served.

Centralised databases' usefulness in reducing the risk of fraud and delivering on development objectives is cited extensively by supporters. However, Dr Isaac Rutenburg, of the Centre for Intellectual Property and Information Technology Law at Strathmore University, Nairobi emphasises that such technologies are not 'neutral' and have not been fully tested. Globally 'there is very little data to show the cost benefit' and efficiency of centralised data systems, he cautions.

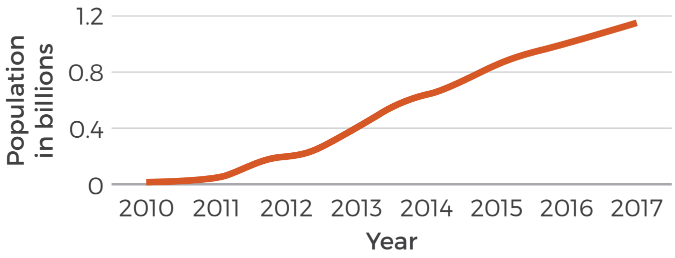
Many of the drivers appear to be coming from private sector business interests. INDEMIA, the French biometric giant reportedly delivering the data capture kits for the Huduma Namba system, was instrumental (under its previous operating name Safran) in introducing electronic voter registration in Kenya during the 2013 and 2017 elections.

IDEMIA subsequently found itself blacklisted by the Kenyan Parliament for both its alleged role in those elections and alleged breaches in company registration regulations. At the time of writing, IDEMIA had launched an appeal[67] and appeared to be continuing to enrol citizens in the Huduma Namba project despite its rollout being halted by the courts.

Commercial operators may gather enough information to re-package their services for different settings and perhaps even offer economies of scale, but there are concerns over suppliers rather than customers (i.e. the government) dictating the pace of biometric rollout.

Furthermore, civil society has raised concerns that such public–private partnerships lack transparency. The risk of limited independent oversight has been demonstrated in India, in what some lawyers describe as 'the world's most ambitious and controversial digital identity programme' – the Aadhaar Biometric Scheme.[68]

Figure 3: Aadhaar – cumulative registrations



Source: Economist.com

The initiative has collected data on some 1 billion individuals, including 'Facial Image, IRIS and Fingerprints for all the residents above 5 years in age'.[69] A system that was initially meant to tackle welfare benefit fraud is now, according to civil society, being used as a tool of mass surveillance by capturing legacy documents and an individual's key life events linked to their biometric ID.[70]

Furthermore, as part of the initiative Indian citizens are invited to join various commercial E-wallet schemes integrated into the system.

While the Aadhaar Biometric Scheme and its various add-on services are premised on the logic of convenience and secure access, organisations such as Privacy International have raised concerns about social profiling, exclusion and data theft – in part because so many different stakeholders can access the data.[71]

In especially the developing world, there is often no robust regulatory framework in place before such systems are rolled out. As a result, 'both the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue and the UN High Commissioner for Human Rights, Navi Pillay express[ed] their "shared concerns"'. These relate to potential 'violations of the right to privacy and the lack of effective protective measures in relation to biometric technologies'.

In addition, there are extensively documented cases of corruption within the Kenyan police and fears that the threat of terrorism is being used as a pretext for impunity.[72]

> There are arguably legitimate concerns about the absence of robust safeguards to protect sensitive data from abuse

Given the multiple terrorist attacks in the country for more than two decades, the Huduma Namba system is firmly entrenched in the country's National Security Strategy.[73] However, the ministry responsible for its implementation is Home Affairs, suggesting some ambiguity of purpose.

The Kenyan government cites '[b]io-terrorism, narco-terrorism, cyber-terrorism, and agro-terrorism' as 'among some of the emerging security challenges that necessitate a radical and progressive reorientation of counter-strategies'.[74]

When fully operational the Huduma Namba system will, according to government documents, enable police officers 'to identify criminal elements and track the "footsteps" of their operations with appreciable accuracy'.[75] Its reach appears to be extensive:

> The fact the system will be interlinked with other databases, including the digital registry of licensed firearm holders and NTSA, [means] information-sharing among security agencies will be smooth and highly reliable. As such, law breakers, rogue motorists and licensed gun owners engaging in criminal activities can be picked out for prosecution at the touch of a button. It is worth noting that the government has rededicated its energies to tracking down and disrupting terrorist financing, and this system will ultimately complement and reinforce the multi-agency approaches to managing security in the country.[76]

In the face of this, there are arguably legitimate concerns about the absence of robust safeguards to protect sensitive data from abuse both by criminal or terrorist networks and by the state.

Furthermore, by locating the system within Kenya's security architecture (although its initial stated purpose was to improve access to government services) opportunities to publicly audit the data may be limited.

Regulation

The new Data Protection Law entered into effect in 2019, encompassing many of the eight International Data Protection principles outlined earlier. However, there are concerns about enforcement.

No independent authority to oversee the implementation of the legislation has yet been set up. The watchdog body does not have statutory powers and there are concerns about how it will be resourced.

Moreover, press reports suggest that the government has sought to downgrade 'the role of the data protection commissioner to a semi-independent data protection agency, with a chairperson appointed by the President'.[77] This raises concerns about the separation of powers and checks and balances needed to build public confidence in the system and reduce the risk of abuse.

'The technology is not seen as neutral,' warns Privacy International. It argues that there is a lack of trust in the government and until there is confidence that it uses the technology for one purpose and not more, 'there are all kinds of red flags'.[78]

There is a very real chance that the technology can be used to persecute dissident groups or marginalise 'undesirables'.[79] Press reports highlight historical difficulties that certain minority groups in Kenya have experienced in getting identification documents.

There are concerns that such exclusions may be replicated by the Huduma Namba scheme, and result in its being used as a means of social and political control. People of Nubian or Somali descent appear to be disproportionately affected.[80] This emphasises the point, made earlier in relation to algorithmic bias, that new technologies may help to perpetuate old divisions.

South Africa

Current landscape

The biometrics landscape in South Africa is arguably slightly more complex, with the financial service sector, the private security industry and government driving technological developments.

For the purpose of this study South Africa's experience of biometric technologies will focus on two key areas:

- Biometric data acquired through public space CCTV and other camera-based access technologies
- Biometric data acquired by and in under the government's proposed centralised digital database (ABIS), which is branded as a system that offers a single point to establish 'truth'[81]

The use of camera-based technologies to verify, authenticate or match a person's identity is driven in part by high levels of commercial crime in South Africa, as well as violent crimes such as theft, robbery, assault and murder.

The Southern African Fraud Prevention Service reported a 99% increase in identity theft between 2018 and 2019

The use of facial verification and facial authentication technology in the financial services industry (which largely relies on one-to-one matches) is rapidly expanding in response to a sharp rise in identity theft. The Southern African Fraud Prevention Service (SAFPS) reported a 99% increase in identity theft between 2018 and 2019.[82]

This has created a surge in demand for companies providing access control and identity verification and authentication services.[83] It has attracted less scepticism among observers largely because one-to-one verification and authentication is based on the principle of consent.

Arguably more controversial has been the deployment of public space CCTV cameras and the use of AI-enhanced facial recognition applications in public spaces. CCTV cameras are used in, among others, streets and shopping centres, near playgrounds and outside government and private buildings.

Michael Sun, a former member of the Johannesburg City Council's Safety and Security Committee, told ISS researchers that biometrics and facial recognition technology had particular appeal for local government for 'public space safety, traffic management, crowd control and disaster prevention'.[84]

While much of the technological know-how resides outside the country, he said that Chinese companies such as Hikvision and Huawei were courting South Africa 'heavily' with 'regular demonstrations' of their products.[85]

The use of public space CCTV surveillance is central to a range of publicly stated crime prevention strategies. Such cameras are used for a variety of purposes. These include licence plate recognition, vehicle-related offences, predictive policing and community surveillance by identifying 'abnormal' behaviours such as loitering and increasingly (but still to a limited extent) facial recognition.

Interviews with Vumacam indicated that 'behavioural detection, i.e. looking at shapes, speed, direction and differences in movement', were of most use in giving security companies 'situational awareness'. When the cameras pick up 'abnormal' movement by examining pixel patterns security patrols can be deployed more efficiently.[86]

Vumacam said its cameras were currently not being used for facial recognition purposes and certain requirements would have to be met before it would consider it. 'They [the cameras used by Vumacam] do not have pan, tilt and zoom ability' and 'we think it is an invasion of privacy.'[87] Vumacam told ISS that until there is regulation and better safeguards, the company had no plans to introduce facial recognition capabilities.

The high-definition digital cameras used by Vumacam and other providers are networked. This means that each is assigned an individual IP address and increasingly operates with the assistance of AI. This lets the camera 'learn' a set of pre-programmed rules and flag deviations from those rules.

Vumacam says its customers use iSentry software, which

> monitors for unusual formations of pixels caused by, for example, someone tripping over as they walk … if the AI detects unusual formations of pixels … it will send an alert to the security company control room where a human control room operator takes over.[88]

Cape Town and Johannesburg have a sizeable CCTV footprint, which comprises both government- and private-owned cameras. In Cape Town private providers must register with the municipality while in Johannesburg no such requirement is currently in place, a point confirmed by councillors and representatives of the private CCTV industry.[89]

This study sought to establish the extent of public space CCTV surveillance and found that the City of Cape Town has 2 345 cameras in its network.[90] These include cameras owned by the Metropolitan Police, the Cape Town Integrated Rapid Transit (MyCiti-IRT) system, the South African National Roads Agency (SANRAL) and privately registered CCTV and licence plate recognition cameras (LPR).

Just over 6% of the Metro Police's camera system has facial recognition technology. The main service provider is Huawei.

The Chinese technology giant, which has close ties to Beijing, provides the 'equipment technology and training' but does not manage the data. This is significant because in 2018 Huawei was accused of being part of a plot to steal data from the Chinese-built African Union (AU) headquarters in Addis Ababa.

In an investigation by the French newspaper *Le Monde*, Huawei was accused of downloading sensitive data on a nightly basis to a central server in Shanghai for five years. Although the company and Beijing have denied this, the subsequent reputational damage has been considerable.[91]

Like the City of Cape Town, Johannesburg's municipal government is stepping up its CCTV capability. During interviews with City of Johannesburg representatives, the ISS established that there were 550 City-owned cameras linked to its Integrated Intelligence Operation Centre (IIOC), a centralised facility managed by the police and city officials.

There is also an active private video surveillance market, where providers are not required to register with the city council. Vumacam, one of the leading players, has 15 000 networked surveillance cameras in Johannesburg,[92] but they are not connected to the IIOC.[93]

As stated earlier, Vumacam does not use facial recognition technology but rather relies on movement detection technologies to pick up what it (or rather its algorithm) considers to be suspicious behaviour.

Nevertheless, there have been media reports of a partnership in the pipeline between cloud video surveillance company Iveda and Axiom, another key technology provider in South Africa. According to reports, a major rollout of cameras with 'built-in face recognition' will soon be deployed at Melrose Arch in Johannesburg. This is part of a project 'to work with the police, local municipalities and private security companies to share information and provide support'.[94] Axiom did not respond to the ISS' request for further details.

There is an active private video surveillance market, where providers are not required to register with the city council

While the City of Johannesburg was unable to confirm how many of its cameras have facial recognition capability, there are clearly hopes to increase their use, although cost is likely to be a constraining factor. Sun said the AI-assisted cameras being considered would have 'multiple functions, not just to catch criminals but to be able to deal with by-law violations, traffic management, emergency and disaster management functions'.[95]

As in Kenya, centralised biometric databases are being used or actively rolled out in South Africa. They are used to streamline data access, provide efficiencies in various government departments, enable cross-referencing of an individual's identity, and assist in law enforcement.

The South African Police Service (SAPS) currently has a fingerprint database consisting of fingerprints from the crime register and from firearms applications. Under its Automated Fingerprint Identification System (AFIS), police teams can monitor persons of interest and deploy mobile units to roadblocks to check identities.

Fingerprints are also used for background checks in the commercial sector and for foreign residents seeking residency or citizenship, to see if applicants have criminal records.

Fingerprint technology is the backbone of HANIS, as new and existing fingerprints can be accessed and verified in real time. This one-to-one verification has also been used extensively in the private sector for access control and identity verification.

However, security issues with HANIS and a lack of consistency in other public service platforms, including immigration and social welfare, are one of the main reasons for the development of an integrated digital biometric system.

As part of the National Identification System Project, the new ABIS will use a wider range of biometric markers, including face, iris, fingerprint and potentially DNA, to prevent identity theft. The database will record life events, including births, deaths and marriages, and is due to come on stream by 2023.

It will be accessed by a range of government departments, including border security, Correctional Services, the SAPS, the South African Social Relief Agency (SASSA) and the South African Revenue Service (SARS). It remains unclear how the data will be managed, secured, audited and controlled, and what legislation will govern the operations of the system.

Heidi Swart, who has researched the subject extensively for the Media Policy and Democracy Project at the University of Johannesburg, highlights a shift in the function of Home Affairs from 'one which issues documents to one which also monitors security'.[96]

Swart concludes that 'with that [shift] comes surveillance, and biometrics is at the heart of their surveillance'.

Other scholars speculate that in many other settings, centralised biometric databases will be declared 'critical databases, which most likely will mean operations will become more and more secretive, so we need to watch the status of that database and who controls it'.[97]

Biometrics, and in particular facial recognition technology, is likely to find its greatest use in crime prevention rather than crime intelligence, according to police sources. Moreover, one senior SAPS source explained in an interview that the prohibitive cost of some of the technologies, coupled with 'a very fragmented approach' to adopting emerging technologies in the police, constrain their deployment.

The perception that South Africa is on the cusp of deploying cutting-edge biometric technologies for bulk surveillance thus needs careful analysis. The use of facial recognition technology in particular at present is limited, if growing.

Key issues

Many of the controversial issues relating to biometric technology – whether deployed through CCTV or centralised databases – have a generic dimension and may include the risk of cyberattack, privacy concerns and function creep. There are also other contextual concerns.

The accumulation of sensitive biometric data by private actors raises concerns about power dynamics

For example, some biometric technologies could be valid in a country such as South Africa, where Parliament and the courts are relatively robust. Yet it is possible that such endorsements could see the accelerated rollout of the technology to other parts of the continent where executive oversight is weaker.

In one instance, civil society actors in Uganda claim that Huawei's technology could be used by the government to target political opponents.[98] As an equipment and software provider, Huawei has sought to distance itself from these accusations and arguably can state that it has limited control over how its technology is used.

The move to the centralisation of biometric data has triggered civil society warnings of a creep towards a 'surveillance state'. Privacy International characterises such a state as one where the surveillance starts of as 'purposeful' and then becomes 'routine', enabling data to be 'retrieved' and 'aggregated so it can be compared, mined and traded'.[99]

While state capacity in South Africa may be too limited to deliver such high levels of surveillance, the accumulation of sensitive biometric data by private actors raises concerns about power dynamics. Strict check and balances are needed.

The very public exit of high-profile IT companies such as Microsoft, IBM and Amazon from the facial recognition market in the US amid concerns of misuse by the police for racial profiling, has had two effects.

Firstly, it shone a spotlight on the ubiquitous nature of biometric technology and the influence of the companies that design the technology. Secondly, it showed the realities of function creep, with the use of facial technology by the police to develop racial profiling.

Although the tech giants in the US case arguably took action on the basis of principle and to minimise reputational damage, controversial uses of biometric technology could well uncover similar points of friction in South Africa.

At the same time, the nature of the response may need to be balanced against the South African context of high levels of identity theft and an energetic IT and private security sector. This may see a trade-off with the need for personal privacy. The response to emerging biometric technologies is therefore likely to be highly context specific.

Centralised biometric databases require regular assessments to protect data from abuse by cybercriminals

As regards ABIS, Home Affairs did not respond to ISS requests to participate in this study. Consequently there are many unanswered questions as to who will provide technical support to ABIS and what the terms of access will be. In particular, it is far from clear what level of access the private sector will have.

With the current HANIS system, banks can access the fingerprint database for identity verification. It is not evident whether this 'one-way flow' of information will remain when ABIS comes on stream or whether there will be an information exchange, thus increasing the risk of data breaches.

Parliamentary papers confirm that the police will have direct access to ABIS.[100] Yet it is still unclear whether it will have unfettered access or under what conditions that access will be granted. While police access to mobile phone data is regulated under RICA legislation, there are no such provisions for data stored under the ABIS project.

Some scholars argue that

> police accessing a database as part of an investigation constitutes a search and therefore needs to be regulated … at the very least in terms of a policy that guarantees that the Home Affairs database will not be accessed for the basis of discrimination or political profiling.[101]

While fraud and identity theft are reportedly on the increase in South Africa, centralising personal biometric data that is highly sensitive may invite further crimes, as it gives hackers a single entry point or a 'single point of failure'[102]. Analysts point to the 2018 breach of the Aadhaar database in India.

The database was hacked using an infected 'patch' (a bundle of code aimed at altering the functionality of a software programme) to disable vital security features. As a result Aadhaar numbers could be generated without the necessarily checks, severely compromising the system.[103]

India's experience is a sobering reminder of the potential for data to be compromised, and Jane Duncan argues that the South African government should take note. She says it 'continues to boast that [its] database cannot be hacked yet the fact that the Aadhaar database was, suggest[s] the Home Affairs database can probably be hacked too'.[104]

Regulation

While the Protection of Personal Information Act 2013 (POPIA) is the main legal instrument to protect against data breaches, its enforcement power must still be fully tested in the realm of biometric technology. The act only became fully operational in July 2020 and data handlers now have a year's grace to ensure they are compliant.

In an interview for this study the office of the information regulator explained that it was still lobbying for resources and developing work plans. At the time of writing it was in the process of establishing an enforcement committee.[105]

Given the speed at which technology advances, the office of the information regulator said 'good data governance principles' would go a long way in minimising data breaches.

In terms of local government, the City of Cape Town has taken some pro-active measures to mitigate risk and develop strong governance principles. In a written response to the ISS, it explained that data acquired through public space surveillance cameras – supplied by, among others, Huawei – is secured at a 'Cape Town managed facility'. In compliance with the POPI Act, it is kept for no longer than 30 days.

The City of Johannesburg has a similar centralised facility for data gathered from cameras owned by the municipality, but there is a noticeable absence of controls to regulate the deployment of private CCTV cameras.

Many cyber experts argue that robust measures to protect network security need to be prioritised as biometric technology becomes more ubiquitous. The Cybercrimes Bill 2017, which awaits presidential assent, is designed to put in place safeguards and emergency response mechanisms, as well as obligations to report cyberattacks. It also sets out penalties.[106]

Dr Brett van Niekerk, senior lecturer in cybersecurity at the University of KwaZulu-Natal, emphasises that cameras and facial recognition software 'can be as vulnerable as a normal computer'. Yet South Africa is 'falling behind on cyber security – Rwanda, Kenya and Mauritius are all ahead of us'.[107]

Resource constraints and the need to speed up engagement with the private sector, where much of the technical know-how resides, threaten to slow down the process of introducing robust and timely cybersecurity measures.[108] However, given the spike in cyberattacks during the Covid-19 pandemic in South Africa,[109] public awareness of data breaches more generally has arguably increased.

At an international level, there are efforts to set norms for states' behaviour in cyberspace. The UN General Assembly has established a Group of Government Experts (of which both Kenya and South Africa are members)[110] and an Open Ended Working Group on ICT.[111]

There are various other initiatives aimed at establishing governance measures and norms for the public and private sector internationally, including the Paris Call for Trust and Security in Cyberspace[112] and the Global Commission on the Stability of Cyberspace.[113]

At the regional level, the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) was adopted in 2014.[114] It aims to provide a framework for cyber security measures, including harmonisation of cyber governance recommendation. However, only a few AU member states have ratified the convention.[115]

Conclusion

There is a significant risk of function creep associated with biometric technologies, resulting in their deployment for a use other than that initially intended. The securitisation of centralised data networks is a particular area of concern and needs further monitoring.

> The spike in cyberattacks during the Covid-19 pandemic in South Africa, has increased public awareness of data breaches

Kenyan security actors should take note of a recent report by the University of Minnesota on the legal challenges in using biometric capabilities as part of counter-terrorism operations.[116] Furthermore, which security actors have access to centralised government databases and under what conditions, remain questions of great importance.

The potential for function creep challenges the principle of minimal use of data.

Furthermore, the collection of personal information associated with contact tracing during the Covid-19 pandemic needs close study to determine the long-term uses of this data.

Biometric surveillance technology is not neutral. There are real risks that already disadvantaged communities will face even more surveillance in order to access centralised government services. The technology may amplify risks of 'social sorting'.

Resource constraints and government capacity are likely to prevent countries such as South Africa and Kenya from becoming fully fledged surveillance states in the near future. Facial verification and authentication technologies are likely to dominate in the short term, driven largely by commercial players.

However, the use of facial recognition technologies can be expected to increase steadily, especially in the realm of public space surveillance.

It is also possible that many countries in Africa with weak regulation can become testing grounds for emerging biometric technologies. This could result in their becoming the setting for a new biometric 'arms race' between competing companies from, for instance, China, Israel and the US.

The rollout of biometric technologies represents an ideological battle, with foreign players exporting competing ideas of surveillance norms. The development of the so-called Smart Cities has been highlighted as an example of a new geopolitical battleground where such competition is played out.[117]

Regulating the biometric space is an urgent priority. Although legislation in Kenya and South Africa seeks to protect data once it is acquired, processed and stored, there are no regulations on how, for example, centralised government biometric databases will be policed.

For legislation to be enforced, the requisite skills must be developed in the commercial crimes unit of the police, the national prosecuting authority and the general public. If citizens are to agree to surrender more personal privacy for the sake of security, biometric technologies must be deployed in a climate of trust.

There is an absence of regulations governing the CCTV industry in South Africa and Kenya. Furthermore, there are no systems in place for auditing the algorithms used for facial recognition purposes, or sanctions for entities that seek to 'harvest' or 'scrape' visual data from the Internet to populate such databases.

Given the concentration of skills and expertise in the private sector, a model of co-regulation should be considered in developing good practice models for the use of biometric technologies as a means of public and bulk surveillance.

The emergence of centralised biometric databases requires regular assessments of the systems and safeguards to protect the data from abuse by private actors (including cybercriminals and hackers), the police or intelligence services.

International and regional engagement on cyber issues, including the AU's cyber security expert group, should ensure that emerging biometric technologies and their potential benefits and harms are entrenched in broader cybersecurity strategies.

Notes

[1] Privacy International, Biometrics, https://privacyinternational.org/learn/biometrics

[2] S Zuboff, *The age of surveillance capitalism*, Newtownabbey: Profile Publishing, 2018.

[3] World Bank, Mobile cellular subscriptions: South Africa, 2019, https://data.worldbank.org/indicator/IT.CEL.SETS?locations=ZA

[4] https://www.is.co.za/about-is/press-releases/looking-beyond-data-sovereignty-to-security/

[5] H Swart, Your cellphone records and the law: the legal loophole that lets state spying run rampant, *Daily Maverick*, 20 May 2018, https://www.dailymaverick.co.za/article/2018-05-20-your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/

[6] South Africa, Department of Home Affairs, Opening speech by Home Affairs Director-General Mkuseli Apleni at the media launch of the Automated Biometric Identification System (ABIS) Project, Taj Hotel, Cape Town, 16 May 2018, http://www.dha.gov.za/index.php/statements-speeches/1123-opening-speech-by-home-affairs-director-general-mkuseli-apleni-at-the-media-launch-of-the-automated-biometric-identification-system-abis-project-taj-hotel-cape-town-16-may-2018

[7] BiometricUpdate.Com, NEC facial recognition border tech for Kenya as airport biometrics rollouts continue, 7 October 2019, https://www.biometricupdate.com/201910/nec-facial-recognition-border-tech-for-kenya-as-airport-biometrics-rollouts-continue

[8] Sub-Saharan Africa is still the lowest-scoring region in Transparency International's Corruption Perception index. See Transparency International, Corruption Perceptions index, https://www.transparency.org/en/cpi/2019#

[9] For more see Identity for All in Africa, https://id4africa.com

[10] L Silver and C Johnson, Majorities in sub-Saharan Africa own mobile phones, but smartphone adoption is modest, Pew Research Center, 8 October 2019, https://www.pewresearch.org/global/2018/10/09/majorities-in-sub-saharan-africa-own-mobile-phones-but-smartphone-adoption-is-modest/

[11] Ibid.

[12] Verification is the process of checking an identity against a document and normally happens once. Subsequent checks on a person's identity are described as authentication and may be done multiple times in order to gain access to a service.

[13] Kenya Law Reform Commission, Constitution of Kenya: Privacy, https://www.klrc.go.ke/index.php/constitution-of-kenya/112-chapter-four-the-bill-of-rights/part-2-rights-and-fundamental-freedoms/197-31-privacy

[14] S Feldstein, The global expansion of AI surveillance, Carnegie Endowment, 17 September 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

[15] Data sovereignty is basen on the concept that data controllers are governed by the law of the country in which that data was gathered. For more see https://www.is.co.za/about-is/press-releases/looking-beyond-data-sovereignty-to-security/

[16] A Chatuvedi, How South Africa uses tech to fight Covid 19, Geospacial World, 21 April 2020, https://www.geospatialworld.net/blogs/how-south-africa-uses-tech-to-fight-covid-19/

[17] H Swart, Video surveillance in Southern Africa, Media Policy and Democracy Project, May 2020.

[18] Smart Africa and Smart Cities Initiative, http://media.firabcn.es/content/S078018/download/14NOV_GF_EGOV_KN2.pdf

[19] A Polyakova and C Meserole, *Exporting digital authoritarianism: the Russian and Chinese models*, Brookings Institution, August 2019, https://www.brookings.edu/research/exporting-digital-authoritarianism/.

[20] Huawei, Smart City brochure, https://e.huawei.com/en/material/industry/smartcity/fa01438ad7df46419a37edafaba1a788

[21] B Prior, Huawei's big plans for safer South African cities, *My Broadband*, 4 March 2019, https://mybroadband.co.za/news/industrynews/298112-huaweis-big-plans-for-safer-south-african-cities.html

[22] Huawei, Video surveillance as the foundation of safe city in Kenya, Press Release, https://www.huawei.com/za/industry-insights/technology/digital-transformation/video/video-surveillance-as-the-foundation-of-safe-city-in-kenya

[23] SABRIC, Annual crime stats 2019, https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2019/

[24] *Times Live*, Massive data attack exposes personal info of 24 million South Africans, 18 August 2020, https://www.timeslive.co.za/news/south-africa/2020-08-19-massive-data-attack-exposes-personal-info-of-24-million-south-africans/

[25] *BBC News*, IBM abandons 'biased' facial recognition tech, 9 June 2020; *IOL*, Will Amazon's move to bar cops from using facial recognition software have consequences?, 11 June 2020.

[26] Burt C *Implementation of CloudWalk Facial Recognition Technology in Zimbabwe progressing in Stages* 18/05/2018 Biometric Update.com https://www.biometricupdate.com/201805/implementation-of-cloudwalk-facial-recognition-technology-in-zimbabwe-progressing-in-stages

[27] For a broader discussion on communications surveillance see M Hunter, Cops and call records: policing and metadata privacy in South Africa, Media and Democracy Project, University of Johannesburg, 2020.

[28] *Amabhungane Centre for Investigative Journalism and SP Sole v Minister of Justice et al.*, Judgment, 16 September 2019, http://www.saflii.org/za/cases/ZAGPPHC/2019/384.pdf

[29] South African Government, High-Level Review Panel on the State Security Agency, https://www.gov.za/documents/high-level-review-panel-state-security-agency-9-mar-2019-0000

[30] D Howden, Terror in Nairobi: the full story behind al-Shabaab's mall attack, *The Guardian*, 4 October 2013, https://www.theguardian.com/world/2013/oct/04/westgate-mall-attacks-kenya

[31] See Privacy International, Track, capture, kill: inside communications surveillance and counterterrorism in Kenya, March 2017.

[32] P Pienaar, #BizTrends 2019: digital, data-driven biometrics, BizCommunity, 15 January 2019, https://www.bizcommunity.com/Article/196/726/185376.html

[33] S Hatrit, Biometric identification: a coveted African market, *The Africa Report*, 22 June 2020, https://www.theafricareport.com/30838/biometric-identification-a-coveted-african-market/

[34] South Africa, Department of Justice, Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, https://www.justice.gov.za/legislation/acts/2002-070.pdf

[35] Interview, Office of the South Africa Information Regulator, August 2020.

[36] Ibid.

[37] United States Department of Commerce, National Institute of Standards and Technology (NIST), https://www.nist.gov

[38] United States Department of Commerce, NIST, *Ongoing Face Recognition Vendor Test (FRVT)*, 5 July 2019, https://www.nist.gov/sites/default/files/ documents/2019/07/03/frvt_report_2019_07_03.pdf

[39] D Harwell, Federal study confirms racial bias of many facial recognition systems, casts doubt on their expanding use, *Washington Post*, 20 December 2019.

[40] Institute for Security Studies, The future of facial recognition tech in South Africa, Webinar, 30 June 2020, https://issafrica.org/events/the-future-of-facial-recognition-tech-in-africa

[41] D Loyn, Surveillance as social sorting: privacy, risk and digital discrimination, Abingdon: Routledge, 2005.

[42] S Shen and J Horwitz, China's Hikvision sees only limited impact from US blacklisting, *Reuters*, https://www.reuters.com/article/us-usa-trade-china-hikvision/chinas-hikvision-sees-only-limited-impact-from-us-blacklisting-idUSKBN1WO0O5

[43] The US sanctions seem to have had only a limited impact on the company, and should arguably be seen within the context of the ongoing China–US trade war and broader strategic issues.

[44] KELIN and the Kenya Populations Consortium, 'Everyone said no': biometrics, HIV and human rights – a Kenya case study, 4 July 2018, https://www.hhrjournal.org/2018/07/everyone-said-no-key-populations-and-biometrics-in-kenya/

[45] J Duncan, *Stopping the spies: constructing and resisting the surveillance state in South Africa*, Johannesburg: Wits University Press, 143.

[46] Kenya, The Security Laws (Amendment) Act 2014, https://www.refworld.org/pdfid/4df202da2.pdf

[47] For a discussion of the case see M Hunter, Cops and call records: policing and metadata privacy in South Africa, Media and Democracy Project, University of Johannesburg, 2020.

[48] *Kenya Gazette Supplement*, The Data Protection Act 2019, 11 November 2019, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

[49] See Annex I.

[50] D Basimanyane and D Gandhi, Striking a balance between CCTV surveillance and the digital right to privacy in South Africa, APCOF, Research Paper 27, December 2019, http://apcof.org/wp-content/uploads/027-cctvsurveillance anddigital-dorcasbasimanyanedumisanigandhi.pdf

[51] Ibid.

[52] J Duncan, *Stopping the spies: constructing and resisting the surveillance state in South Africa*, Johannesburg: Wits University Press, 144.

[53] AFP, UK police use of facial recognition ruled unlawful, *EWN Eyewitness News*, 11 August 2020, https://ewn.co.za/2020/08/11/uk-police-use-of-facial-recognition-ruled-unlawful?

[54] M Laibuta, What awaits the Data Protection Commissioner, Blog, https://www.laibuta.com/data-protection/what-awaits-the-data-protection-commissioner

[55] Intersoft Consulting, General data protection regulation (GDPR), https://gdpr-info.eu

[56] World Bank, Inclusive and trusted digital ID can unlock opportunities for the world's most vulnerable, 14 August 2019, https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable

[57] United Nations, Sustainable Development Goals, Goal 16, https://sdgs.un.org/goals/goal16

[58] KICTA, Data protection In Kenya, https://www.kictanet.or.ke/download/data-protection-in-kenya/

[59] Biometric Update.com, NEC facial recognition border tech for Kenya as airport biometrics rollouts continue, October 2019, https://www.biometricupdate.com/201910/nec-facial-recognition-border-tech-for-kenya-as-airport-biometrics-rollouts-continue

[60] Biometric Update.com, Kenyan police launch facial recognition on urban CCTV network, 24 September 2018, https://www.biometricupdate.com/201809/kenyan-police-launch-facial-recognition-on-urban-cctv-network; T Brewster, Thousands of banned Chinese surveillance cameras wat over US government sites, *Forbes*, 21 August 2019, https://www.forbes.com/sites/thomasbrewster/2019/08/21/2000-banned-chinese-surveillance-cameras-keep-watch-over-us-government-sites/#61bd9cbc7f65

[61] Comprehensive analysis provided by R Prince, A politics of numbers ? Digital registration in Kenya's Experiments with universal health coverage, Somatosphere, 2020, http://somatosphere.net/2020/digital-registration- kenya-universal-health-coverage.html/

[62] Huduma Namba, https://www.hudumanamba.go.ke

[63] See the full judgment at Kenya Law, Consolidated petitions no. 56, 58 and 59 of 2019, http://kenyalaw.org/caselaw/cases/view/189189/

[64] Privacy International, Why the Huduma Namba ruling matters for the future of digital ID, and not just Kenya, 6 February 2020, https://privacyinternational.org/news-analysis/3350/why-huduma-namba-ruling-matters-future-digital-id-and-not-just-kenya

[65] Ibid.

[66] *Reuters*, Kenya's High Court unanimously upholds ban on gay sex, 24 May 2019, https://af.reuters.com/article/topNews/idAFKCN1SU1M7-OZATP

[67] Biometric Update, IDEMIA ban by Kenyan National Assembly appealed as biometric national ID drive passes 15m, 8 May 2019, https://www.biometricupdate.com/201905/idemia-ban-by-kenyan-national-assembly-appealed-as-biometric-national-id-drive-passes-15m

[68] BBC News, Viewpoint: The pitfalls of India's biometric ID scheme, 22 April 2018, https://www.bbc.com/news/world-asia-india-43619944

[69] Aadhaar, Biometric data capture guidelines, https://www.uidai.gov.in/authentication/authentication/2016-05-12-05-56-17.html

[70] Privacy International, Understanding identity systems part 3: the risks of ID, 31 January 2019, https://privacyinternational.org/explainer/2672/understanding-identity-systems-part-3-risks-id

[71] Privacy International, Biometrics: friend or foe of privacy?, Briefing, https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf

[72] K Allen, Kenya's counter-terrorism trade-off, *ISS Today*, 20 April 2020, https://issafrica.org/iss-today/kenyas-counter-terrorism-trade-off

[73] Huduma Namba, Huduma Namba and our national security strategy, http://www.hudumanamba.go.ke/huduma-namba-and-our-national-security-strategy/

[74] Ibid.

[75] Ibid.

[76] Ibid.

[77] Interview, Privacy International.

[78] Interview, Privacy International.

[79] Interview, Dr Isaac Ruttenberg, Center for intellectual Property and Information Technology Law, Strathmore University.

[80] A Latif Dahir, Kenya's new digital IDs may exclude millions of minorities, *The New York Times*, 28 January 2020, https://www.nytimes.com/2020/01/28/world/africa/kenya-biometric-id.html

[81] K Breckenridge, The biometric state: the promise and peril of digital government and the new South Africa, *Journal of Southern African Studies*, 31:2, June 2005, 267–282.

[82] BusinessTech, Big increase in identity fraud cases in South Africa, 19 September 2019, https://businesstech.co.za/news/technology/342057/big-increase-in-identity-fraud-cases-in-south-africa/

[83] For a detailed discussion see ISS, The future of facial recognition tech in Africa, webinar, 30 June 2020, https://issafrica.org/events/the-future-of-facial-recognition-tech-in-africa

[84] Interview, Cllr Michael Sun, former MMC Johannesburg City Council, July 2020.

[85] Ibid.

[86] Interview, Ricky Crook, CEO Vumacam, August 2020.

[87] Ibid.

[88] Vumacam's emailed response to ISS questions, August 2020.

[89] Interview, Ricky Crook, CEO Vumacam, August 2020.

[90] Alderman JP Smith, Mayoral Committee Member for Safety and Security City of Cape Town, in response to ISS questionnaire.

[91] E Olander, African Union caught in crossfire of US–China feud over Huawei, *theafricareport*, 19 November 2019, https://www.theafricareport.com/20280/african-union-caught-in-crossfire-of-us-china-feud-over-huawei/

[92] H Swart, Visual surveillance and weak cyber security, part one: when cameras get dangerous, *Business Maverick*, 13 June 2019, https://www.dailymaverick.co.za/article/2019-06-13-visual-surveillance-and-weak-cyber-security-part-one-when-cameras-get-dangerous/

[93] Interview, Cllr Michael Sun, former MMC Safety and Security Committee City of Johannesburg, July 2020.

[94] C Burt, Iveda brings biometrics and surveillance analytics to South Africa with AXIOM partnership, Biometric update.com, 7 June 2019, https://www.biometricupdate.com/201906/iveda-brings-biometrics-and-surveillance-analytics-to-south-africa-with-axiom-partnership

[95] Interview, Cllr Michael Sun, former MMC Safety and Security Committee City of Johannesburg, July 2020.

[96] Parliamentary Monitoring Group (PMG), BMA Bill: NCOP amendments; Performance Audit on undocumented immigrants; with Minister & Deputy Minister, 4 February 2020, https://pmg.org.za/committee-meeting/29634

[97] Interview, Prof. Jane Duncan, University of Johannesburg, August 2020.

[98] *The Financial Times*, Uganda confirms use of Huawei facial recognition cameras – police deny surveillance technology is monitoring opposition politicians, 20 August 1019.

[99] Privacy International, Defining the surveillance state, 31 October 2013, https://privacyinternational.org/blog/1513/defining-surveillance-state

[100] PMG, Question NW2530 to the Minister of Home Affairs, 11 September 2018, https://pmg.org.za/committee-question/9898/

[101] Interview, Prof. Jane Duncan, University of Johannesburg, 7 August 2020.

[102] Interview, Prof. Jane Duncan, University of Johannesburg, 7 August 2020.

[103] *Huffington Post India*, UIDAI's software hacked: ID database compromised, experts confirm, 11 September 2018, https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/

[104] Interview, Prof. Jane Duncan, University of Johannesburg, 7 August 2020.

[105] Interview, Office of the South Africa Information Regulator, August 2020.

106 S Mzekandaba, SA's Cyber Crimes Bill edges forward amid increased attacks, *ITWeb*, 15 June 2020, https://www.itweb.co.za/content/nWJad7bekJavbjO1

107 See International Telecommunication Union (ITU), Global Cybersecurity Index 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

108 K Allen, Is Africa cybercrime savvy?, *ISS Today*, 26 June 2019, https://issafrica.org/iss-today/is-africa-cybercrime-savvy

109 IOL, Spike in cyberattacks as cyber criminals exploit Covid-19 lockdown – report, 12 April 2020, https://www.iol.co.za/technology/software-and-internet/spike-in-cyberattacks-as-cyber-criminals-exploit-covid-19-lockdown-report-46424508

110 United Nations (UN), Disarmament: Group of Governmental Experts, https://www.un.org/disarmament/group-of-governmental-experts/

111 UN, Disarmament: Open-ended Working Group, https://www.un.org/disarmament/open-ended-working-group/

112 Paris Call, https://pariscall.international/en/

113 Global Commission on the Stability of Cyberspace, https://cyberstability.org; K Allen, Could norms be the answer to policing cyberspace?, *ISS Today*, https://issafrica.org/amp/iss-today/could-norms-be-the-answer-to-policing-cyberspace

114 African Union IAU), African Union Convention on Cyber Security and Personal Data Protection, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

115 As of June 2020, only eight out of 55 AU member states had ratified the convention.

116 K Huszti-Orban and F Aolain, Use of biometric data to identify terrorists: best practice or risky business?, Human Rights Centre University of Minnesota, 2020.

117 A Ekman, China's smart cities: the new geopolitical battleground, Institut Francais des relations internationals, December 2019.

Enhancing Africa's response to transnational organised crime

This project is funded by the European Union

About the authors

Karen Allen is a Senior Research Advisor on Emerging Threats in Africa as part of ISS's Complex Threats in Africa Programme. She holds a Masters in International Relations and Contemporary War from King's College London and is a Visiting Fellow at the same institution. She was previously a BBC foreign correspondent working across East and Southern Africa and Afghanistan.

Isel van Zyl, Research Officer in the Complex Threats in Africa programme, holds a Master's degree in Advanced European and International Studies from the Centre international de formation européenne (CIFE) in Nice, France.

About ENACT

ENACT builds knowledge and skills to enhance Africa's response to transnational organised crime. ENACT analyses how organised crime affects stability, governance, the rule of law and development in Africa, and works to mitigate its impact. ENACT is implemented by the ISS and INTERPOL, in affiliation with the Global Initiative Against Transnational Organized Crime.

Acknowledgements

The author wishes to thank all participants for their time and valuable insights, which have helped to inform this paper.

ENACT is funded by the European Union (EU). This publication has been produced with the assistance of the EU.

ISS INSTITUTE FOR SECURITY STUDIES

INTERPOL

GLOBAL INITIATIVE AGAINST TRANSNATIONAL ORGANIZED CRIME

Cover image © Adobe Stock – only4denn.