Surveillance Law in Africa: a review of six countries

South Africa country report

Grace Mutung'u

DOI: 10.19088/IDS.2021.059

Introduction

This report explores South Africa's existing surveillance law in comparison to the United Nations (UN) Draft Legal Instrument on Government-led Surveillance and Privacy (UN 2018). The Draft Instrument calls for narrowing of the reasons for surveillance and requires that surveillance be undertaken with judicial oversight and other checks and balances. This report finds that South Africa's law aligns with certain aspects of the Draft Instrument – for example, the existence of a surveillance law that requires pre-authorisation from a judge. However, the report identifies breaches in practice and gaps in the legislation and resourcing, making recommendations on the need for additional protections, increased capacity and improved safeguards. It also recommends strengthening of the law to make it human rights-centred and to increase transparency and accountability.

South Africa is one of the few African countries that has a law dedicated to governing surveillance as recommended by the UN Draft Legal Instrument (UN 2018). Recent history points to four eras of surveillance in South Africa (Africa 2009). The first two are the colonial and apartheid eras, followed by post-apartheid and the current post-9/11 era. During the colonial and apartheid periods, law enforcement employed various surveillance methods to control movement, and the political and economic activities of black people and their allies (Breckenridge 2014). These included requirements for black people to have movement passes, and intelligence-gathering through police and special forces (Africa 2009). In tandem, black political parties such as the African National Congress (ANC) had their own intelligence units (Duncan 2018). Following the transition to democracy in the 1990s, there were negotiations that led to an amalgamation of security services, including intelligence (Africa 2009). The Interception and Monitoring Prohibition Act (IMPA) of 1992 was also enacted to regulate surveillance activities. The subsequent 1996 Constitution provided a strong Bill of Rights as well as the creation of post-apartheid intelligence institutions. The South African Bill of Rights includes guarantees of the right to privacy of correspondence, communication and data (Republic of South Africa (RSA) 1996).

A year after the 9/11 attacks in the United States (US) in 2001, the IMPA was replaced with the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA 2002). At the same time, the country increasingly invested in mass surveillance systems varying from signal intelligence to biometric identity technologies (Duncan 2018; Allen and van Zyl 2020). While the existence of a law regulating surveillance prevents arbitrary interception of communication, studies show that the institutions and processes created under RICA do not uphold the right to privacy (Kwet 2017; Duncan 2018; Allen and van Zyl 2020). A 2021

constitutional court judgement faults RICA for unlawful bulk surveillance and foreign signal interception (amaBhungane Centre 2021). The judgement calls for creation of post-surveillance notification and the independence of the judges authorising surveillance warrants.

Like other African countries, South Africa is also adopting biometric technologies in identification of persons and access to government services. Biometric technologies have been applied in social welfare grants while learners in schools are registered using unique personal identifier numbers. There is also wide use of closed-circuit television (CCTV) by city governments as well as private persons. These new technologies create new capabilities that could be used for government surveillance (Black Sash 2019; Kwet 2017; Allen and van Zyl 2020).

1. What reasons does the South African government use to justify surveillance?

During the colonial and apartheid eras, surveillance was undertaken for political and social control. Surveillance studies caution that although colonialism and apartheid were abolished, many of the colonial institutions and practices were carried over into the post-apartheid era. For example, surveillance of journalists and protest movements is common, even though the constitution guarantees the rights of journalists as well as the right to protest (Duncan 2018). There have also been national scandals involving surveillance of political leaders despite the constitutional and legal guarantees for political neutrality and lack of partisanship in government surveillance (Swart 2015).

During the transition to democracy, South Africa developed a policy on intelligence based on holistic and human security. The White Paper on Intelligence (1994) advanced the idea that many of the threats to South Africa's stability would be internal, hence a need to not only solve crime but prevent it (Nathan 2009). This has resulted in intelligence-led policing where police not only enforce the law but are also concerned with risk management. It has also created a basis for broadening surveillance for reasons such as food and security (Farrell 2019).

In addition to national security, protecting 'national interests' is another motivation for surveillance. Duncan (2018) argues that this rationale has been applied in economic surveillance of business leaders in private interests such as oil and minerals. Foreign communications surveillance has been carried out by the National Communications Centre (NCC) of the country's civilian intelligence agency, the State Security Agency (SSA). It was temporarily halted by the country's apex court after the court found that there was no specific legal authority for the NCC to carry out foreign surveillance (amaBhungane Centre 2021).

Surveillance is also practised as part of anti-terrorism measures since the 9/11 attacks in the US. The Snowden revelations in 2013 reignited interest in surveillance by civil society and academia. South Africa's three terms as a non-permanent member of the UN Security Council also influenced the country's adoption of surveillance laws and practices (Kwet 2020). This is particularly so in areas of anti-terrorism and financial surveillance. Financial

surveillance is undertaken by the Financial Intelligence Centre created under the Financial Intelligence Centre Act (FICA) of 2001.

At an ideological level, South Africa's surveillance is also driven by its relations with pro-surveillance development partners (Feldstein 2019). For example, it has intelligence research and training facilities not only for training of officers, but which also serve as grounds for permeation of intelligence doctrines (Marais 2021). Collaboration with countries such as China and Russia in intelligence research and training have served to advance domestic intelligence through various means such as social media surveillance and building of smart cities with surveillance capabilities (Bosch and Roberts 2021). Related to this is that South Africa is a surveillance technology producer, and the birthplace of the surveillance technology company VASTech. The company, which was initially funded by the South African government, was implicated in supplying surveillance technology to the Libyan government in 2011 (Privacy International 2014; McLaughlin 2016). This may therefore contribute to South Africa acquiring vendor-driven surveillance technology, even when the country does not face major terrorism threats (Duncan 2018).

In 2020, when the Covid-19 pandemic struck, South Africa turned to geolocation data for contact tracing (Gillwald *et al.* 2020). Following pressure from activists, contact tracing regulations were developed (Bosch and Roberts 2021). They require the Department of Health to protect the privacy of persons whose information is in the contact tracing database. A judge, referred to as the Covid-19 designated judge, was also appointed to oversee aspects of the contact tracing database such as receiving reports on activities undertaken during contact tracing and on the lapse of the pandemic period (RSA 2020). Notably, regulation 11(b) restricts use of the data in the contact tracing database to contact tracing and not movement restriction.

2. Which international conventions protecting privacy has South Africa adopted?

Although a founding member of the UN, South Africa did not sign the Universal Declaration of Human Rights (UDHR) in 1948 as the government then upheld the apartheid doctrine whereby a person's rights and entitlements were dependent on the colour of their skin. In 1974, South Africa was suspended from the UN as part of the anti-apartheid struggle and only re-admitted in 1994 when apartheid ended. In 1996, South Africa adopted a new constitution that domesticates international human rights law, including the right to privacy through its Bill of Rights. Among the international treaties the country has ratified are the International Covenant on Civil and Political Rights (ICCPR), which obligates the country to protect and promote various rights including privacy. The country is also a member of the African Union (AU) but has not signed the African Union Convention on Cyber Security and Personal Data Protection. South Africa is also active in the regional bloc, the Southern African Development Community (SADC). SADC has been pursuing a harmonised information and communications technology (ICT) regulatory environment, including developing model laws on cybersecurity. The model laws approach information as an asset and criminalise unauthorised interception (Tembo 2013). South Africa has taken leadership by enacting a data privacy law in 2013, although its implementation was phased (Calandro and Berglund 2019). A dedicated cybercrimes law was also enacted in 2021.

3. Which domestic laws enable or limit permitted surveillance in South Africa?

Article 14 of the Constitution protects privacy, including the right to not have one's communications infringed. Article 36 further stipulates that rights may only be limited in accordance with international principles of legality, necessity and proportionality. The right to privacy is further elaborated by the Protection of Personal Information Act (POPI), which fully came into force in 2020. The Act has national security exemptions for processing of personal data. Section 6 sets out some exclusions, such as national security activities, anti-terrorism, public defence, public safety, prevention of money laundering, and investigation and prosecution of offences. The Constitution also guarantees the right of access to information, giving people an entitlement to request information related to surveillance.

The Constitution outlines principles for national security that include: equality of all people and pursuit of a better life; peace and security; rule of law, including international law; and subjugation of national security to checks and balances by Parliament and the executive.

There are therefore several laws on security, information and privacy. Intelligence is governed by the Intelligence Services Act, National Strategic Intelligence Act and the Intelligence Services Oversight Act, all dated 1994. These laws create operational and oversight mechanisms for domestic and foreign surveillance. More recent security laws that establish a basis for surveillance include the Protection of Constitutional Democracy against Terrorist and Related Activities Act of 2003 and FICA of 2001. National security-related information laws include the Protection of State Information Bill – a draft law on the classification and protection of state information. It is intended to replace the Protection of Information Act 84 of 1982. The Cybercrimes Act was recently enacted. It creates offences of unlawful interception of data, messages, computers and networks involving hacking, ransomware attacks and cyber extortion. The Act also grants law enforcement agencies extensive powers to investigate, search, access and seize various articles, such as computers, databases or networks. The Act further imposes a duty to report certain offences on the part of electronic communications service providers and financial institutions within 72 hours. Failure to make the required report could lead to a fine of up to 50,000 rands (ZAR) on conviction.

South Africa has had a dedicated surveillance law since the early 1990s. The current law, the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 (RICA), prescribes the limited 'legitimate aims' of interception of citizen communications (RSA 2002). These are listed in section 16 as serious offence, public health or safety, national security, or compelling national economic interests. RICA creates a judicially supervised mechanism for lawful interception of communications. Where there is no consent of one of the parties to the surveillance, then law enforcement officers are required to apply for an interception warrant from a designated judge (section 16). A RICA judge can also issue a real-time communication-related warrant (section 17) and any magistrate can issue an order for archived communication (section 19). In addition to these RICA provisions, law enforcement officers have a separate route for obtaining metadata under section 205 of the Criminal Procedure Act (1977).

RICA also stipulates mandatory SIM card registration. The Act requires communications service providers to retain communications-related information (metadata) for between three and five years. RICA-related interceptions are undertaken by the Office for Interception Centres (OIC) on behalf of applicants.

Other laws forming the basis of surveillance include FICA (2001). FICA was enacted to identify proceeds of unlawful activities as well as to combat money-laundering activities. It establishes a financial reporting centre to collect data that may be useful in achieving its goals. Financial institutions are therefore required to collect and keep records of their clients and transactions, and to report suspicious transactions as well as transactions above certain limits (FICA 2001, sects. 28 and 29). The financial reporting centre and law enforcement officers can access the records of a financial institution, after obtaining a court warrant. As per section 26 of the Act, grounds for issuance of such a warrant include identifying proceeds of unlawful activities and combating money-laundering activities. In addition, section 35 of FICA links FICA to RICA by empowering the RICA judge to consider applications for monitoring a person suspected of handling the proceeds of crime or money-laundering. Such an application and order is made without notice to the person suspected of these crimes.

4. How does South African surveillance law compare with that in other countries in Africa/US/EU/UK?

South Africa has a dedicated surveillance framework, including specific legislation as well as oversight mechanisms such as a parliamentary committee on intelligence. The law is similar to the Investigatory Powers Act (IPA) in the United Kingdom (UK) as well as the USA PATRIOT Act.[1] South Africa's law was enacted in 2020, the year after the 9/11 attacks in the US, and it shares an anti-terrorism rationale.

The Snowden leaks in 2013 exposed some of the surveillance activities undertaken by the US, the UK and other governments as being outside what is provided for under the law. Documents filed in a case challenging mass surveillance also revealed extra-legal surveillance in South Africa (Mohapi 2019). Duncan (2018) has argued that the reason for state surveillance is not primarily anti-terrorism but domestic politics, since South Africa does not face the same threats as Eastern African countries. A 2008 Commission of Inquiry report noted that intelligence agencies were embroiled in partisan intelligence-gathering and recommended reforms to laws and services. Recent scandals involving unauthorised surveillance on politicians and businesspersons show that the gap in oversight of surveillance operations still exists (Nathan 2017).

Despite South Africa having a specific law on surveillance, RICA has some shortcomings compared to similar frameworks in other countries. For example, RICA does not protect the rights of people who are under surveillance. This is in contrast to the US procedure for interception of wire, oral or electronic communications where people under surveillance in criminal matters must be notified within 90 days of the lapse of a court order. This lack of a post-notification procedure was among the issues criticised in the RICA judgement in the amaBhungane case, described further in section 7.

Similar to the issues in the amaBhungane case, a 2020 judgement on the German foreign intelligence service (BND Act) considered the issue of foreign signal interception. In both cases courts found that foreign communication surveillance was legally subject to the same standards as domestic

1 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

surveillance. While the German law was revised in 2021, there is a probability that a new law for foreign intelligence will be enacted in South Africa.

Another shortcoming of RICA is its weak reporting mechanisms. While countries such as the UK, US and Germany have independent reporting mechanisms, in South Africa, parliamentary reports are written by the RICA judge – the same judge who hears applications for surveillance warrants.

5. How does South African surveillance law compare with the UN Draft Legal Instrument?

South Africa's legal framework for surveillance meets the 'legality' requirement of the International Principles on the Application of Human Rights to Communications Surveillance (Electronic Frontier Foundation (EFF) 2013) as all surveillance needs to be prescribed in legislation and authorised by the court. However, reports indicate that surveillance, particularly mass surveillance and foreign signal interception, is carried out outside of the law (Duncan 2018). For example, there is no clear legal basis for mass surveillance, yet the government admits to tapping communications in undersea cables (Mohapi 2019). RICA and other existing legislation is insufficiently clear regarding use of novel surveillance technologies such as CCTV, biometric identities and artificial intelligence for surveillance, leaving them to broad use which may not be necessary and proportionate (Allen and van Zyl 2020). For example, government agencies such as the South African Social Security Agency (SASSA), which use biometrics such as fingerprints and face photographs in identification of social welfare beneficiaries, outsourced welfare distribution to third party companies, without sufficient oversight of how beneficiaries' personal data would be used (Black Sash 2019). In addition, the country is adopting biometric technologies, including facial verification for national identity as well as social protection programmes (Allen and van Zyl 2020). CCTV is widely deployed by local governments in large cities to deter crime. While aspects of such surveillance (for example, privately owned CCTV) are covered under the data privacy law, the POPI Act, public surveillance may be exempt from the Act. This is despite the fact that some cities are adopting facial verification and facial recognition technology (Allen and van Zyl 2020). This calls for a review of the law to limit the use of biometric identity data in surveillance.

RICA also defines legitimate aims of surveillance as recommended in the UN Draft Legal Instrument. Legitimate aims of surveillance under the law include actual and potential threats to national security, as well as public health. However, these categories are quite broad, and they have been used to target investigative journalism as well as legitimate work of non-governmental organisations (NGOs) and protest movements (Duncan 2018). The amaBhungane case also demonstrated that mass surveillance and bulk signal interception occurs outside the law, a clear violation of the UN Draft Legal Instrument, which calls for surveillance to be based on law. There

is also research indicating that law enforcement officers sometimes obtain metadata without a warrant (Swart 2015).

Targeted surveillance in South Africa requires pre-authorisation by a judge appointed specifically to consider applications under the RICA Act. This fulfils the requirement under the UN Draft Legal Instrument for a 'competent judicial authority' to assess surveillance requests. The judicial process is carried out in secret, even the application for archived information. Section 42(3) of RICA prohibits disclosure that a direction has been issued under this Act, that a communication is being or has been or will probably be intercepted, or that real-time or archived communication-related information is being or has been or will probably be provided. There are therefore no legal means for a subject of surveillance to know that they were under surveillance and for what reason, and thereby to appeal, correct or seek remedy.

The judge periodically reports to a committee of Parliament that specifically deals with intelligence issues – the Joint Standing Committee on Intelligence (JSCI). Reports by the judge featured in Duncan (2018) demonstrate the challenges of oversight of surveillance requests. These include the high number of requests to be considered by one judge, lack of sufficient information in the applications as well as over-reliance on the grounds of threat to national security for legitimate situations such as communications between journalists or protest organisers.

While RICA provides oversight mechanisms, it fails in transparency. Operational oversight is achieved through institutional arrangements. Various law enforcement officers can apply for interception warrants through the Office for Interception Centres (OIC). The OIC makes quarterly reports on its activities to the State Security Agency (SSA). However, surveillance reports are also not published for public scrutiny.

There are mechanisms for public complaints – for example, under the Intelligence Services Oversight Act. A Committee of Members of Parliament (MPs) on Intelligence as well as the Office of the Inspector-General of Intelligence have wide powers such as review of intelligence and counter-intelligence activities of any law enforcement service as well as review and investigation of public complaints. However, the lack of notification to surveillance subjects makes it difficult for the public to make use of these avenues, as surveillance subjects may not be aware that their communications are being intercepted.

6. Does legislation provide adequate definitions of key legal terms?

RICA lists some of the legitimate aims of surveillance in section 16(5). Reasonable threats are broadened under section 16(5)(a)(iii), which allows intelligence-gathering for potential threats on public health and safety as well as national security. However, these terms are not closely defined in the legislation and in practice the majority of RICA-related warrants are issued for investigations involving 'drug-dealing and drug-trafficking, vehicle theft and car hijacks, armed robberies, corruption and fraud, assassinations, murder and terrorism' (Duncan 2018: 101). Legislation originally motivated by terrorism is now routinely being used to police crimes, including auto-theft. Clear definition of legitimate aims and judicial oversight is necessary to confine privacy violation to narrowly targeted surveillance of the most serious crimes.

South Africa has a broad definition of national security. Article 198 of the Constitution outlines national security principles that encompass human security as well as prevention of armed conflict within the country's borders (RSA 1996). Consequently, security and intelligence policies take a broad view on security that includes national security concerns such as terrorism and organised crime as well as human security issues such as food and water security and illicit financial flows. Nathan (2009) argues that a progressive interpretation of human security should include taking into consideration the work of other stakeholders such as NGOs and academics as opposed to increasing the mandate of intelligence bodies.

7. How do legal safeguards, checks and balances, and independent oversight operate in practice?

The existence of a surveillance law in South Africa aims to protect people from arbitrary surveillance since law enforcement officers are required to get pre-authorisation from a judge. Reporting requirements also open the subject of surveillance to scrutiny by Parliament, and this creates a window for oversight.

However, as noted from the amaBhungane case, the checks and balances under RICA are not sufficient. In that case, Stephen (Sam) Sole, an investigative journalist and executive director of a non-profit news outfit (the amaBhungane Centre for Investigative Journalism), discovered that he had been a subject of government surveillance under RICA. He had previously had concerns that he was under surveillance and attempted to get information on whether he was being surveilled through an information request to the Inspector-General of Intelligence, an office that is charged with oversight of intelligence services. His information request was declined, with the Inspector-General replying that he had found no evidence of wrongdoing on the matter, as everything was done within the regulatory framework. Seven years later, transcripts of Sam Sole's conversations with a senior prosecutor were annexed to an affidavit in a case involving South Africa's former president, Jacob Zuma. This raised questions such as under what reasonable grounds an interception order had been issued against a journalist, as well as when and how long the intercepts had been kept. Sam Sole sought another information request from the SSA, and learnt that a judge had issued an interception warrant in 2007 and renewed it in 2008. He therefore instituted a case challenging several aspects of RICA, including: lack of notification of people under surveillance; lack of clarity under RICA on how interceptions are stored and processed; mandatory data retention under RICA; lack of procedural justice in the appointment of the RICA judge, their lack of tenure and lack of open justice in RICA interception applications; and inadequate protection for journalists and their sources (amaBhungane Centre 2021).

The case demonstrated deficiencies in safeguards, oversight and checks. For example, the court heard that the authorisation for surveillance solely depends on the designated RICA judge, who is often overwhelmed by applications. The judge also only hears one side, making the process biased towards law enforcement and therefore not independent. This is worsened

by the lack of user notification, which means that people under surveillance cannot appeal wrongful surveillance. This breaches due process and diminishes the right to privacy.

8. How effective are existing laws and practices in protecting privacy and limiting surveillance?

Analysis of the number of interception orders granted shows that they have increased over the years. Between 2008 and 2015, there were at least 315 interception applications each year, with the highest number being 752 in 2015. The addition of the financial reporting centre to the RICA framework in 2014 contributed to a rise in interception applications (Duncan 2018). The number of orders issued by judges versus interceptions reported by the OIC also suggests that the scope of the orders was broad, defeating the proportionality principle *(ibid.)*. This could also be attributed to the administrative over-breadth of the OIC, which results in use of the framework for interception orders for ordinary crimes (Klaaren 2015).

Very few applications for targeted surveillance were denied. Nevertheless, there are examples of orders being given for surveillance where the facts were contested. In the amaBhungane case, a journalist's communications were 'lawfully' monitored on the grounds of suspicion of trading in guns, yet he was following a corruption investigation. Had the journalist been informed of the surveillance, he might have had the opportunity to contest it. In another case, an order for surveillance of a lawyer was extended to his family and clients, even though they were not of interest to the case. This infringed the confidentiality of the lawyer's clients. In these cases, there were interception directions that had been confirmed by the Inspector-General of Intelligence as lawful.

Duncan (2018) also raises issue with reports to Parliament being written by the judge who issued the orders, arguing that the reports could be partial and also statistical as opposed to analytic. For example, the judge reported on the number of applications for interception directions, the state agency that made the applications, and the number that were granted or refused, with very general comments on trends in applications.

The requirement for communications service providers to keep metadata, or information about communications, is another source of concern, as metadata can give granular insights into a person's behaviour. Coupled with the fact that the OIC houses the fibre optic cables from the communications service providers, this makes it possible for the OIC to carry out surveillance without authorisation, or to extend authorisation to further surveillance.

Despite RICA requirements, South African law enforcement can and sometimes does use section 205 of the Criminal Procedures Act to obtain metadata. This provision allows officers to request a court to order production of metadata for investigations without the service provider having to appear in court. The request does not have to be before the RICA judge, making it possible for law enforcement to obtain orders from the other available courts (Swart 2017). This creates another, less stringent avenue for communication surveillance that goes unreported and sits outside of judicial safeguards and parliamentary oversight.

9. Are existing surveillance practices in South Africa 'legal, necessary and proportionate'?

Although most of the targeted surveillance in South Africa is carried out under RICA, it is plausible that some of the surveillance takes place without going through the authorisation process outlined under RICA. In addition, as noted above, law enforcement officers can also get metadata using a different procedure under the Criminal Procedure Act (Duncan 2018; Swart 2017).

Duncan (2018) and Swart (2017) are among researchers who have faulted practices under RICA. For example, statistics on the number of orders under RICA versus the number of interceptions lead them to conclude that law enforcement agencies often use one RICA warrant to carry out several interceptions. This is partly due to the under-resourcing of the competent judicial authority – a sole judge has to hear all RICA applications. A review of the RICA judge's report under the Act also indicates that the increase in number of surveillance requests to the OIC (the office that makes applications on behalf of law enforcement agencies) increased the risk of making mistakes in RICA applications. This means that RICA does not have sufficient mechanisms to guarantee necessity and proportionality of targeted surveillance.

As was the finding in the amaBhungane case, foreign signal interception as well as bulk surveillance are carried out without a legal basis. RICA therefore violates the International Principles on the Application of Human Rights to Communications Surveillance (EFF 2013).

10. How has surveillance law played out in court in South Africa?

The apartheid era case of *Mistry v. Interim National Medical and Dental Council of South Africa* (1998) is often used not just in South Africa but other African countries to argue the link between privacy as part of dignity that is protection from surveillance. The more recent case, amaBhungane (2021), will also now form part of jurisprudence. It examined the limitations of privacy, noting that states can use prevention of crimes as a ground for limiting privacy in a law. However, the court pointed out that such interceptions must also be limited; they cannot be indiscriminate, hence the finding that bulk interception was unlawful.

The amaBhungane case is also important for its discussion on checks and balances. While agreeing that it may not be practical to notify people prior to targeted surveillance, the court found that post-notification was an important check that could partly address the impunity of law enforcement officials who carry out wrongful surveillance.

Information gathered under RICA is admissible as evidence in court. There are examples of prosecutions where information on crimes such as murder is obtained from interception of mobile phones. Mobile phone data has also been used to track associates of criminals. However, mobile phone data evidence has also been contested in other cases. In a 2009 case, evidence from cellphone records obtained during the investigation was found inadmissible, after it was noted that the orders were extended to the accused person's advocate, their private investigator and their family (State vs. Agliotti 2010).

11. What is working? What gaps are there in existing policy, practice, knowledge and capacity?

RICA is useful as it outlaws arbitrary surveillance. However, the law is not sufficient to protect privacy in the digital age, given its ambiguity in metadata collection. The judicial authorisation process is also cloaked in secrecy, denying protection of the rights of surveillance subjects.

The amaBhungane judgement highlights the weaknesses in South Africa's surveillance law. It shows that bulk surveillance and foreign signal interception go against the necessity principle and can therefore not be a lawful limitation of the right to privacy. It also calls for transparency through post-surveillance notification and for the independence of the judge responsible.

The judgement does not, however, annul the law in its entirety, as it is cognisant of the importance of a legal framework for government-led surveillance. The UN Draft Legal Instrument and the International Principles provide some pointers for areas where the law could be strengthened. These include: transparency through notification of surveillance subjects as well as better reporting to both the public and Parliament; creation of mechanisms for appeal against wrongful surveillance; carrying out a human rights assessment of the Act, to remove provisions and tools that defeat the right to privacy (for example, metadata retentions); and involvement of a range of stakeholders such as academics, lawyers and journalists in oversight of the law.

On surveillance oversight, reports by the JSCI have not sufficiently addressed technology-based surveillance. The Committee therefore needs to increase its focus on emerging surveillance through artificial intelligence so as to provide the required checks and balances.

There also appears to be a gap in public awareness on the problem of mass surveillance in South Africa. By expanding the critical mass of people who are aware of mass surveillance, the public and social movements would be more informed to demand greater transparency of surveillance.

12. What recommendations arise for future legislation, practice, or further research?

- As South Africa goes through the process of reforming its surveillance law to align with the amaBhungane judgement, the UN Draft Legal Instrument can provide some guidelines on the law. Some recommendations for the Instrument include the following.
    - The surveillance law should redefine the basis of surveillance to clearly and more narrowly delineate reasons for surveillance such as financial monitoring and terrorism. The law should also incorporate regulation of mass surveillance.
    - There should be a subject-notification requirement in RICA to enable people under surveillance to be aware of the fact and of the nature of that surveillance.
    - The judicial pre-authorisation regime could be reformed by having independent judges who are well resourced to handle the large number of applications for targeted surveillance. In addition, the law should incorporate a public advocate in RICA warrant applications. Such a person or organisation would provide alternative insights to the RICA judge and increase the accountability in the application process.
    - The grounds for surveillance, especially on crime, should be revised to be more succinct. Standards such as probable cause should be incorporated to strengthen rights protection for the current regime where interception warrants can be issued for threats to national security, public health and safety.
    - RICA provides for law enforcement to acquire metadata, but without protections on metadata retention. In light of the increasing use of data for surveillance, data protection principles such as data minimisation, retention, transparency, lawfulness and fairness should be applied to metadata interception.
    - Other areas that could be strengthened under RICA include the governance and oversight mechanisms. Opportunities for civilian oversight of the regime, where experts in surveillance matters could also advise on the RICA reports, should be

opened up. There is need for independent oversight with access to all data in order to verify whether the legislature's intentions are reflected in practice and to provide public confidence.

- The law should protect public interest professionals such as journalists and lawyers from breaking their professional codes or duty of care owed to their clients and sources.

- Further recommendations on legal reform include the following.
  - Exceptions under the POPI Act should be reviewed to ensure that government offices are not entirely exempted from the privacy law but from some of its provisions (for example, seeking consent). This would bring an added oversight to surveillance activities from the Office of the Information Regulator.
  - Other important areas of South African law that require urgent intervention in relation to surveillance include the regulation of CCTV. In addition, there is a need for governance of algorithms used for surveillance-related purposes such as facial recognition.
- Besides laws, there is a need for greater awareness of surveillance practices among the public. This will increase the critical mass of people who keep the state accountable for surveillance, especially with new data-intensive programmes such as digital ID and smart cities.
- RICA has not been subjected to a human rights impact assessment. Since its implementation has been suspended for a year to allow for rectification of the issues identified in the amaBhungane judgement, this provides an opportunity for multi-stakeholder engagement in reform of the law as well as the surveillance environment to make it more rights-centric.
- Areas of further research include:
  - Studies on South Africa as a surveillance producer and exporter – the actors, hidden actors and impacts of the industry.
  - The impact of artificial intelligence and surveillance in African countries, with South Africa as a case study.
  - A study on how the Mistry case (see Section 10, page 14) has been used in other African countries to argue for the link between privacy and surveillance.

References

Africa, S. (2009) 'The South African Intelligence Services: A Historical Perspective', in S. Africa and J. Kwadjo (eds), *Changing Intelligence Dynamics in Africa*, Birmingham: Global Facilitation Network for Security Sector Reform

Allen, K. and van Zyl, I. (2020) ***Who's Watching Who? Biometric Surveillance in Kenya and South Africa***, ENACT (accessed 10 August 2021)

amaBhungane Centre for Investigative Journalism and Stephen Patrick Sole v. Minister of Justice and Correctional Services and Nine Others (2021) **Constitutional Court of South Africa. Case CCT 278/19** (accessed 10 August 2021)

Black Sash (2019) Black Sash ***Submission UN General Assembly on Digital Technology, Social Protection and Human Rights***, Cape Town: Black Sash (accessed 10 August 2021)

Bosch, T. and Roberts, T. (2021) 'South Africa Digital Rights Landscape Report' in T. Roberts (ed), ***Digital Rights in Closing Civic Space: Lessons from Ten African Countries***, Brighton: Institute of Development Studies (accessed 9 August 2021)

Breckenridge, K. (2014) *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*, Cambridge: Cambridge University Press

Calandro, E. and Berglund, N. (2019) ***Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC Case***, Research ICT Africa (RIA) (accessed 9 August 2021)

Duncan, J. (2018) *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa*, Johannesburg: Wits University Press

EFF (2013) ***International Principles on the Application of Human Rights to Communications Surveillance***, Electronic Frontier Foundation (accessed 9 August 2021)

Farrell, N. (2019) **'UK and South African Government are Tapping Sea Cables'**, *Fudzilla*, 9 September (accessed 10 August 2021)

Feldstein, S. (2019) ***The Global Expansion of AI Surveillance***, Washington DC: Carnegie Endowment for International Peace (accessed 10 August 2021)

Gillwald, A.; Razzano, G.; Rens, A. and van der Spuy, A. (2020) 'South Africa: Protecting Mobile User Data in Contact Tracing', in L. Taylor, G. Sharma, A. Martin and S. Jameson (eds), *Data Justice and COVID-19: Global Perspectives*, London: Meatspace Press

Klaaren, J. (2015) **Three National Security Legislative Regimes in South Africa**, *SSRN* (accessed 9 August 2021)

Kwet, M. (2020) **'Surveillance in South Africa: From Skin Branding to Digital Colonialism'**, in The Cambridge Handbook of Race and Surveillance, *SSRN* (accessed 9 August 2021)

Kwet, M. (2017) ***Operation Phakisa Education: Why a Secret? Mass Surveillance, Inequality, and Race in South Africa's Emerging National e-Education System***, *SSRN* (accessed 9 August 2021)

Marais, N. (2021) ***Building a Fit for Purpose South African Intelligence Service***, Johannesburg: Brenthurst Foundation (accessed 9 August 2021)

McLaughlin, J. (2016) ***'South African Spy Company Used by Gadaffi Touts its NSA-like Capabilities'***, *The Intercept,* 31 October (accessed 9 August 2021)

Mistry v. Interim National Medical and Dental Council of South Africa (1998) ***Constitutional Court of South Africa, Case CCT 13/97*** (accessed 9 August 2021)

Mohapi, T. (2019) '***South Africa's Mass Surveillance Revealed'***, *iAfrikan,* 2 September (accessed 9 August 2021)

Nathan, L. (2017) '***Who's Keeping An Eye on South Africa's Spies? Nobody, and That's the Problem'***, *The Conversation,* 25 September (accessed 10 August 2021)

Nathan, L. (2009) 'Exploring the Domestic Intelligence Mandate: The Case of South Africa', in S. Africa and J. Kwadjo (eds), *Changing Intelligence Dynamics in Africa*, Birmingham: Global Facilitation Network for Security Sector Reform

Privacy International (2014) **'South African Government Still Funding VASTech, Knows Previous Financing Was For Mass Surveillance'**, *Privacy International,* 30 January (accessed 9 August 2021)

Republic of South Africa (RSA) (2020) ***Disaster Management Act: Regulations Relating to COVID-19, Government Notice 318 of 2020*** (accessed 10 August 2021)

RSA (2004) ***Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004*** (accessed 10 August 2021)

RSA (2002) ***Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002*** (accessed 10 August 2021)

RSA (2001) ***Financial Intelligence Centre Act 38 of 2002*** (accessed 10 August 2021)

RSA (1996) ***Constitution of the Republic of South Africa*** (accessed 10 August 2021)

RSA (1994) ***Intelligence White Paper*** (accessed 13 Aug 2021)

State v. Agliotti (2010) **South Gauteng High Court SS 154/2009** (accessed 10 August 2021)

Swart, H. (2017) **'Op-Ed: Big Brother is Watching your Phone Call Records'**, *Daily Maverick,* 10 May (accessed 10 August 2021)

Swart, H. (2015) **'Say Nothing – The Spooks are Listening'**, *Mail & Guardian,* 17 December (accessed 10 August 2021)

Tembo, J.M.C. (2013) **Support for Harmonization of the ICT Policies in Sub-Sahara Africa, 2nd workshop on Lesotho National Transposition of SADC Cybersecurity Model Laws, Maseru, 2–5 April, HIPSSA** (accessed 10 August 2021)

United Nations (2018) ***Draft Legal Instrument on Government-Led Surveillance and Privacy*** (accessed 10 August 2021)